**CENTRO DE POSGRADOS**

**Tema:**

# INCORPORACIÓN DE MECANISMOS DE CIBERSEGURIDAD EN EL SISTEMA DE INFORMACIÓN CATASTRAL DEL GAD DE MERA

**Proyecto de investigación y desarrollo previo a la obtención del título de Magister en Ciberseguridad**

**Línea de investigación:**

SEGURIDAD DE LA INFORMACIÓN

**Autor:**

Roger Israel Espín Lascano

**Director:**

PhD. Omar Salvador Gómez Gómez

**Ambato – Ecuador**

**Agosto 2025**

## DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **ROGER ISRAEL ESPÍN LASCANO,** con cédula de ciudadanía **1600493835**, autor del trabajo de graduación intitulado: “INCORPORACIÓN DE MECANISMOS DE CIBERSEGURIDAD EN EL SISTEMA DE INFORMACIÓN CATASTRAL DEL GAD DE MERA”, previo a la obtención del título profesional de **MAGISTER EN CIBERSEGURIDAD**, en el centro de **POSGRADOS.**

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, agosto 2025

Roger Israel Espín Lascano
CC. 1600493835

**PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR**

**SEDE AMBATO**

**APROBACIÓN DEL TRIBUNAL DE GRADO**

**Tema:**

**INCORPORACIÓN DE MECANISMOS DE CIBERSEGURIDAD EN EL SISTEMA DE INFORMACIÓN CATASTRAL DEL GAD DE MERA**

**Línea de investigación:**

SEGURIDAD DE LA INFORMACIÓN

**Autor:**

Roger Israel Espín Lascano

Omar Salvador Gómez Gómez, Ing. PhD. f._____

CC. 1756723431

**CALIFICADOR**

Darío Javier Robayo Jácome, Ing. Mg. f._____

**CALIFICADOR**

Galo Mauricio López Sevilla, Ing. Mg. f._____

**CALIFICADOR**

Dayamy Lima Rojas, Lic. Mg. f._____

**DIRECTORA CENTRO DE POSGRADOS**

Diego Gonzalo Coca Chanalata, Dr. f._____

**SECRETARIO GENERAL PUCESA**

**Ambato – Ecuador**

**Agosto 2025**

**RESUMEN**

En el presente proyecto de investigación se propone un modelo de prototipo de ciberseguridad para el sistema de gestión catastral “ANZU” del GADM del cantón Mera con el fin de determinar los mecanismos más adecuados de ciberseguridad que protejan la información generada en la municipalidad.

Se inicia a través de la metodología Deming, que consiste en: Planificar, Hacer, Revisar y Actuar (PDCA). En la fase de planificación se pueden ver reflejados dos objetivos primarios: recopilar bibliográficamente información sobre los mecanismos de ciberseguridad existentes y diagnosticar la situación actual del sistema de información catastral; en el primero se eligen mecanismos ya conocidos a implementar, mientras que el segundo comienza un análisis de riesgos con la metodología CIS RAM (*Center for Internet Security Risk Assessment Method*) que posteriormente es evaluado en la fase revisión.

A continuación se usa varios mecanismos existentes en la segunda fase y gestionando los riesgos mediante políticas, herramientas de software, controles de seguridad y reestructuración de la infraestructura de red se concluye la fase de “hacer” finalmente en la fase de “verificar” se evalúan a las amenazas después de la aplicación del prototipo, planificando acciones correctivas y de mejora, concluyendo que el riesgo se reduce al 50 por ciento, entrando en un valor aceptable según los criterios de evaluación escogidos en la metodología, además, en la fase de “actuar” se plantean acciones correctivas, con el fin de reducir el riesgo de ataques.

**Palabras clave:** simulación, software, instalación, generación, seguridad.

**ABSTRACT**

*This research project proposes a cybersecurity prototype model for the cadastral management system "ANZU" of the GADM of the canton of Mera to determine the most appropriate cybersecurity mechanisms to protect the information generated in the municipality.*

*It starts through the Deming methodology, which consists of Plan, Do, Check, and Act (PDCA). In the planning phase, two primary objectives are reflected: to gather bibliographic information on existing cybersecurity mechanisms and to diagnose the current situation of the cadastral information system; in the first one, already known mechanisms to be implemented are chosen, while the second one starts a risk analysis with the CIS RAM methodology (Center for Internet Security Risk Assessment Method), which is later evaluated in the review phase.*

*Then, using various existing mechanisms in the second phase and managing the risks through policies, software tools, security controls, and restructuring of the network infrastructure concludes the "do" phase, and finally, in the "verify" phase, the threats are evaluated after the application of the prototype. Eventually, the threats are reviewed after the application of the prototype, planning corrective and improvement actions, concluding that the risk is reduced to 50 percent, entering an acceptable value according to the evaluation criteria chosen in the methodology, in addition, in the "act" phase, corrective actions are proposed, to reduce the risk of attacks.*

***Keywords:*** *simulation, software, installation, generation, security.*

## ÍNDICE GENERAL DE CONTENIDOS

## ÍNDICE DE TABLAS

## ÍNDICE DE ILUSTRACIONES

## INTRODUCCIÓN

El crecimiento y el despliegue del internet contribuyeron a la evolución de los sistemas de información, marcando un antes y después en los métodos y formas en las que la sociedad accede a la información. Juntamente con este mencionado crecimiento nacieron los denominados “Ciberdelincuentes” que han venido desarrollando numerosas técnicas para aprovechar vulnerabilidades con el fin de acceder a información confidencial y obtener algún beneficio (Gamon, 2017).

Según un reporte de la revista *Statista*, Ecuador en el 2018 era el país con mayor penetración de internet entre los países más poblados de América latina (*Infografía*, 2018). Sin embargo, esto no ha sido del todo bueno pues solo en 2018 el Centro de Respuesta a Incidentes Informáticos (EcuCERT) perteneciente a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) reporto 1′609,997 direcciones IP’s comprometidas con una variedad de incidentes (ARCOTEL, 2019).

Las instituciones públicas proveen varios servicios a través de internet con el fin de facilitar el acceso a la información y mejorar la interacción con la cadena de valor de estas. Múltiples tecnologías se han desplegado para brindar estos servicios a los ciudadanos con una variedad de beneficios como facilitar pagos, consultas, boletines informativos, etc. Un ejemplo de esto es que para la interacción entre sistemas de gobierno existe la plataforma denominada bus de servicios gubernamental (BSG) esta, además, de permitir transportar datos da la posibilidad de consultas para instituciones públicas que lo requieran. Solo hasta el 2018 se realizaban 740000 consultas diarias (“Bus de Servicios Gubernamentales MINTEL”, 2018), todo esto trae consigo varios desafíos tales como: rendimiento, aplicabilidad, pero sobre todo en temas de ciberseguridad.

En el 2021 un gran número de instituciones públicas fueron blanco de ataque por parte de ciberdelincuentes. El consejo de comunicación el Servicio de Rentas Internas (SRI), la Empresa Pública de Hidrocarburos (PETROECUADOR), el Instituto de Seguridad Social (IEES) y la Corporación Nacional de Telecomunicaciones (CNT) se vieron afectadas por ataques cibernéticos, esta última fue la más perjudicada pues tardaron varios días hasta reestablecer los

servicios a sus clientes (P. Y. L. 4 de A. de 2021 D. Quito, s/f; P. Y. L. 19 de J. de 2021 D. Quito, s/f).

Otra empresa pública que fue víctima de un incidente de ciberseguridad fue la Agencia nacional de Transito (ANT) pues en Julio del 2021 presentaron una denuncia formal alegando que: “Las denuncias tiene que ver con la vulneración de los sistemas informáticos y la entrega ilegal de licencias a nivel nacional” pues se entregaban licencias de manejar irregulares y ha causado graves pérdidas económicas a la institución ("ANT presenta quinta denuncia contra ataques informáticos", 2021).

La gestión de la seguridad de la información tiene que ser una parte integral de todas las instituciones públicas. La gran cantidad de información municipal que se genera en estas instituciones obliga el establecimiento de políticas, normas y procedimientos puntuales para la manipulación, procesamiento y resguardo de datos procesados, todo esto bajo cumplimiento de la ley Orgánica de Protección de Datos Personales (LOPD) aprobada en 2021 (“Ecuador y su primera Ley Orgánica de Protección de Datos Personales”, 2021).

Los Gobiernos Autónomos Descentralizados (GAD) al ser instituciones que gozan de autonomía financiera, administrativa y política (Jarrín et al., s/f) tienen a su cargo ciertos procesos que son su competencia exclusiva como por ejemplo: la difusión, manipulación, formación y mantenimiento de los catastros. Un catastro predial es la base para la planificación rural y urbana como también para el cálculo del impuesto predial (Peña Segura, s/f). Hoy en día los GAD cuentan con sus propios sistemas web publicados para el acceso de la ciudadanía o para automatizar procesos internos, uno de ellos son los sistemas catastrales que tiene como objetivo inventariar, calificar y valorar los bienes. Estos sistemas generalmente están basados en sistemas de información geográfica (GIS).

En Ecuador, con el fin de garantizar la seguridad de la información se pretende implementar las todas las instituciones el denominado Esquema Gubernamental de Seguridad de la información (EGSI) que según la página del gobierno es “EGSI busca preservar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos de seguridad de la

información y la selección de controles para el tratamiento de los riesgos identificados" ("EGSI v2", s/f).

En las revisiones de las definiciones de casos de uso que implementan en las redes de área amplia definida por *software* no se consideran implementaciones a nivel local porque no existen, sin embargo, se investigó casos de éxito en países que cuentan con tecnologías avanzadas donde promueven y apoyan la protección de la información y la gestión de la seguridad según el modelo de defensa en profundidad.

El GAD municipal del cantón Mera ubicado en la provincia de Pastaza no contaba con un sistema destinado a manejar la información de los catastros, a pesar de que el GAD cuenta 2224 viviendas ocupadas según el INEC (Mera & Areas, s/f), todo esto suponía ciertos conflictos para la automatización, digitalización y consultas externas acerca de las características físicas de cada bien inmueble. En el año 2020 la administración de ese entonces decidió adquirir un sistema WEB basado en las normas técnicas nacionales para el catastro de bienes inmuebles urbanos - rurales y avalúos de bienes; operación y cálculo de tarifas por los servicios técnicos de la dirección nacional de avalúos y catastros (*Acuerdos. 017-21 Refórmese el Acuerdo Ministerial No. 020-20 de 25 de mayo de 2020*, s/f). Sin embargo, no se han tomado medidas con respecto a ciberseguridad.

Por lo tanto, la problemática dentro del sistema ANZU es que no cuenta con mecanismos de ciberseguridad para proteger a los servicios y la información catastral de los ciudadanos del cantón Mera. Por lo que lo hace vulnerable a intermitencias en el servicio o hasta secuestro y difusión de información confidencial.

Este proyecto tiene como objetivo la incorporación de mecanismos de ciberseguridad al sistema catastral, por lo tanto, el GAD cantonal de Mera juntamente con el autor de este proyecto, son los responsables de la implementación y cumplimiento del prototipo resultante de esta investigación. Comprometiéndose a realizar auditorías para verificar el correcto funcionamiento y realizar las correcciones del caso.

**Objetivos general**

- Incorporar mecanismos de ciberseguridad en el sistema catastral del GAD de Mera, para mejorar la integridad de la información.

**Objetivos específicos**

- Recopilar bibliográficamente información sobre los mecanismos de ciberseguridad existentes.
- Diagnosticar la situación actual del sistema de información catastral del GAD de Mera.
- Determinar mecanismos de ciberseguridad para sistema de información catastral del GAD de Mera.
- Desarrollar un prototipo de mecanismos de ciberseguridad en sistema de información catastral del GAD de Mera.

Esta investigación comprende el diseño de los mecanismos de ciberseguridad para el sistema de información catastral del GAD de Mera haciendo hincapié en sus activos relacionados y en los procesos sobre los que basa su funcionamiento. Para llegar al objetivo se plantea una metodología en fases (PDCA) que consiste en Planificar, Hacer, Revisar y Actuar. En la etapa inicial, es decir planificar, se utiliza una metodología de seguridad de la información para el análisis de riesgos denominada CIS RAM (Center for Internet Security Risk Assessment Method) que analiza los riegos asociados a cada activo relacionado al sistema catastral. Cada fase permite llegar al objetivo que es implementar mecanismos de ciberseguridad y diseñar un prototipo que permita proteger al sistema como tal, además, de una mejora continua.

Por lo tanto, la ejecución de este proyecto está justificada, el GAD municipal tiene como obligación proteger la información catastral de la ciudadanía del cantón, así como, garantizar la continuidad de los servicios. Los beneficios no son solo técnicos sino de imagen institucional, una institución pierde credibilidad cuando existen vulneraciones o filtraciones de datos, un ciudadano debe tener la tranquilidad de que su información está en las manos correctas y siempre esté disponible.

# CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

## 1.1. Conceptos de seguridad de la información

### Seguridad de la información

La seguridad es un concepto que tiene como objetivo proteger los recursos personales, información e instalaciones de un individuo u organización particular. La seguridad de la información se puede definir como un conjunto de medidas o políticas para asegurar la información existente dentro de un sistema de información y que es transmitida por un sistema de comunicación, siempre teniendo en cuenta que se mantendrá la confidencialidad, integridad y la disponibilidad de esta (Gutiérrez & Ayuso, 2003).

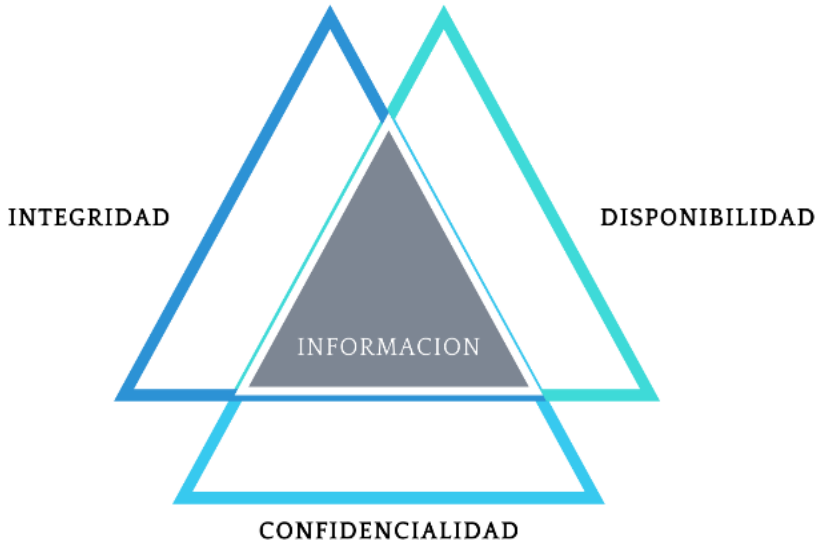
### Confidencialidad

La confidencialidad asegura que el acceso a la información esté disponible solo para las personas con las que se desea compartirla, es decir trata de proteger los datos de aquellos que no estén autorizados (Briceño, 2021). Desde un usuario normal hasta grandes instituciones tienen información que es confidencial. No asegurar dicha confidencialidad significarían grandes consecuencias como la pérdida de reputación y confianza de dicha institución o en el caso de un usuario normal la información íntima revelada y afectaría la honra de la persona (Karamanian, 2011).

### Integridad

La integridad es un concepto que hace referencia a la fidelidad de la información, su objetivo es prevenir modificaciones no autorizadas. La información trasmitida por un medio o almacenada dentro de una base de datos tiene que mantener su información original, por ejemplo, mientras esta información está en tránsito podría ser modificada por un tercero (Karamanian, 2011). Existen muchas técnicas para garantizar la integridad, una de las más usadas es las funciones resumen o *Hash*. Este *Hash s*e adjunta de manera encriptada al mensaje, si al desencriptar los *hashes* no coinciden, la información fue modificada en algún momento de su trayecto (MIGUEL, 2019).

**Ilustración 1.** Principios seguridad de la información




**Fuente:** elaboración propia

## Autenticación y no repudio

A la autenticación se la define como el proceso para identificar a todas las partes que participan en una comunicación y asegurar que cada una es quien dice ser, como, por ejemplo, un usuario que quiere acceder a un recurso requiere una identificación puesto que es necesario que el sistema sepa quién es y una autenticación para demostrar al recurso que es quien dice ser. Un sistema de autenticación contará con al menos tres fases: autenticación, autorización y un registro de los acceso al sistema (CARLOS & ANTONIO, 2017).

Aquí nace otro concepto, el no repudio, este se encarga de asegurar que un usuario realizó cierta acción (enviar un mensaje) y que no quede duda de ello. Existen dos tipos de no repudio

- **En origen**: Indica que el mensaje fue enviado por el emisor, sin que dé lugar a dudas de quien fue el autor. El emisor no puede negar que realizó dicha acción puesto que el que recibió el mensaje puede probarlo.
- **En destino**: Indica que el mensaje fue recibido por el receptor y no pueda negarlo. El receptor no puede negar que recibió el mensaje, puesto que la persona que lo envió tiene prueba de ello (TERÁN, 2014).

## Autorización

La autorización es concepto que dicta que, a un usuario, sistema u otro involucrado se permite o deniega el acceso a un recurso según los permisos que corresponden o sean asignados. Una de las buenas prácticas dentro de cualquier organización es identificar bien los niveles de acceso según las políticas dentro de la empresa (Briceño, 2021). Toda autorización depende de la criticidad de la información, las organizaciones suelen tener niveles de criticidad dentro de ellas, por lo tanto, los recursos y datos tendrán su propio nivel de autorización. Además, la autorización siempre garantizará la integridad y confidencialidad (López, 2010).

## Amenaza

Una amenaza es cualquier evento intencional o accidental que provocaría daños a una organización. Dichos eventos aprovechan las vulnerabilidades presentes en un recurso en particular presentando efectos negativos sobre cualquier elemento de los recursos. Se lo clasifica en tres categorías:

- **Amenazas naturales**: Pueden ser cualquier evento natural que afecte al normal funcionamiento de un sistema en particular como lluvia, incendio o fallos eléctricos.
- **Agentes externos**: Espionaje, virus, sabotaje, conflictos sociales, ingeniería social, etc.
- **Agentes internos**: Empleados descontentos o que no cuentan con la formación adecuado, errores en la administración de sistemas, etc., (CARLOS & ANTONIO, 2017).

## Vulnerabilidad

Las vulnerabilidades son fallos o debilidades en un sistema o recurso informático que pueden ser aprovechada por una amenaza, la ISO 27005 la define como:

> Una debilidad de un activo o grupo de activos que serían explotados por una o más amenazas cibernéticas donde un activo es cualquier cosa que tenga valor para la organización, sus operaciones comerciales y su continuidad, incluidos los recursos de información que respaldan la misión de la

organización (*ISO/IEC 27005:2018(en), Information technology — Security techniques — Information security risk management*, s/f).

Las vulnerabilidades suelen están relacionadas a:

- Sistemas complejos
- Mala gestión de contraseñas
- Errores de *software* y sistemas operativos
- Configuraciones por defecto
- Usuarios finales (Smith, 2011).

**Riesgo**

El concepto de riesgo es bastante ambiguo, sin embargo, en seguridad de la información se lo define como la probabilidad de que una amenaza aproveche una vulnerabilidad en algún recurso o activo. Una entidad puede ser la suma de varias partes, un riesgo de igual manera, por lo tanto, se tienen los siguientes componentes de un riesgo.

- **Evento**: Es una situación que es posible, pero no es seguro que ocurra. En una evaluación de riesgos un evento siempre será algo negativo y siempre será visto a futuro.
- **Activo:** Un activo es un objeto directo o indirecto de evento, desde el punto de vista de la seguridad de la información un activo será una base de datos, *software*, etc.
- **Resultado:** Es el resultado del evento o el impacto que este pueda tener, desde el punto de vista de un análisis de riesgo siempre será negativo, pues es una circunstancia adversa que afectaría a un activo.
- **Probabilidad:** Una medición cuantitativa de que ocurra un evento futuro (Talabis & Martin, 2012).

## 1.2. Estándares de seguridad de la información

### ISO 27000

La familia de estándares ISO 27000:2018 provee un conjunto de normas para la implementación de un Sistema de gestión de seguridad de la información (SGSI), pudiendo ser aplicables a organizaciones pequeñas, medianas y grandes (*ISO/IEC 27000 – Key International Standard for Information Security Revised*, s/f).

- ISO 27001: es una norma de seguridad de la información, Esta establece que la seguridad de la información es la preservación de la confidencialidad integridad y disponibilidad de todos los sistemas que traten, procesen y almacenen información dentro de una organización, se orientan a proteger los activos de información y se basan en normas, técnicas, políticas y demás elementos para aplicar medidas de seguridad. Este estándar define 14 secciones desglosada en 114 controles:
    - Políticas de seguridad de la información.
    - Organización de la seguridad de la información.
    - Seguridad de los recursos humanos.
    - Gestión de activos.
    - Controles de acceso.
    - Criptografía – Cifrado y gestión de claves.
    - Seguridad física y ambiental.
    - Seguridad operacional.
    - Seguridad de las comunicaciones.
    - Adquisición, desarrollo y mantenimiento del sistema.
    - Gestión de incidentes de seguridad de la información.
    - Cumplimiento (Heredero et al., 2019).

- ISO 27002: es un estándar titulado: Técnicas de seguridad, Código de prácticas para los controles de seguridad de la información, que determina las mejores prácticas para la administración de seguridad de la información y la interoperabilidad de los sistemas, esta norma está conformada por 14 dominios, 35 objetivos de control y 114 controles (Calder, 2011).

- ISO 27003: es una guía de implementación para un SGSI, su objetivo básicamente es definir los aspectos más importantes para un diseño exitoso y una implementación basada en las ISO 27001 (*ISO/IEC 27003 - Guía para la implementación de un Sistema de Gestión de Seguridad de la Información.*, 2014).

- ISO 27004: define un conjunto de prácticas o normas para evaluar los resultados de un SGSI basado en 27001. Este estándar recomienda que la estructura tenga el sistema de medición, cómo medirlas, qué parámetros y cuándo medirlos. El estándar plantea seis etapas:

    - Elección de los objetivos y procesos de medición
    - Descripción de las líneas principales
    - Selección de datos
    - Desarrollo de un sistema de medición
    - Interpretación de los valores medidos
    - Notificación de los valores de medición (Andress & Leary, 2016).

- ISO 27005: se encarga de definir normas y orientaciones sobre gestión de riesgos de seguridad de la información que son parte de la implementación del SGSI, también gran parte del estándar define la evaluación de riegos desde una óptica de alto nivel y cuenta con 6 áreas de interés.

    - Establecimiento del contexto.
    - Evaluación de Riesgos de Seguridad de la Información.
    - Tratamiento de Riesgos de Seguridad de la Información.
    - Aceptación de Riesgos de Seguridad de la Información.
    - Comunicación de Riesgos de Seguridad de la Información.
    - Monitoreo y Revisión de Riesgos de Seguridad de la Información (Talabis & Martin, 2012).

### *CIS (Center for Internet Security)*

Los Controles críticos de seguridad del Centro para la seguridad de Internet (CIS) son un conjunto de normas, políticas, buenas prácticas y acciones para mejorar la ciberseguridad de las organizaciones con el fin de prevenir los ataques más comunes (DDoS, Filtraciones de datos, espionaje corporativo, etc.) y con más impacto para la misma. CIS ayudará a responder preguntas como el origen o causa de los ataques, dominios críticos para una gestión de riesgos y herramientas que ayudarán a resolver problemas (Priyadarshini & Cotton, 2022).

Los controles CIS se dividen en tres categorías: básicos, fundamentales y organizacionales, que a su vez se dividen en 20 controles cada uno con sub-controles.

Básicos

- Inventario y control de activos de *hardware.*
- Inventario y control de activos de *software .*
- Gestión continua de vulnerabilidades.
- Uso controlado de los privilegios administrativos.
- Configuración segura para el *hardware* y el *software* de los dispositivos móviles, laptops, estaciones de trabajo y servidores.
- Mantenimiento, monitoreo, y análisis de *logs* de auditoría.

Fundamentales

- Protección de correo electrónico y navegador web
- Defensas contra *malware*
- Limitación y control de puertos de red, protocolos y servicios
- Funciones de recuperación de datos
- Configuración segura para dispositivos de red, tales como *firewalls, routers* y *switches*
- Protección perimetral
- Protección de datos
- Control de acceso basado en la necesidad de saber

- Control de acceso inalámbrico
- Monitoreo y control de cuentas

Organizacionales

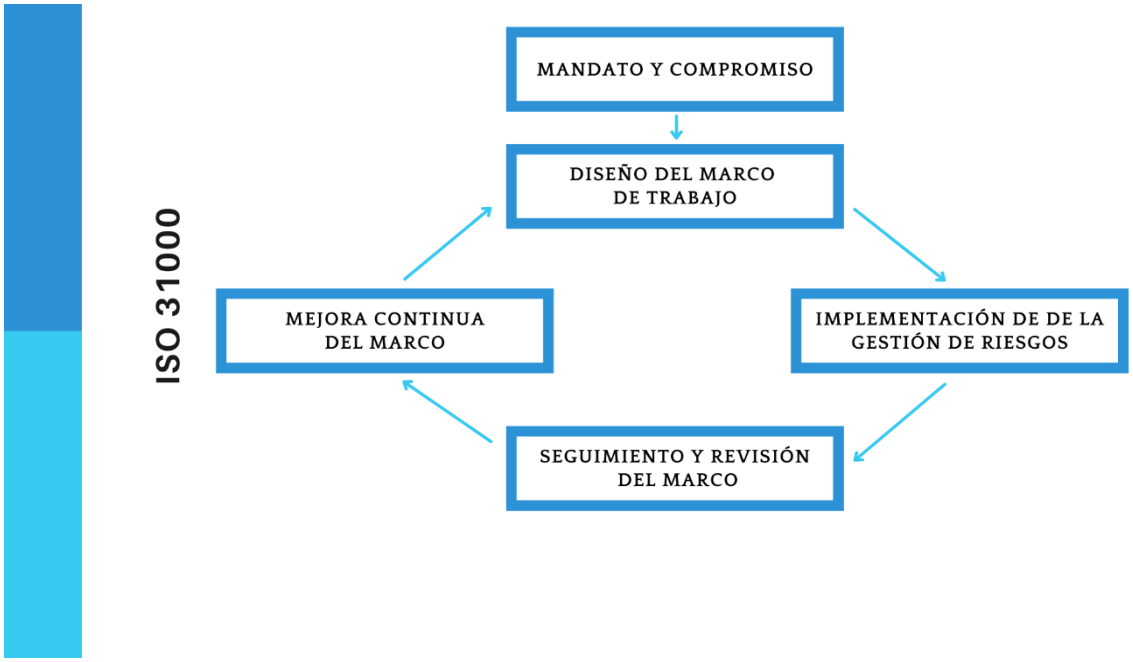
- Implementar un programa de concienciación y capacitación en seguridad
- Seguridad del *software* de aplicación
- Respuesta y gestión de incidentes
- Pruebas de penetración y ejercicios de equipo rojo (*Learn about the CIS Controls™*, s/f).

## Metodologías de evaluación de riesgos

### *Magerit*

*Magerit* es una metodología para la gestión y análisis de riesgos que se encuentra bajo mantenimiento por la Secretaría General de Administración Digital (Ministerio de Asuntos Económicos y Transformación Digital) juntamente con el Centro Criptológico Nacional (CCN). *Magerit*, además, esta alineada al estándar ISO 31000 respondiendo al “Proceso de Gestión de los Riesgos” que se encuentra en la sección 4.4 “Implementación de la Gestión de los Riesgos”. El principal objetivo de usar esta metodología suele ser tomar decisiones para implementar un proceso de gestión de riegos para el uso de tecnologías de la información (*Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*, s/f).

**Ilustración 2.** ISO 31000 - Marco de trabajo para la gestión de riesgos




**Fuente:** Marco de trabajo para la gestión de riesgos ISO 31000

## Objetivos

*Magerit* divide sus objetivos en dos partes: objetivos directos e indirectos. Los objetivos directos son:

- Crear conciencia a la alta dirección de las organizaciones acerca de los riesgos de los activos de información.
- Que la alta dirección sepa gestionar los riesgos.
- Ofrecer una metodología sistemática para el análisis y gestión de riesgos procedentes del uso de tecnologías de la información.
- Auxiliar en el descubrimiento de planes para que el tratamiento de riegos sea adecuado y oportuno.

Mientras que los objetivos indirectos son:

- Preparar a la organización para que su sistema de gestión de seguridad de la información sea auditado, evaluado o certificado (*Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*, s/f).

## Guías

La metodología tiene tres volúmenes:

### Volumen I: Método

- Capítulo I: Fase introductoria donde se detallan organismos que lo crearon.
- Capítulo II: Visión de Conjunto en el cual se definen las actividades de análisis y tratamiento de riesgos.
- Capítulo III: Método de Análisis de Riesgos en el cual se define esquemáticamente el procedimiento para el análisis de riesgos.
- Capítulo IV: Proceso de Gestión de Riesgos, un listado de los procedimientos dentro de la Gestión de Riesgos
- Capítulo V: Proyectos de Análisis de Riesgos, que se centra en los planes de ejecutar análisis de riesgos en los que nos veremos inmersos para verificar los riesgos de un sistema y eventualmente verificar los cambios sustanciales sobre el tratamiento de estos.
- Capítulo VI: Plan de Seguridad que es una guía para ejecutar un Plan de Seguridad con el resultado del Análisis y Gestión de Riesgos, con el fin de tomar decisiones para su tratamiento.

### Volumen II: Catálogo de elementos

Este volumen proporciona tareas para aplicar la metodología con dos objetivos principales: facilitar el trabajo de las personas involucradas en el proyecto y estandarizar los resultados del análisis. Los elementos en los que intervienen son:

- Criterios de evaluación
- Amenazas
- Controles y salvaguardas
- Tipos de activos (*Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*, s/f).

**Volumen III: Guía de Técnicas**

El objetivo de este apartado es describir técnicas y métodos para el análisis y gestión de riesgos que ayudan a alcanzar los objetivos propuestos, las principales técnicas que recoge son:

- Análisis mediante tablas
- Análisis algorítmico
- Vectores de ataque
- Técnicas generales
- Diagramas de procesos
- Técnicas gráficas
- Sesiones de trabajo (*Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*, s/f).

**CIS RAM *(Center for Internet Security Risk Assessment Method)***

El Centro para la Seguridad de Internet (CIS) desarrolló una metodología para el análisis de riesgos que se basa en los denominados controles CIS, aunque también cumple con los estándares establecidos por ISO 27005, NIST SP 800-30 y RISK IT. En abril del 2018 se presentó su primer borrador, actualmente la versión que está vigente es la 2.1(CIS, s/f). CIS RAM que provee una metodología para el análisis de riesgos en ciberseguridad, su núcleo se basa en tres principios que establecen las características de las evaluaciones de riesgo que, a su vez, se alinean con las normas regulatorias y legales, estos principios son:

- El análisis de riesgos considerará los intereses de todas las partes que puedan verse perjudicadas por estos.
- Los riesgos deben reducirse a un nivel que la alta gerencia y las partes potencialmente afectadas encuentren apropiado.
- Las salvaguardias no deben ser más costosas que los riesgos que evitan.

También se ajustan a un conjunto de prácticas

- El análisis de riesgo considera la probabilidad de que ciertas amenazas puedan crear daños de gran impacto.
- Los riesgos y las salvaguardas se evalúan con los mismos criterios para que puedan ser comparados.
- La valoración de impacto y probabilidad tienen un componente cualitativo que establece de manera concisa las preocupaciones de las partes interesadas, las autoridades y la organización evaluadora.
- Las puntuaciones de impacto y probabilidad se derivan de un cálculo numérico que permite realizar una comparación entre todos los riesgos evaluados, salvaguardas y contra los criterios de aceptación del riesgo.
- Las definiciones de impacto aseguran que la magnitud del daño a una de las partes se equipare con la magnitud del daño a las demás partes involucradas.
- Las definiciones de impacto tendrán un límite explícito entre valores que serían aceptables para todas las partes y para aquellas que no lo serían.
- Dirección de definiciones de impacto; la misión o utilidad de la organización para explicar por qué la organización y otros se involucran en el riesgo, los objetivos de interés propio de la organización y las obligaciones de la organización para proteger a otros de cualquier daño.
- El análisis de riesgos se basa en un estándar para analizar los controles actuales y las salvaguardas recomendadas.
- El riesgo es analizado por expertos en la materia que usan evidencias para evaluar riesgos y salvaguardas.
- Las evaluaciones de riesgos no evaluarán todos los riesgos previsibles. Las evaluaciones de riesgo deben repetirse en intervalos regulares (Williams, 2021).

**Proceso**

Dentro del CIS RAM, se evalúa el riesgo a través del siguiente proceso:

1. Definir el alcance mediante un inventario de activos.

2. Dialogar y documentar con los propietarios de los activos particularidades acerca de los mismos.
3. Realizar evaluación de riesgos y criterios de aceptación para evaluar y aceptar el riesgo.
4. Revisar si existen controles a los activos.
5. Modelar los riesgos a través de la evaluación de los controles actuales.
6. Realizar la evaluación de riesgos a través de la estimación de la probabilidad y el impacto para calcular el valor cuantitativito de riesgo.
7. Proponer salvaguardas de controles CIS y evaluar que sean efectivas a la hora de reducir el riesgo siempre sin crear una carga económica, ni administrativa a la organización (Williams, 2021).

**Parámetros de evaluación**

- **Criterios de impacto.**
    - Imperceptible
    - Aceptable
    - No aceptable
    - Alto
    - Catastrófico
- **Niveles de ocurrencia**
    - Remoto
    - Improbable
    - Poco probable
    - Muy probable
    - Definitivo
- **Objetos de impacto**
    - Impacto en la misión
    - Impacto en el objetivo operacional
    - Impacto obligaciones con terceros
    - Impactos económicos.

- **Riesgos aceptables**
    - Para calcular el riesgo se realizará una operación al multiplicar el nivel de ocurrencia por el impacto según su objeto, por lo tanto, definirá un valor de riesgo aceptable (CIS, s/f).

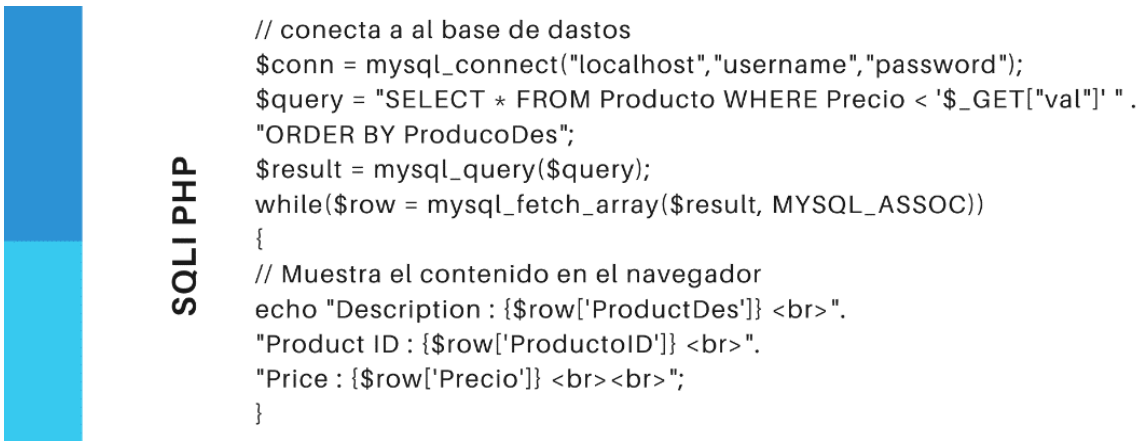
## 1.3. Amenazas

### SQLi *Injection*

Es una vulnerabilidad que resulta cuando un atacante logra influir en las consultas *Structured Query Language* (SQL) deliberadamente, ya sea por fallos en el código o configuraciones erróneas del servidor, SQLi no solamente afecta a sistemas web sino a cualquier aplicativo que acepte entradas desde un cliente no confiable (Aplicaciones de escritorio, móviles etc.). SQLi aprovecha la falta de filtrado o validación de las entradas de un sistema ejecutando consultas para obtener información, además elimina o modifica, todo lo permite SQL (Hartley, 2012).

En la ilustración 3 podemos ver un ejemplo de una falta de validaciones de los datos, la variable ‘val’ no está filtrada, ni escapada, por lo tanto, todos los caracteres que ingresen serán válidos.

**Ilustración 3.** Vulnerabilidad SQLi




**Fuente:** elaboración propia

### *Cross Site Scripting (XSS)*

XSS es una vulnerabilidad grave que será clasificada como inyección de código, resultando una de las más severas y las más comunes dentro de los sistemas WEB. XSS se presenta cuando un atacante inserta un código malicioso dentro de sitios confiables ejecutando esto por lo general dentro del lado del cliente con tecnologías como *JavaScript*. Este tipo de ataque tiene diversos fines como robar *cookies, tokens* de sesión o combinar ataques, al igual que SQLi una de las principales causas es el inapropiado filtrado de los métodos de entrada permitiendo la ejecución del código (Gupta & Chaudhary, 2020).

Según el *Open Web Application Security Project* (OWASP) las vulnerabilidades de XSS se clasifican en los siguientes tipos (*Cross Site Scripting (XSS) Software Attack* | *OWASP Foundation*, s/f):

- Ataques XSS almacenados: Esta variante de XSS se caracteriza porque el código inyectado se almacena permanente en el servidor, la víctima ejecuta el código al realizar una consulta de la base de datos o *log.*

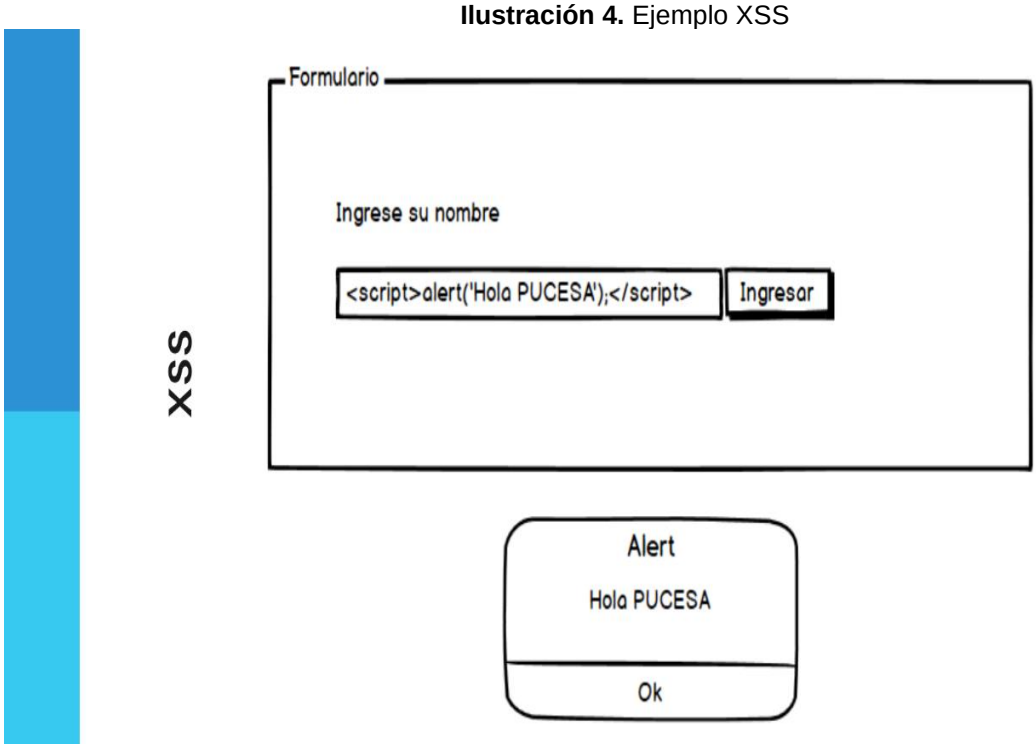
- Blind XSS: Para este caso, al igual que un ataque XSS almacenado, el *payload* se almacena en el servidor y se refleja en la victima al ejecutar el código *backend.*

- Ataques XSS reflejados: XSS reflejados el *script* inyectado se refleja en el servidor web como una respuesta incluyendo parte o toda la solicitud que fue enviada al servidor. En este caso la victima navega en una página aparentemente legitima o un *link* que recibió por correo electrónico, entonces el código es enviado al servidor y refleja el ataque del lado del cliente finalizando con la ejecución de código puesto que aparentemente viene de un sitio confiable.

- DOM *Based* XSS: Esta variante de XSS permite que un atacante ejecuté un código modificando el entorno del modelo de objeto de documento (DOM) dentro del navegador de la víctima. El atacante utiliza el código original del lado del cliente para que se ejecute de manera no adecuada recibiendo la

respuesta HTTP correcta, pero el código del cliente se ejecutara según las modificaciones del atacante (*DOM Based XSS Software Attack* | *OWASP Foundation*, s/f).

**Ilustración 4.** Ejemplo XSS




**Fuente:** elaboración propia

***Broken Access Control***

Los controles de acceso básicamente son un conjunto de políticas y mecanismos para que los usuarios no tengan la capacidad de interactuar más allá de los permisos que se le fueron asignados, mecanismos como manejar la autenticación y la autorización. *Broken access* control es una falla en los mecanismos para limitar el acceso a los recursos entre ellos incluye escalación de privilegios, evadiendo controles de acceso y modificando parámetros para ganar acceso (Deane, 2020). OWASP lo catalogó como la vulnerabilidad más común actualmente con un 94% de incidencia (*A01 Broken Access Control - OWASP Top 10:2021*, s/f).

En la ilustración 5 se verá un esquema general.

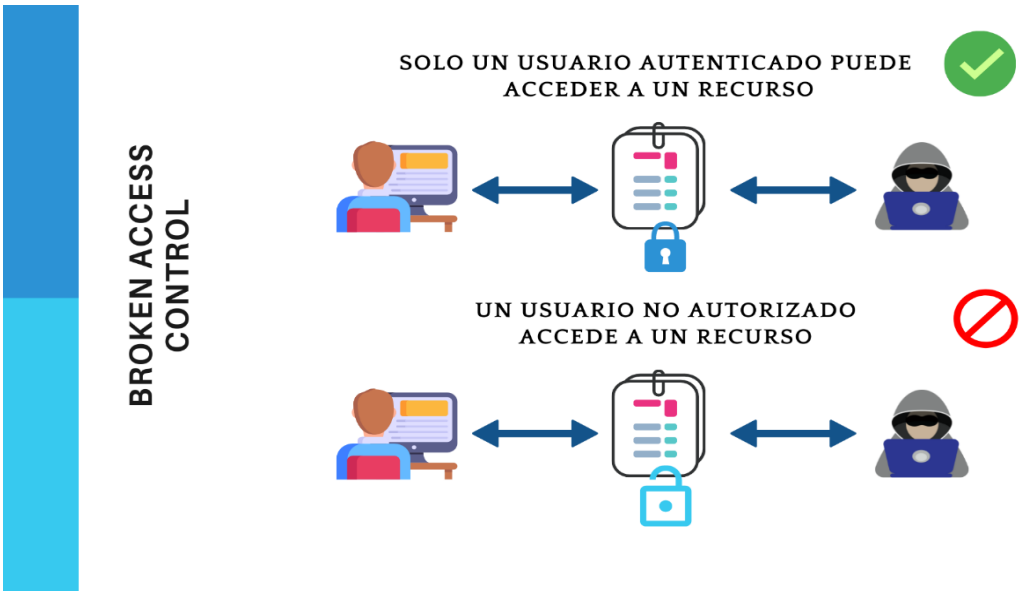
Son 3 tipos:

- **IDOR (*Insecure Direct Object Reference*):** Referencia insegura directa a objeto, esta vulnerabilidad ocurre cuando un sistema falla en sus métodos de autorización y permite acceder directamente a objetos, estos objetos pueden ser funciones o archivos (Canlas & Price, 2021).

- **CSRF (*Client-Side Request Forgery*):** La técnica llamada falsificación de petición en sitios cruzados. Este tipo de ataque suplanta la petición de un usuario en un sitio web vulnerable, utilizando la confianza que el sitio tiene en un usuario autenticado (*¿En qué consiste la vulnerabilidad Cross Site Request Forgery (CSRF)?*, 2015).

- **CORS (*Cross-Origin Resource Sharing*)** el uso compartido de recursos de origen cruzado permite administrar y controlar el acceso a recursos fuera de un dominio, esta vulnerabilidad es una mala configuración, pues si no es implementada la política permitirá ataques de CSRF.

**Ilustración 5.** Esquema *Broken Access Control*




**Fuente:** elaboración propia

## DDoS

Los ataques de denegación (DoS) de servicio o ataques denegación de servicio distribuidos (DDoS) es uno de los ataques más comunes existiendo desde 1974,

con el crecimiento de tecnologías como *BlockChain, Internet of Things* (IoT) o *Cloud Computing* también el DDoS han evolucionado con nuevos métodos y variantes (Gupta & Dahiya, 2021).

Un ataque de denegación de servicio básicamente consiste en hacer que un servicio no esté disponible negando así el acceso a los usuarios. Una de las técnicas más efectivas es generar muchas solicitudes falsas, cuando estas provienen de diferentes orígenes, es un ataque “distribuido” haciendo que el servidor no pueda procesar peticiones legitimas. Un error de personas que no están relacionadas o entendidas en ciberseguridad es pensar que las vulnerabilidades siempre se tratan de errores de *software*, un DDoS se diferencia de los errores de *software* en que el éxito de un ataque dependerá del conocimiento del atacante de la infraestructura y la capacidad de manejar varias fuentes.

Este tipo de ataques suelen tener varias motivaciones: desde hacktivistas, cibercriminales, usuarios enojados, y gente que busca hacerse conocida, pues existen servicios para realizar un DDoS a gran escala pagando un monto de criptomonedas (Chou & Groves, s/f).

Existen varios tipos de DDoS pudiendo ser agrupados así:

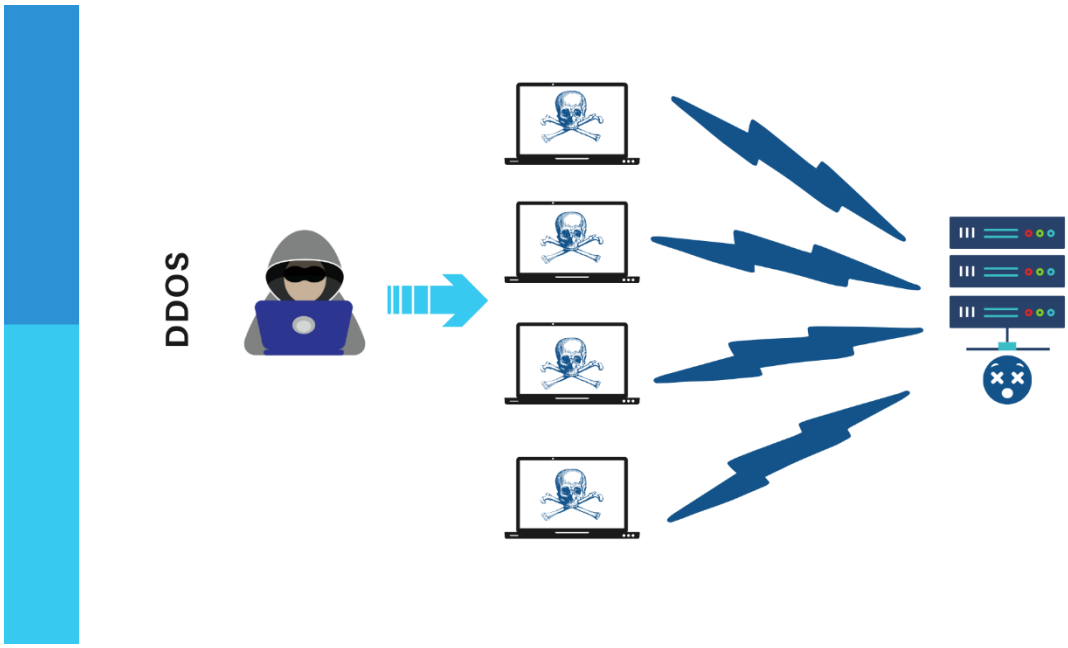
- **Inundaciones volumétricas:** Un atacante inunda la red con tráfico para dejarlo sin respuesta a solicitudes legítimas, todos los dispositivos de la red serán objetivos, el servidor DNS, el servidor web. Las solicitudes provienen de múltiples orígenes y los paquetes no necesitan estar formateados correctamente, lo que hace que cada paquete sea probablemente exitoso.

- **Ataques a nivel de protocolos de red**: El internet está construido sobre un modelo, en dicho modelo cada una de las 7 capas cuenta con protocolos y cada una de estas presenta ciertas vulnerabilidades. TCP y UDP se encuentran en la capa de transporte y son los objetivos principales en un DDoS que tratará de agotar sus capacidades de procesamiento. El ataque es común en el TCP SYN FLOOD en el que se inunda al objetivo de peticiones SYN (Chou & Groves, s/f).

- **Ataques a nivel de aplicación:** Los ataques a nivel de aplicación consisten en agotar la capacidad de una aplicación de responder a las solicitudes legítimas, por ejemplo, a nivel de HTTP enviará miles de solicitudes GET asumiendo que el servidor no contará con los recursos necesarios.

- **Ataques combinados:** Una técnica de DDoS que no es muy común combina ataques a nivel del protocolo y a nivel de aplicación (Gupta & Dahiya, 2021).

**Ilustración 6.** Esquema *DDoS*




**Fuente:** elaboración propia

## 1.4. Mecanismos de ciberseguridad existentes

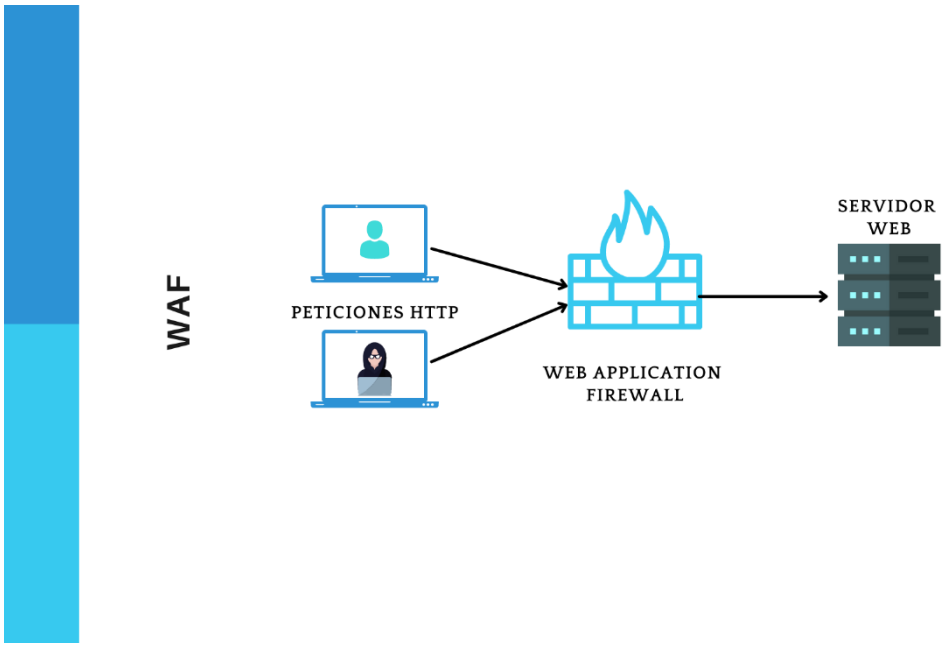
### *Web Application Firewall (WAF)*

Un *Web Application Firewall* (WAF) o *firewall* de aplicaciones web protege sistemas de delincuentes informáticos. El funcionamiento básico de un WAF consiste en un análisis profundo del tráfico HTTP que existe entre un cliente a un servidor web expuesto en internet, esta inspección se basa en un conjunto de reglas denominadas políticas que tienen como objetivo desplegar un ambiente seguro ante posibles ataques.

La protección de un WAF cubre los ataques más comunes mencionados anteriormente (XSS,DDoS, SQLi, etc.) todo esto gracias a que mediante las reglas establecidas separarán el tráfico detectado como riesgoso (Rathore et al., 2022).

En la ilustración 7 se observa una arquitectura simple de un WAF donde esta analiza el tráfico que proviene de las solicitudes de los clientes. Un WAF estará configurado dentro de tres modelos: 1. lista blanca en la cual solo permite el tráfico aprobado y cumple con las reglas definidas; lista negra en la cual solo bloquea las vulnerabilidades más conocidas y 3. un modo híbrido de ambas (datalinknetworks, s/f).

**Ilustración 7.** WAF




**Fuente:** elaboración propia

Un WAF tendrá varios tipos de arquitecturas, sin embargo, está clasificado en tres grupos de acuerdo con su tipo de despliegue;

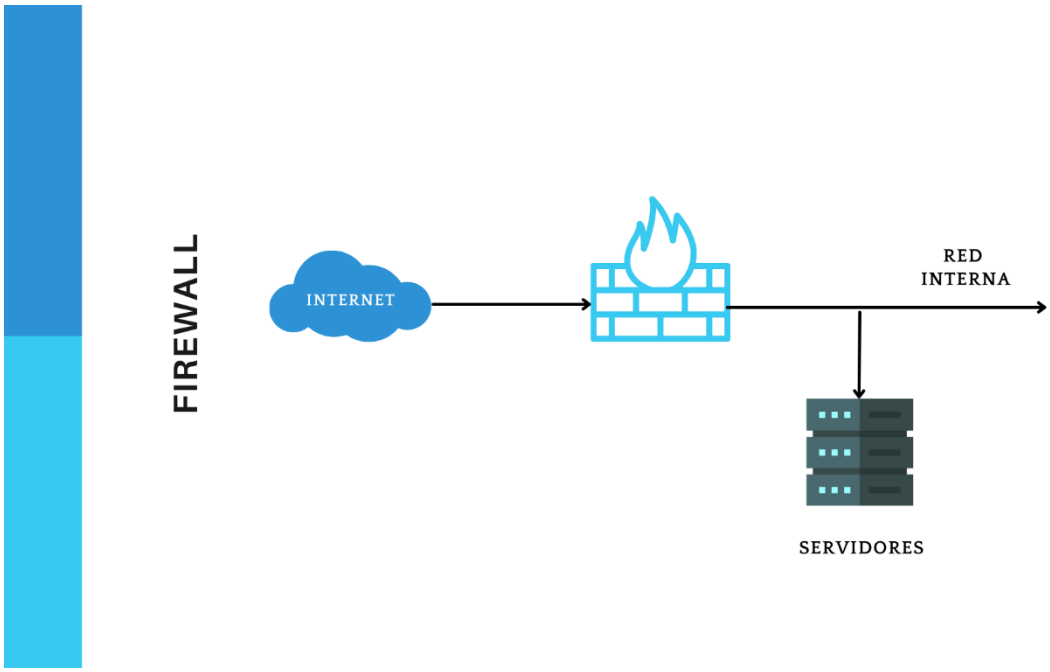
- WAF Basado en *hardware*: consta de un *appliance* físico desplegado dentro de la infraestructura local, su principal ventaja el rendimiento.
- WAF Basado en *software*: este tipo de WAF se encuentra virtualizado *on-premise*, es decir, dentro de la granja de servidores de la organización.

- WAF Basado en *cloud*: son los denominados WAF de nueva generación, estos están en la modalidad *Software as a Service (*SaaS), su principal ventaja es que al estar desplegados en la nube no necesitan instalar nada dentro de la infraestructura (“3 Types of Web Application Firewalls”, 2020).

### *Firewall*

Un *firewall* es un dispositivo de *software* y/o *hardware* orientado al monitoreo de todo el tráfico de red que transita por este. Su principal funcionalidad, aunque no la única, es la de denegar o permitir el tráfico según reglas establecidas, dichos tipos de *firewall* suelen ser llamados *firewall* basados en reglas. Ciertos *firewalls* no funcionan únicamente bajo reglas establecidas, sino que analizan el comportamiento del tráfico entrante y saliente basando esto en firmas o inteligencia artificial (Stewart & Kinsey, 2020). En la ilustración 8 se muestra una arquitectura simple de *firewall.*

**Ilustración 8.** Arquitectura básica con un *Firewall*




**Fuente:** elaboración propia

Depender totalmente de un *firewall* para la seguridad es considerado como una mala práctica, puesto que el *firewall* generalmente no bloquea código malicioso, lo

ideal es tener un *software* de antivirus. También será considerado como un punto crítico de falla, si el aplicativo de seguridad llega a fallar toda la organización se verá expuesta a ataques informáticos por lo que se conjugarán con otros mecanismos de seguridad para una solución integral.

**Tipos de *firewall***

Se categorizan de varios modos. Según el modo de funcionamiento

- *Stateless*, el filtrado de paquetes se realiza analizando un paquete y lo permite o lo niega basándose únicamente en las reglas del *firewall* previamente definidas.
- *Statefull*, el filtrado de paquetes se lo realiza utilizando las reglas del *firewall*, pero también el estado de la conexión, es decir, guarda un historial de conexión de los dispositivos externos que realizan las peticiones y en base a ello y a las reglas deniega o permite el paso de un paquete (Ciampa, 2020).

Por su implementación se clasifican en;

- *Firewalls* por *software*: un *firewall* también suele incluirse dentro de un sistema operativo impidiendo el acceso sin autorización al equipo de cliente final. Su objetivo es monitorear y bloquear el tráfico (Mondesir, 2015).
- *Firewalls* por *hardware*: un *firewall* estará implementando en un *appliance* físico que es un dispositivo de *hardware* instalado dentro de la infraestructura es decir *on-premise* (Crawley, 2015).
- *Cloud firewall*: su funcionamiento suele estar parecido a un *firewall on-premise,* pero toda su infraestructura esa en la nube (Moallem, 2021).

**Soluciones *endpoint***

La protección *endpoint* también denominada seguridad de puntos finales es una solución que una organización implementa para proteger su red haciendo énfasis en los dispositivos de cliente final como teléfonos inteligentes, computadoras, tabletas u otros dispositivos como servidores que se encuentran dentro de la red. El masivo aumento de las tecnologías móviles ha hecho que estos dispositivos sean un vector de ataque y un riesgo para una organización puesto que llegarán a

perderse y comprometer información confidencial, las soluciones *endpoint* no solo son una solución a este problema sino también a posibles amenazas del usuario, este causará incidentes de ciberseguridad intencionalmente o no, también excedería el uso de datos en un dispositivo móvil entre otros. A simple vista un *endpoint* parecerá igual que un antivirus común, sin embargo, su principal diferencia es que el antivirus protege solo un dispositivo específico, mientras que las *endpoint* cubren un panorama más general y protegen varios los aspectos de la red (Moallem, 2021).

**Tecnologías *endpoint***

- Soluciones Antivirus: un antivirus basa su funcionamiento en la detención de y prevención de *malware*, sin embargo, con el crecimiento de las técnicas de ciberataques se ha convertido en una barrera contra *ransomware*, gusanos y otros métodos de amenazas. Un antivirus tiene tres métodos para defenderse de las amenazas:

    - Heurística: no utiliza firmas, en su lugar realiza un análisis del código para detectar comportamiento malicioso.
    - Detección de *sandbox*: a través de un ambiente virtual se prueba una posible amenaza para verificar si es seguro ejecutarlo normalmente.
    - Inteligencia artificial o minería de datos: utiliza una recolección de datos e inteligencia artificial para clasificar comportamientos anormales (Moallem, 2021).

- *Endpoint Detection and Response* (EDR). Una solución EDR brinda funcionalidades que un antivirus común no podría, con las técnicas actuales un atacante puede evadirlo con cierto grado de dificultad. EDR recopila datos continuamente en los clientes finales con el fin de actuar de manera proactiva a un incidente con el aprendizaje basado en la información que almacenó (Bhattacharya, 2020).

- *Secure Email Gateway* (SEG). Es una solución de seguridad para correo electrónico que se encuentra entre el internet y el servidor de correo de la organización con el fin de inspeccionar todo el correo entrante y saliente

antes de que llegue a su destino final (*What Is a Secure Email Gateway (SEG)?*, s/f). Las principales características de un SEG son:

- *Sandboxing*: análisis aislado de los adjuntos y URLs de los correos electrónicos.
- *Data Loss Prevention* (DLP): El correo electrónico suele ser el medio más usado para compartir información, DLP identifica información potencialmente confidencial según las reglas definidas y evita que se trasmita a terceros (*What Is a Secure Email Gateway (SEG)?*, s/f).
- *Anti-Phishing*: El *Phishing* actualmente es una de las amenazas más comunes dentro una organización, este método de ataque intenta extraer información personal como tarjetas de crédito o credenciales. Esta característica bloquea intentos de obtener dicha información mediante correos apartemente confiables (Chakraborty et al., 2020).
- *Post-Delivery Protection*: una amenaza que ha sido pasada por alto durante el análisis del tráfico en curso, sobre todo en ataques de día cero. Esta protección actúa verificando el correo electrónico del usuario dentro de su bandeja de entrada y lanzando una advertencia sobre un posible incidente (*What Is a Secure Email Gateway (SEG)?*, s/f).
- *Domain-Based Message Authentication, Reporting, and Conformance* (DMARC): DMARC es una protección contra el denominado *email spoofing* o suplantación de correo, este mecanismo verifica si el remitente posee esta misma protección a través de otros registros (Wu & Irwin, 2016).

### *Disaster Recovery Plan (DRP)*

Una de las mayores preocupaciones a nivel de disponibilidad de servicios en TI es la recuperación de desastres, un *Disaster Recovery Plan* (DRP) o plan de recuperación de desastres en un procedimiento o conjunto de acciones contra posibles desastres que afectarán a uno o más servicios, atentando así contra la

continuad de un negocio. Las claves dentro del DRP consisten en que no existirá pérdida de información y que los tiempos para restablecer los servicios serán óptimos (Surianarayanan & Chelliah, 2019).

Un sistema de respaldos y de recuperación es clave dentro de una organización que tenga un sistema de información crítico. Un *Service Level Agreement* (SLA) o nivel de acuerdo de nivel de servicio juega un papel importante con el procedimiento de recuperación y respaldos pues brinda un porcentaje en el que un servicio en particular estará fuera de línea (Guise, 2017).

En DRP existen varias terminologías:

- *Critical Business Function* (CBF) o Función Empresarial Crítica es cualquier función, servicio o proceso de valor agregado que la organización considere como vital. Si estas fallan la organización perderá la capacidad de cumplir la misión de esta.
- *Maximum Acceptable Outage* (MAO) o Interrupción Máxima Aceptable es el tiempo máximo que una función, servicio o proceso de valor agregado estará inactivo antes de afectar la misión de la organización, como objetivo de un DRP estará que un sistema será recuperable antes de que se iguale el MAO.
- *Business Impact Analysis* (BIA) o Análisis de impacto al Negocio es un estudio de las consecuencias e impacto que tendría una organización en el caso que los servicios de tecnologías de la información fallen.
- *Business Continuity Plan* (BCP) o Plan de Continuidad de negocio es un conjunto de estrategias que ayudan a una organización a protegerse de emergencias con el fin de garantizar las funciones criticas incluso después de una falla o desastre (Gibson & Igonor, 2020).

Un modelo de DRP para cualquier empresa tendrá al menos:

- Tolerancia a fallas.
- Redundancia o sitios alternos.
- Manual de procedimientos.
- Recuperabilidad con respaldos fuera de sitio.

## Respaldos

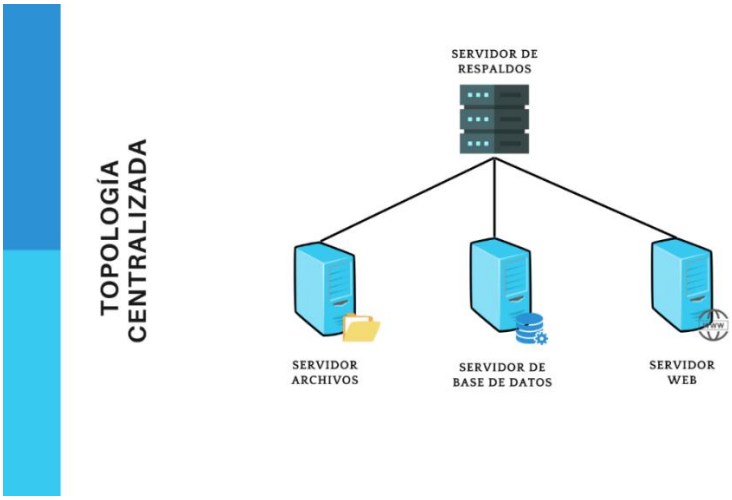
Se definirá a un respaldo o *backup* como una copia de seguridad completa o parcial de un sistema de información, base de datos, sistema operativo, configuraciones o datos críticos. Los respaldos suelen realizarse fuera del anfitrión que alberga el tipo de activo, sin embargo, también suelen ser locales. La importancia de un respaldo radica en que la posibilidad que información valiosa pueda ser eliminada o modificada seria devastador para una organización. Existen varias amenazas que pueden atentar contra la información como acceso no autorizado, sistemas vulnerables o desastres ambientales (Fox, 2013).

La topología dentro de un sistema de *backups* es una parte integral del mismo, este se ajustará al presupuesto de la organización y a la estructura del sistema de información, por lo general se clasifican en dos tipos:

### Sistema de respaldos centralizado

Un sistema de respaldos centralizado consta de un solo servidor de respaldos como se muestra en la ilustración 9. Todos los activos de información tales como servidor de archivos o base de datos respaldan sus archivos dentro de dicho servidor, esto trae consigo varias ventajas pues requiere menos recursos de infraestructura y de configuración. También se pueden realizar mediante varias tecnologías de comunicación como TCP/IP fibra o conexiones directas siendo una de las claves el hecho de que la transmisión de los metadatos este separado lógicamente del tráfico de respaldos/recuperación (Guise, 2017).

**Ilustración 9.** Topología de respaldos centralizada




**Fuente:** elaboración propia

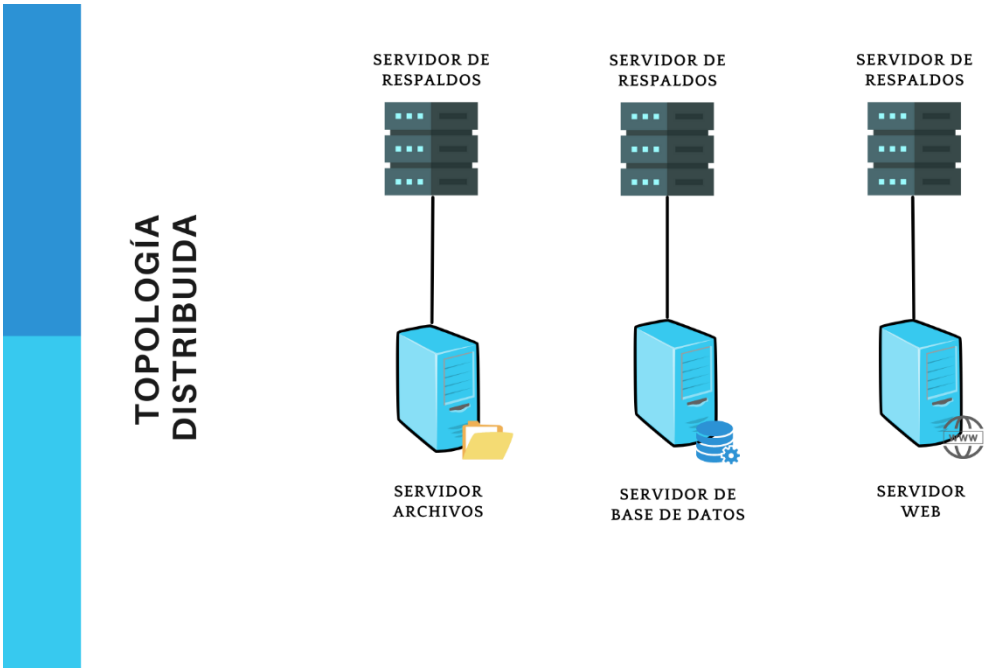
## Sistema de respaldos distribuido.

Una topología distribuida para sistemas de respaldos se caracteriza porque cada servicio dentro de la infraestructura tiene un servidor de respaldo. La arquitectura común se muestra en la ilustración 10.

Generalmente para este tipo de arquitectura se utilizan soluciones comerciales, estás se encargan de realizar el respaldo en su servidor asignado y de toda la administración consecuente. Generalmente este tipo de topologías son usadas por empresas medianas o pequeñas, sin embargo, sus desventajas suelen ser mayores a las ventajas que ofrecerían, entre algunas se mencionan:

- Costo elevado
- Almacenamiento ineficiente
- Configuración compleja (Guise, 2017)

**Ilustración 10:** Topología de respaldos distribuido




**Fuente:** elaboración propia

# CAPITULO II. DISEÑO METODOLÓGICO

## 2.1. Metodología de investigación

Se utiliza una metodología mixta. La primera es cuasiexperimental, se implementará un escenario simulado con características similares al ambiente real para realizar el análisis de vulnerabilidades, además, para el desarrollo de controles se utiliza una metodología basada en el ciclo de *Deming* o *Plan, Do, Check, Act* (PDCA) o en español: Planificar, Hacer, Revisar y Actuar (PDCA). También es utilizada para la implantación del EGSI, dicha metodología funciona en 4 fases:

### Planificación

Como parte de la planificación se realiza una investigación del estado del arte actual y mecanismos similares implementados en sistemas de información web expuestos en internet y a nivel de infraestructura.

En esta fase se definen los objetivos del proyecto a nivel de ciberseguridad, el alcance del proyecto y levantamiento de información preliminar. Un aspecto importante es el de definir el contexto de la organización gubernamental y del sistema en catastral, un diagnóstico de la inicial de situación del sistema y un levantamiento de los activos de información involucrados dentro de este. Un análisis de riesgos es clave con el fin tratarlos e implementar mecanismos y controles de ciberseguridad, para este proyecto se hizo uso de la metodología CIS RAM debido a que es la que más se ajusta al objetivo del proyecto. Además de lo anteriormente definido, se realizará un análisis de vulnerabilidades de los activos informáticos involucrados, con el fin de tener un diagnóstico de la situación actual a nivel de infraestructura de TI.

Con la información anteriormente obtenida se planifica una estructura de cumplimiento, los mecanismos a aplicar, la arquitectura a implementar y los tiempos a cumplir para tener un prototipo de ciberseguridad aplicable al sistema.

### Hacer

Este paso tiene como objetivo ejecutar lo planificado, implementar los controles de seguridad y el tratamiento de los riesgos.

### Verificar

Realizar una auditoría de los controles aplicados, realizar unas pruebas de penetración y también verificar el cumplimiento de las políticas definidas con el fin de evaluar la efectividad del prototipo.

### Actuar

Realizar actividades correctivas de los incidentes que se dieron dentro del ciclo de desarrollo de esta implementación. También mejorar en todos los aspectos el prototipo de esquema de ciberseguridad.

**Ilustración 11.** Ciclo *Deming*


**Fuente:** elaboración propia

## 2.2. Aproximación a la solución

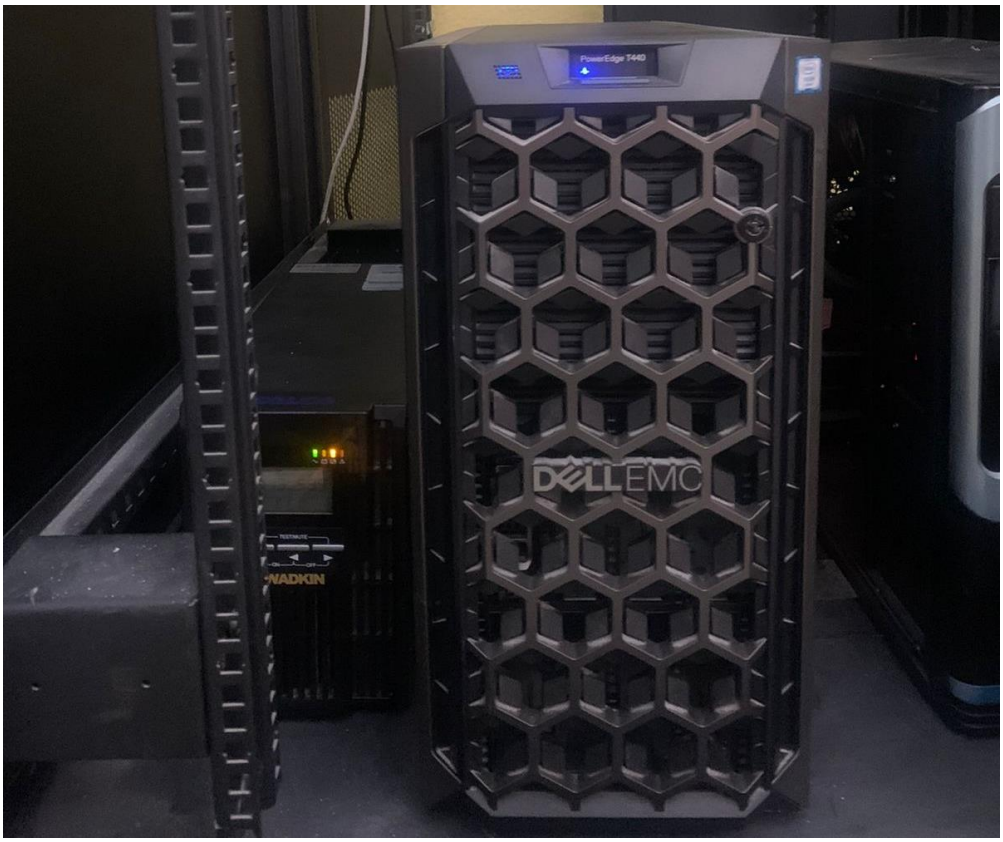
Este trabajo pretende determinar un modelo de ciberseguridad para el sistema catastral del GAD de Mera, con el fin de tener una visión completa, se realizará un diagnóstico en varios ámbitos relacionados con el sistema, esto es un factor clave para el éxito de la determinación de los mecanismos a usar.

### Diagnóstico de situación actual

### Diagnóstico físico

El cuarto donde se encuentra almacenado el servidor tiene libre acceso por lo que representa un riesgo, de igual manera el servidor no está en el *rack* con los demás servidores puesto que es de torre y es exclusivo para el sistema catastral tal y como se observa en la ilustración 12.

**Ilustración 12.** Server DELL del sistema ANZU



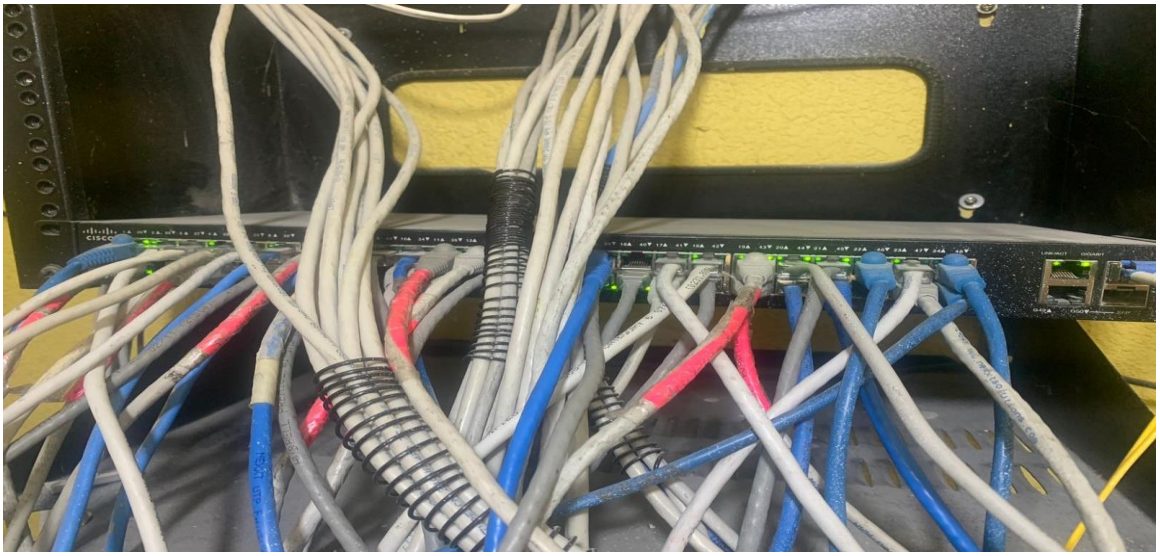

**Fuente:** elaboración propia

En el cuarto de servidores también están un servidor físico en el *rack* principal, se visualiza que la administración de cables es deficiente puesto que los cables no están certificados y son de diferente categoría. En la ilustración 13 y 14 muestra los activos del *rack.*

**Ilustración 13.** Servidores *RackeadoS*

**Fuente:** elaboración propia

**Ilustración 14.** Cableado estructurado



**Fuente:** elaboración propia

El cuarto de servidores con un UPS APC provee 1000VA (Voltios-Amperios), pero según la potencia del servidor (600W) tiene una duración de 6 minutos, un tiempo que no es suficiente en el caso de un corte de energía.

**Ilustración 15.** UPS del cuarto de servidores


**Fuente:** elaboración propia

En el análisis visual se observa que los principales riesgos son la disponibilidad y la confidencialidad. La disponibilidad porque no existe un enlace de respaldo en caso de caída del proveedor principal, como se observa en la ilustración 16, además que el UPS no provee la duración necesaria en caso de un corte de energía y que el cableado estructurado no tiene una administración correcta y también lo es que sea heterogéneo, pues usa cables de diferente categoría, en los tres casos afectan a la disponibilidad de los servicios del sistema catastral.

Para el caso de la confidencialidad e integridad no existe un control de acceso adecuado, permite insertar medios de almacenamiento removibles en los servidores.

**Ilustración 16.** Router del proveedor de servicios.


**Fuente:** elaboración propia

A nivel de ciberseguridad empresarial y sin importar el estándar, uno de los controles que siempre son obligatorios es el inventario de activos de información. Este inventario sirve para realizar el análisis de riesgos y será actualizado a periodos regulares. En la tabla número 1 se muestra el detalle los activos de información, estos incluyen: *software, hardware*, personal y datos.

## Levantamiento de activos de información

A nivel de ciberseguridad empresarial y sin importar el estándar, uno de los controles que siempre son obligatorios es el inventario de activos de información. Este inventario sirve para realizar el análisis de riesgos y será actualizado a periodos regulares. En la tabla número 1 se muestra el detalle los activos de información, estos incluyen: *software, hardware*, personal y datos.

**Tabla 1.** Activos de información de infraestructura y aplicaciones

| ACTIVOS DE INFORMACIÓN | | | | | | | |
|---|---|---|---|---|---|---|---|
| **No** | **Proceso Macro** | **Aplicativo** | **Subproceso** | **Tipo de Activo** | **Nombre de Activo** | **Descripción del Activo** | **Ubicación** |
| A1 | Gestión de tecnologías de la información e infraestructura | Sistema Catastral | Infraestructura | *Hardware* | SERVIDOR TORRE *POWEREDGE DELL* 9R6LPX2 | Servidor físico en el cual se aloja el sistema catastral. | *Datacenter* ubicado en la planta baja |
| A2 | | | Infraestructura | *Hardware* | UPS *WADKIN* 1KVA TORRE | Procesamiento del tráfico de red para acceso de los clientes finales. | *Datacenter* ubicado en la planta baja |
| A3 | | | Aplicaciones informáticas | *Software* | *ARCGIS ENTERPRISE WORKGROUP STANDARD UP TO TWO CORES LICENSE* | *Software* licenciado para el sistema de información geográfica | *Datacenter* ubicado en la planta baja |
| A4 | | | Aplicaciones informáticas | *Software* | *ARCGIS FOR DESKTOP ESTANDAR SINGLE LICEN* | *Software* licenciado para el sistema de información geográfica. | *Datacenter* ubicado en la planta baja |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A5 | | | Aplicaciones informáticas | *Software* | *LICENCIA WINDOWS SERVER STD 2016 OEM 64 BIT* | *Software* licenciado el sistema operativo del servidor. | *Datacenter* ubicado en la planta baja |
| A6 | | | Aplicaciones informáticas | *Software* | *SQL SERVER 2016 SERVICE PACK 2 OEM - ESQUEMAS* | Software licenciado la base de datos denominada GEOMERA. | *Datacenter* ubicado en la planta baja |
| A7 | | | Aplicaciones informáticas | *Software* | *INTERNET INFORMATION SERVICES* (*IIS*) – APLICATIVO EN .NET | Servidor web en el corre el aplicativo en .NET | *Datacenter* ubicado en la planta baja |

**Fuente:** elaboración propia

**Tabla 2.** Activos de información de personal

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A8 | | | Redes y comunicaciones | Redes | *SWITCH DE ACCESO CISCO WS-C2960X-24TD-L* | Procesamiento del tráfico de red para acceso de los clientes finales. | Datacenter ubicado en la planta baja |
| A9 | | | Redes y comunicaciones | Redes | *ROUTER TP LINK DIR-819* | Enrutamiento entre el dispositivo de borde provisto por el proveedor | *Datacenter* ubicado en la planta baja |
| A10 | | | Redes y comunicaciones | Redes | CABLEADO E UTP CATEGORIA 6 | Conexión entre equipos de red | Toda la Institución |
| A11 | | | Personal involucrado | Personal | CHRISTIAN A. | Usuario del sistema | Oficina TI |
| A12 | | | Personal involucrado | Personal | ALEXIS A. | Usuario del sistema | Oficina de Gerencia |
| A13 | | | Personal involucrado | Personal | ANA BELEN A. | Usuario del sistema | Oficina de Gerencia |
| A14 | | | Personal involucrado | Personal | ANGEL C. | Usuario del sistema | Oficina de Gerencia |
| A15 | | | Personal involucrado | Personal | USUARIO CONSULTA | Usuario del sistema | Oficina de Gerencia |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A16 | | | Personal involucrado | Personal | DANIELA B. | Usuario del sistema | Oficina de Gerencia |
| A17 | | | Personal involucrado | Personal | DIANA L. | Usuario del sistema | Oficina de Gerencia |
| A18 | | | Personal involucrado | Personal | DANIEL M. | Usuario del sistema | Oficina de Gerencia |
| A19 | | | Personal involucrado | Personal | DANIEL N. | Usuario del sistema | Oficina de Gerencia |
| A20 | | | Personal involucrado | Personal | DAVID O. | Usuario del sistema | Oficina de Gerencia |
| A21 | | | Personal involucrado | Personal | ESTEFANÍA C. | Usuario del sistema | Oficina de Gerencia |
| A22 | | | Personal involucrado | Personal | ERICKA L. | Usuario del sistema | Oficina de Gerencia |
| A23 | | | Personal involucrado | Personal | ELCIRA L. | Usuario del sistema | Oficina de Gerencia |
| A24 | | | Personal involucrado | Personal | FREDDY S. | Usuario del sistema | Oficina de Gerencia |
| A25 | | | Personal involucrado | Personal | GUIDMON T. | Usuario del sistema | Oficina de Gerencia |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A26 | | | Personal involucrado | Personal | ISMAEL F. | Usuario del sistema | Oficina de Gerencia |
| A27 | | | Personal involucrado | Personal | ISRAEL M. | Usuario del sistema | Oficina de Gerencia |
| A28 | | | Personal involucrado | Personal | JACQUELINE C. | Usuario del sistema | Oficina de Gerencia |
| A29 | | | Personal involucrado | Personal | JORDY M. | Usuario del sistema | Oficina de Gerencia |
| A30 | | | Personal involucrado | Personal | JOANA M. | Usuario del sistema | Oficina de Gerencia |
| A31 | | | Personal involucrado | Personal | JESSY N. | Usuario del sistema | Oficina de Gerencia |
| A32 | | | Personal involucrado | Personal | JOSUE V. | Usuario del sistema | Oficina de Gerencia |
| A33 | | | Personal involucrado | Personal | JOHANA Z. | Usuario del sistema | Oficina de Gerencia |
| A34 | | | Personal involucrado | Personal | LIZETH F. | Usuario del sistema | Oficina de Gerencia |
| A35 | | | Personal involucrado | Personal | LIGIA N. | Usuario del sistema | Oficina de Gerencia |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A36 | | | Personal involucrado | Personal | LUIS R. | Usuario del sistema | Oficina de Gerencia |
| A37 | | | Personal involucrado | Personal | MARCO T. | Usuario del sistema | Oficina de Gerencia |
| A38 | | | Personal involucrado | Personal | MAYRA V. | Usuario del sistema | Oficina de Gerencia |
| A39 | | | Personal involucrado | Personal | MAYRA V. | Usuario del sistema | Oficina de Gerencia |
| A40 | | | Personal involucrado | Personal | NUNKUI A. | Usuario del sistema | Oficina de Gerencia |
| A41 | | | Personal involucrado | Personal | OLGA M. | Usuario del sistema | Oficina Registro de la propiedad |
| A42 | | | Personal involucrado | Personal | PABLO C. | Usuario del sistema | Oficina de Gerencia |
| A43 | | | Personal involucrado | Personal | ROGER E. | Usuario del sistema | Oficina TI |
| A44 | | | Personal involucrado | Personal | RICARDA L. | Usuario del sistema | Oficina de Gerencia |
| A45 | | | Personal involucrado | Personal | SEGUNDO V. | Usuario del sistema | Oficina de Gerencia |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A46 | | | Personal involucrado | Personal | SASKIA P. | Usuario del sistema | Oficina de Gerencia |
| A47 | | | Personal involucrado | Personal | YADIRA R. | Usuario del sistema | Oficina de Gerencia |

**Fuente:** elaboración propia

## Análisis de riesgos

## Criterios de evaluación

La metodología elegida para el análisis de riegos es CIS RAM en su versión 2.1, en su guía detalla que el primer paso es elegir los criterios de evaluación de riesgos y en la tabla 2 se muestra los criterios según el impacto.

**Tabla 3.** Criterio de impacto

| **Impacto** | **Misión** | **Objetivos operacionales del sistema catastral** | **Objetivos financieros** | **Obligaciones con terceros** |
|---|---|---|---|---|
| Definición | "El Gobierno Autónomo Descentralizado Municipal del Cantón Mera es un modelo de gestión institucional con una estructura orgánica consolidada y eficiente, equipamiento moderno y principios de calidad en la gestión del desarrollo. Fortalece una cultura institucional para la formación integral, fomentando la capacidad intelectual y creatividad de sus clientes internos y externos. Robustece la información y comunicación, democratizando su gestión a través de las instancias de participación ciudadana establecidas, en interrelación con el Comité de Gestión de Desarrollo Institucional." | Automatizar el proceso inventariar, calificar y valorar los bienes con el fin de mejorar la atención a los habitantes del cantón Mera. | | Cumplir con Ley Orgánica de Protección de Datos Personales y no afectar al ciudadano en general. |
| Imperceptible | Se lograría cumplir la misión del Gobierno Autónomo | Se cumple el objetivo | | No se incumple con la ley de |

| | | | | |
|---|---|---|---|---|
| | Descentralizado Municipal del Cantón Mera | operacional del sistema catastral. | | datos personales ni se afecta al ciudadano. |
| Aceptable | La misión del Gobierno Autónomo Descentralizado Municipal del Cantón Mera no se cumpliría al 100%, pero las operaciones serán restablecidas con ciertos ajustes. | El objetivo operacional del sistema catastral no se cumpliría al 100%, pero estaría dentro de lo aceptable. | | Cualquier incumplimiento que pudiera resultar no requeriría corrección, reparación o compensación para que las partes perjudicadas. |
| No aceptable | Se tendría que reorganizar procesos para cumplir con la misión del Gobierno Autónomo Descentralizado Municipal del Cantón Mera | Se tendría que reorganizar procesos para cumplir el objetivo operacional del sistema catastral. | | Se incumple parcialmente con la ley de datos personales, pero no se afecta al ciudadano. |
| Alto | La misión del Gobierno Autónomo Descentralizado Municipal del Cantón Mera no se lograría. Si no se realizan esfuerzos, recursos o inversiones significativas y no planificadas, es posible que nunca se pueda lograr la misión. | El objetivo operacional del sistema catastral no se cumpliría, y se tiene que realizar cambios significativos. | | Puede ocurrir un daño corregible a hacia la ley de datos personales, o un daño que puede corregirse parcialmente para los ciudadanos. |
| Catastrófico | El Gobierno Autónomo Descentralizado Municipal del | No se es capaz de cumplir el | | Se incumple totalmente con la ley de datos |

| | | | | |
|---|---|---|---|---|
| | Cantón Mera no sería capaz de cumplir la misión | objetivo operacional del sistema catastral. | | personales y se afecta al ciudadano. |

**Fuente:** elaboración propia

El nivel de ocurrencia o de expectativa en un evento se detalla en la tabla 3.

**Tabla 4:** Niveles de ocurrencia

| **Valor cuantitativo** | **Ocurrencia** | **Criterio** |
|---|---|---|
| 1 | Remoto | Un mecanismo de ciberseguridad evitaría de forma fiable la amenaza. |
| 2 | Improbable | Un mecanismo de ciberseguridad evitaría de manera confiable la mayoría de las ocurrencias de la amenaza. |
| 3 | Poco Probable | Un mecanismo de ciberseguridad evitaría tantas amenazas como pasaría por alto. |
| 4 | Muy Probable | Un mecanismo de ciberseguridad evitaría algunos casos de amenazas. |
| 5 | Definitivo | Un mecanismo de ciberseguridad no evitaría nunca ese tipo de amenazas. |

Fuente: elaboración propia

Un valor de riesgo aceptable se calcula con la formula:

$$\text{Riesgo aceptable} = \text{ocurrencia} * \text{impacto}$$

La tabla 4 define de manera cuantitativa cuando un riesgo no es aceptable.

**Tabla 5:** Valores aceptables para riesgos

| **Ocurrencia** | **Impacto** |
|---|---|
| 3 | 3 |
| Un riesgo es aceptable si es menor a: | 9 |

**Fuente:** elaboración propia

Para clasificar los activos y el impacto que tendrían se definen los siguientes parámetros detallados en la tabla 5.

**Tabla 6.** Parámetros de impacto

| **Tipo de activo** | **Impacto en la misión** | **Impacto en el objetivo operacional del sistema catastral** | **Impacto obligaciones con terceros** |
|---|---|---|---|
| Empresariales | 2 | 2 | 2 |
| Dispositivos | 2 | 2 | 1 |
| Aplicaciones | 2 | 2 | 1 |
| Datos | 3 | 2 | 3 |
| Redes | 2 | 2 | 1 |
| Usuarios | 2 | 2 | 3 |

**Fuente:** elaboración propia

Los riesgos catalogados como no aceptables son los que cuantitativamente son mayores o iguales a 9, asumiendo que el nivel de madurez del control del riesgo es 1, este valor es un cuantitativo del nivel de aplicación de un control para un riesgo que va desde el 1 al 5, es decir que no se ha implementado ninguna acción, en la tabla 6 se muestran un resumen de los riesgos que no son aceptables adicional al análisis que se ha hecho, dicha tabla incluye el valor del riesgo y el código de activo en referencia a la tabla 1 que es el listado de activos.

**Tabla 7.** Riesgos no aceptables

| **Descripción del riesgo** | **Valor** | **Activo** | **Valor riesgo** |
|---|---|---|---|
| No se cuentan con copias de seguridad automatizadas periódicas. | 15 | A7 | 9 |
| No se realizan copias de seguridad completas del sistema. | 12 | A1 | 9 |
| No un inventario de información confidencial | 12 | Todo el personal | 9 |
| No elimina los datos confidenciales o sistemas a los que la organización no accede regularmente. | 12 | Todo el personal | 9 |
| Se permiten dispositivos USB. | 15 | A1 | 9 |
| No cuentan con autenticación multifactor. | 12 | A7 | 9 |

| | | | |
|---|---|---|---|
| No limita el acceso a las herramientas de *script* en el servidor. | 15 | A1 | 9 |
| No controla o monitorea cuentas asociadas con pruebas de penetración. | 15 | A7 | 9 |
| No usa herramientas de análisis de vulnerabilidades y pruebas de penetración. | 15 | A7 | 9 |
| No se implementa *firewalls* de aplicaciones web (WAF). | 15 | A7 | 9 |
| El personal no cuenta capacitación acerca de: manejo de datos confidenciales, sobre las causas de la exposición no intencional de datos, notificación de incidentes de ciberseguridad, ingeniería social y autenticación segura. | 12 | Personal | 9 |
| No tiene un plan de contingencia, como un enlace secundario o un servidor para alta disponibilidad. | 12 | A1<br>A8<br>A9 | 9 |
| Los equipos de red no cuentan con un respaldo de sus configuraciones. | 12 | A1<br>A8<br>A9 | 9 |
| No se cuenta con un equipo de seguridad perimetral ni con *endpoint.* | 12 | A1<br>A8<br>A9 | 9 |

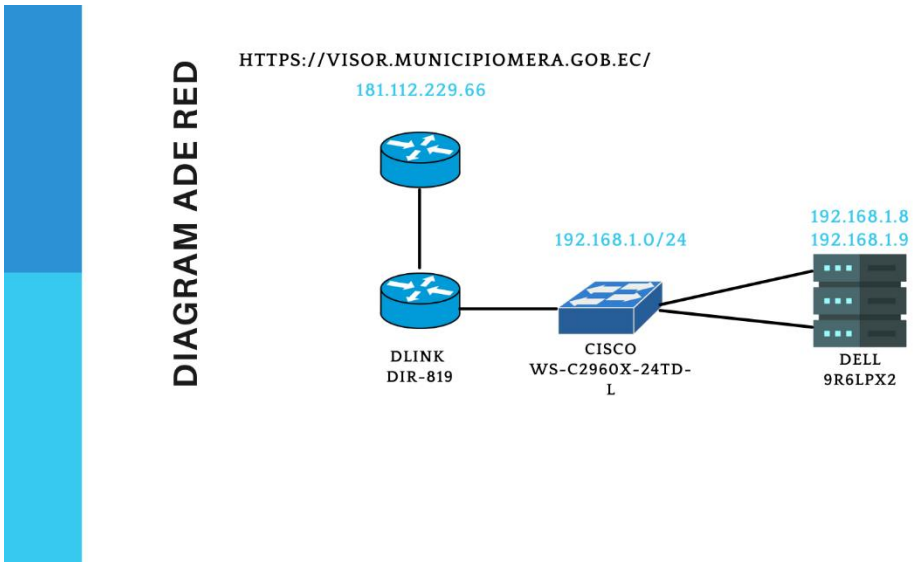
Fuente: elaboración propia

## Análisis de vulnerabilidades

### Vulnerabilidades web

En la ilustración 17 está el esquema actual de la red, con su respectiva IP pública y su dominio. Tenemos el servidor DELL con IP privada 192.168.1.9, un switch marca CISCO para conectar a los clientes finales, un *router* intermedio marca DLINK y el dispositivo de borde del proveedor.

**Ilustración 17.** Diagrama de red

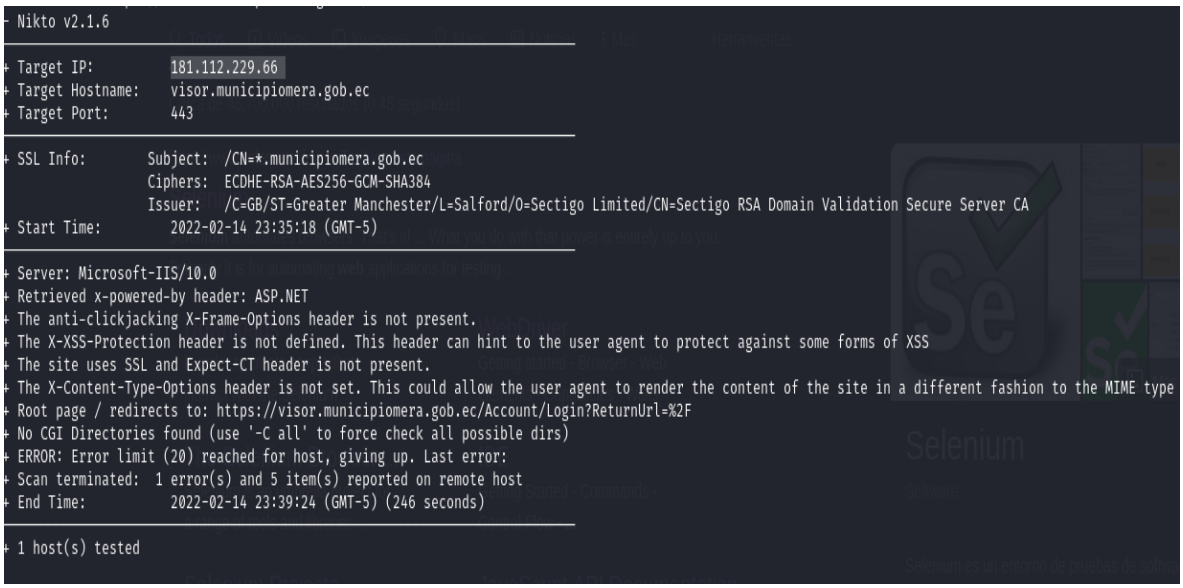



**Fuente:** elaboración propia

Realizar un análisis en busca de vulnerabilidad tanto en el sistema como en su infraestructura relacionada es tan importante como realizar un análisis de riesgos con el fin de tener un conocimiento total de la situación actual del sistema de información. Existe una variedad de aspectos a analizar: seguridad en infraestructura de red, seguridad en sistemas operativos, seguridad a nivel de aplicación, etc. El primer paso es buscar vulnerabilidades a nivel de aplicación web y para esto existen herramientas automatizadas, sin embargo, también se realizarán pruebas manuales con el fin de cubrir de mejor manera todas las posibilidades. *Nikto* es una herramienta de búsqueda de vulnerabilidades a nivel web, esta permite buscar de manera automatizada vulnerabilidad sin importar su lenguaje o *framework* de desarrollo.

En la ilustración 18 un primer escaneo a través de la IP pública ofrece ciertos detalles del servicio.

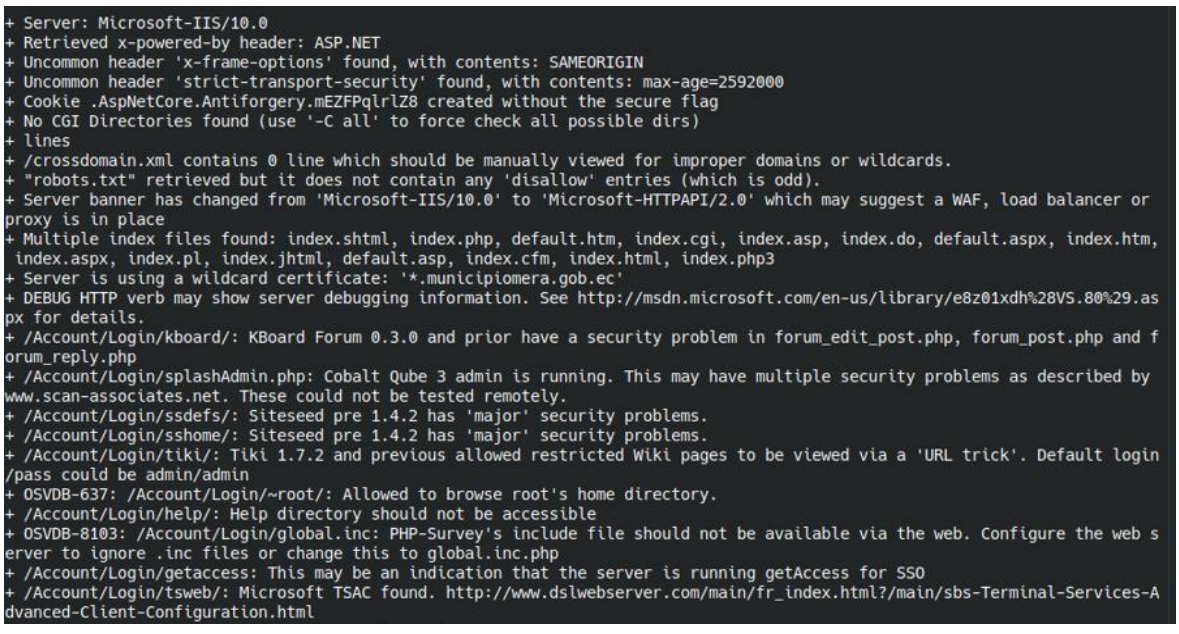
**Ilustración 18.** Escaneo con Nikto




**Fuente:** elaboración propia

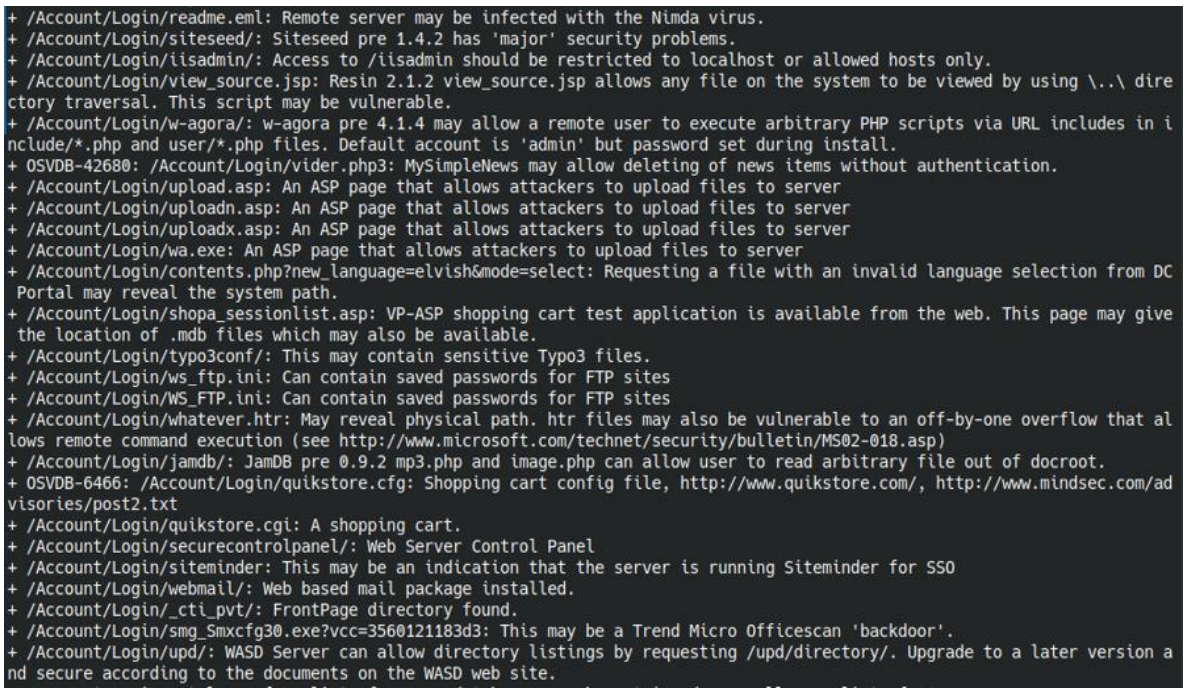
El escaneo automatizado arroja un primer vistazo y muestra que existen múltiples vulnerabilidades a nivel de aplicación web, en las ilustraciones 19 y 20 se observa el resultado.

**Ilustración 19:** Vulnerabilidades encontradas por Nikto




**Fuente:** elaboración propia

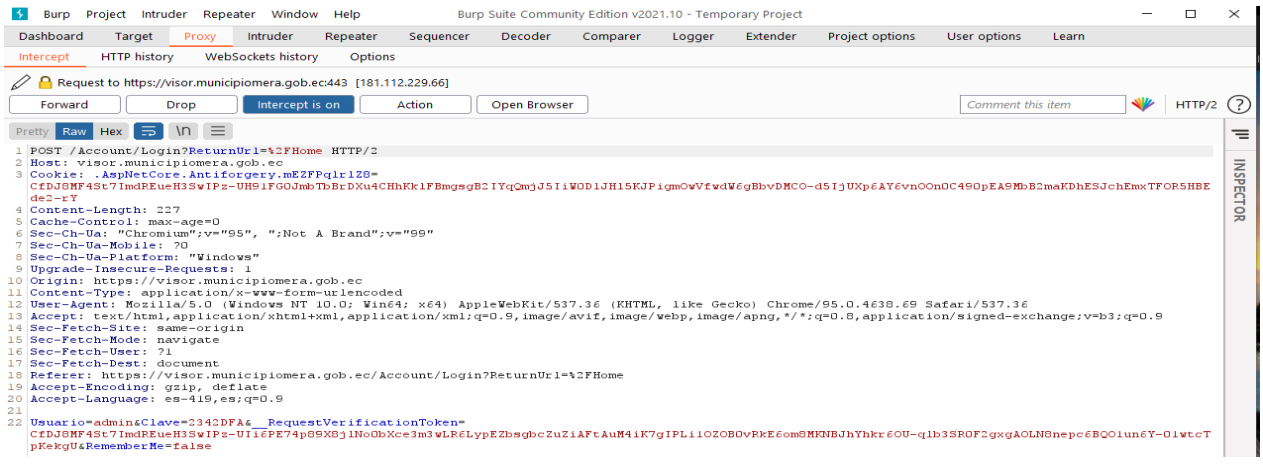
**Ilustración 20.** Vulnerabilidades encontradas por Nikto




**Fuente:** elaboración propia

La herramienta *Burp Suite* es sumamente útil para pruebas de penetración a sistemas web, para este caso de estudio, se realizan pruebas para conocer si además de los resultados que arrojaron las pruebas automáticas nos muestra otras vulnerabilidades como fuerza bruta o criptografía deficiente. En la ilustración 21 se muestra un análisis simple con *Burp Suite*.

**Ilustración 21.** Análisis de vulnerabilidades con *Burp Suite*



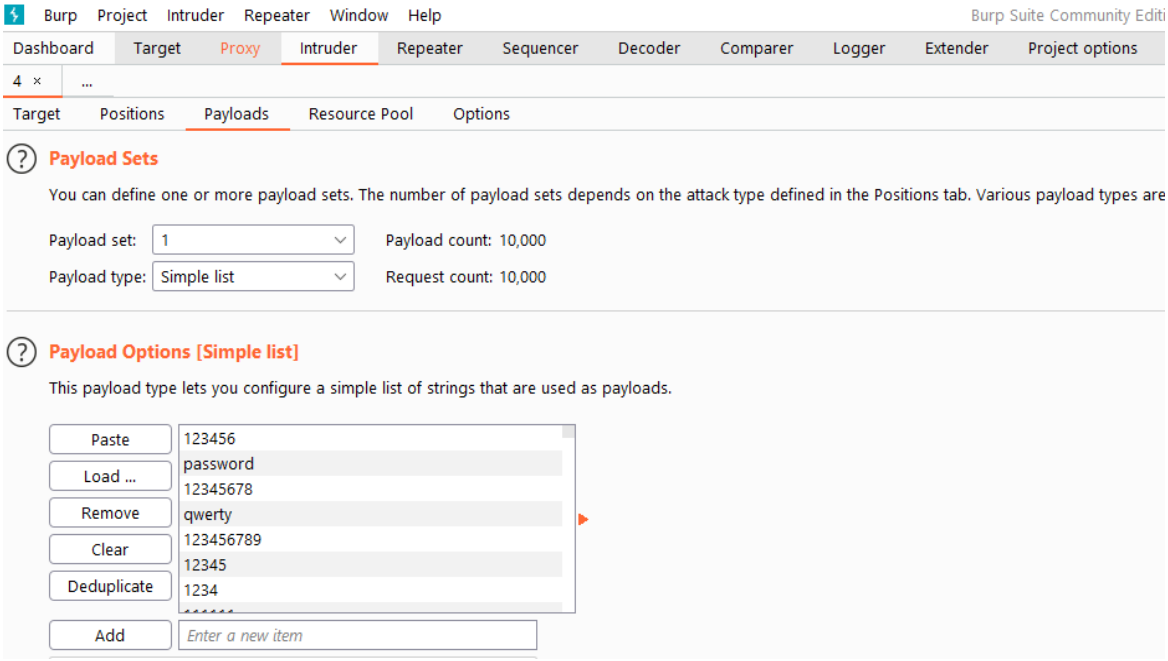

**Fuente:** elaboración propia

El repositorio de github (*MIESSLER*, 2012/2022) nos provee varios listados con claves conocidas y comumnete usadas en sistemas. La opcion *intruderdel Burp*

*suite* nos permite repetir peticiones al servidor agregando *payloads* dentro de estas, la figura 22 muestra cómo se inserta el listado de 10000 contraseñas dentro de la peticion al *login* con usuarios como; admin, administradorm, anzu y mera.

En las ilustración 22 se observa que a pesar de la supuesta seguridad de las contraseñas robustas, el sistema no tiene mecanismos para limitar el número de intentos.

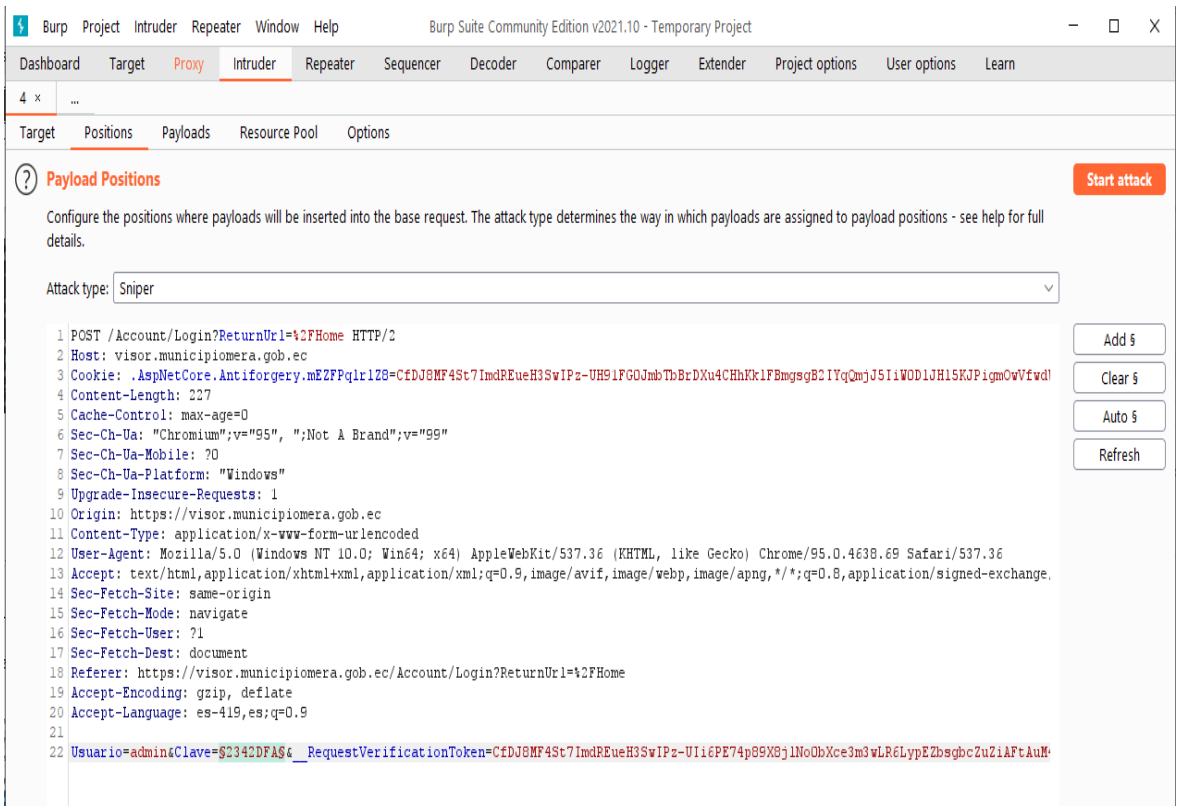
**Ilustración 22.** Ataque de fuerza bruta al *login*




**Fuente:** elaboración propia

La utilidad *intruder* de *Burp Suite* permite repetir las solicitudes al servidor, para esta prueba se realiza un intento *login* para atrapar la petición y poder enviarla al *intruder.* Con la petición se envían los *payloads* anteriormente cargados en modo de lista tal y como lo muestra la ilustración 23.

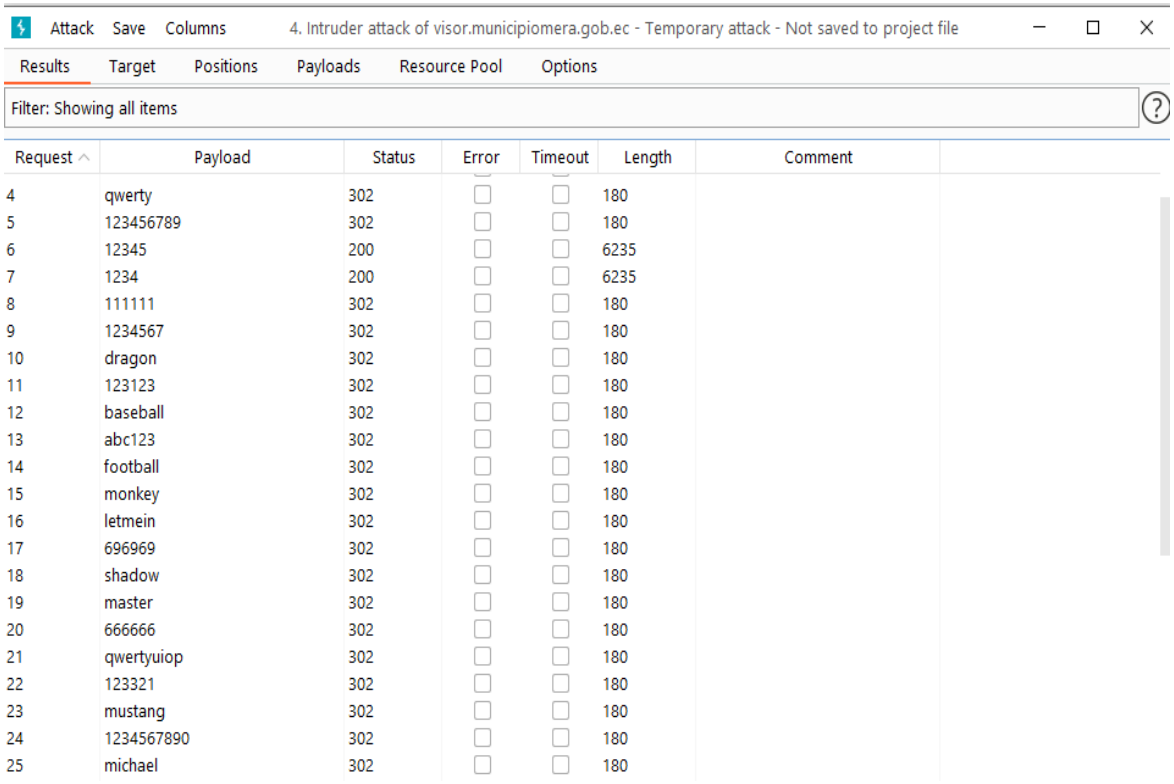
**Ilustración 23.** Inserción de *payloads*




Fuente: elaboración propia

Un ataque de fuerza bruta o de diccionario consisten en probar varias claves para tratar de encontrar una combinación con el fin de vulnerar, la autenticación con *Burp* permite realizar este tipo de pruebas como se muestra en la figura 24 la respuesta tiene un valor de 200 lo que a nivel de HTTP *response* significa una respuesta exitosa. Sin embargo, la respuesta dice que la complejidad del *password* es insuficiente para los parámetros del sistema, lo que es erróneo puesto que ese tipo de error aparece solo al registrar un nuevo usuario tal y como lo muestra la ilustración 24.

**Ilustración 24.** Burp Suite con 10000 contraseñas




| Request | Payload | Status | Error | Timeout | Length | Comment |
|---|---|---|---|---|---|---|
| 4 | qwerty | 302 | | | 180 | |
| 5 | 123456789 | 302 | | | 180 | |
| 6 | 12345 | 200 | | | 6235 | |
| 7 | 1234 | 200 | | | 6235 | |
| 8 | 111111 | 302 | | | 180 | |
| 9 | 1234567 | 302 | | | 180 | |
| 10 | dragon | 302 | | | 180 | |
| 11 | 123123 | 302 | | | 180 | |
| 12 | baseball | 302 | | | 180 | |
| 13 | abc123 | 302 | | | 180 | |
| 14 | football | 302 | | | 180 | |
| 15 | monkey | 302 | | | 180 | |
| 16 | letmein | 302 | | | 180 | |
| 17 | 696969 | 302 | | | 180 | |
| 18 | shadow | 302 | | | 180 | |
| 19 | master | 302 | | | 180 | |
| 20 | 666666 | 302 | | | 180 | |
| 21 | qwertyuiop | 302 | | | 180 | |
| 22 | 123321 | 302 | | | 180 | |
| 23 | mustang | 302 | | | 180 | |
| 24 | 1234567890 | 302 | | | 180 | |
| 25 | michael | 302 | | | 180 | |

**Fuente:** elaboración propia

Un mecanismo usado para resguardar la confidencialidad es *Secure Sockets Layer* (SSL). Esto con el fin de que el tráfico punto a punto esté encriptado y sea ilegible para atacantes. El sistema web cuenta con su respectivo certificado SSL, este es de tipo *wildcard* y emitido por la entidad certificadora *Sectigo* y utiliza algoritmos como SHA-256 con RSA para el certificado y la llave pública con RSA 2048 tal y como lo muestra la ilustración 25.

**Ilustración 25.** Certificado SSL


**Fuente:** elaboración propia

### Vulnerabilidades de infraestructura de red

NMAP es una herramienta de escaneo con múltiples utilidades, principalmente el de escanear puertos y servicios abiertos. En la ilustración 26 se visualiza la ejecucion del comando “nmap -Pn -sC 181.112.229.66  -f –open”. Este comando se ejecuta a la IP pública para verficiar que puertos están expuestos en internet. Si un puerto esta abierto sin una utilidad aparente es una vulnerabilidad.

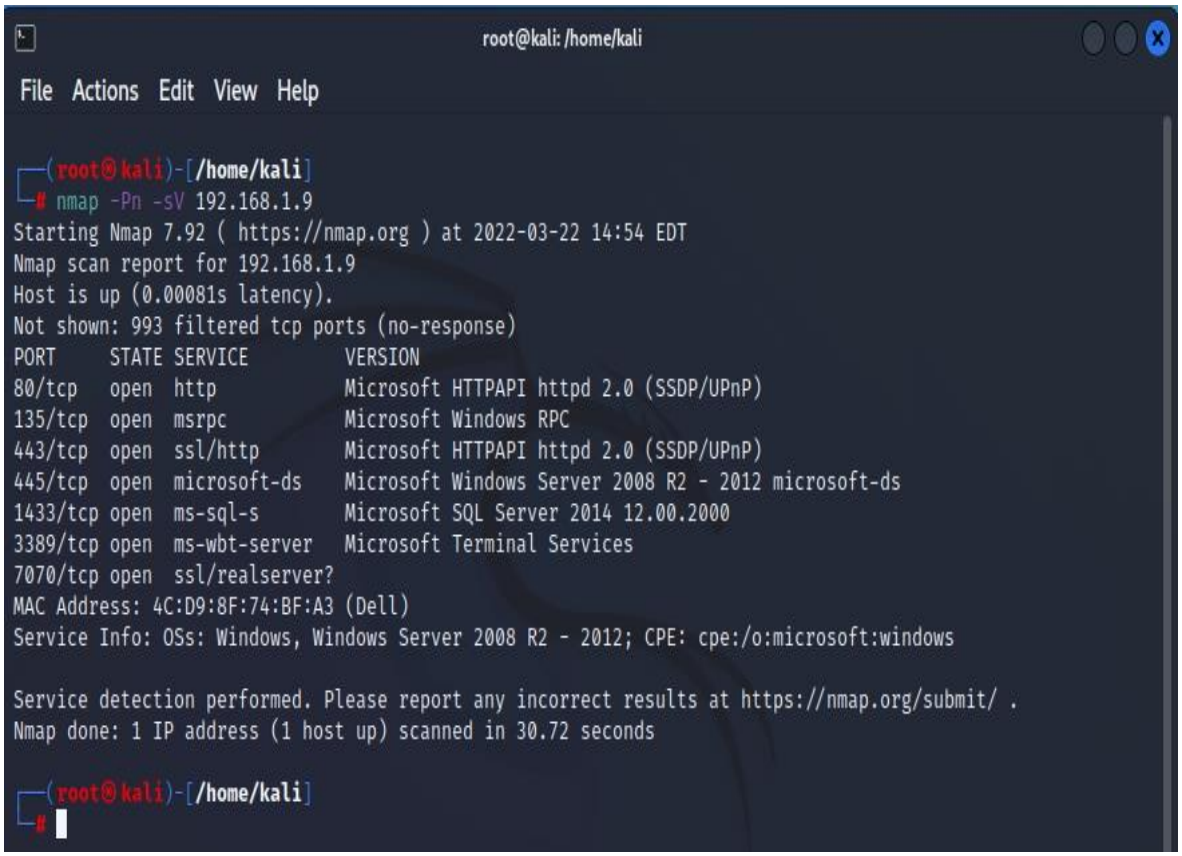
**Ilustración 26.** NMAP


**Fuente:** elaboración propia

Al revisar el análisis del escaneo se visualiza que existen servicios expuestos que no deberían estarlo como, por ejemplo, la base de datos y el FTP.

La ilustración 17 muestra el diagrama de red que tiene el sistema catastral en la infraestructura de la institución, para tener un análisis de vulnerabilidades completo se contará con un análisis de todos los dispositivos involucrados dentro de este. La ilustración 27 muestra cómo se realiza un escaneo simple con NMAP al servidor para ver los puertos que tiene abiertos.

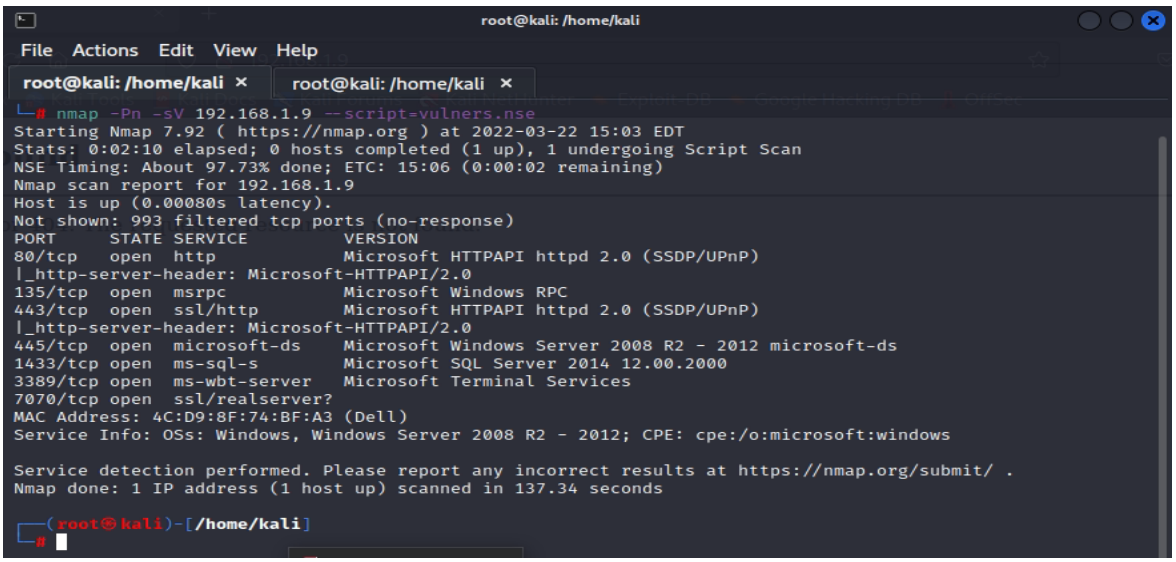
**Ilustración 27.** NMAP con vulners al servidor




**Fuente:** elaboración propia

NMAP también permite realizar un escaneo de vulnerabilidades utilizando *scripts* externos, como, por ejemplo, el de *vulners.* Este nos devuelve los puertos abiertos, los servicios y si existen vulnerabilidades con su respectivo CVE asociado. En la figura 28 se observa el resultado del escaneo donde aparateramente no tiene vulnerabilidades a nivel de servidor, ni de sus aplicaciones.

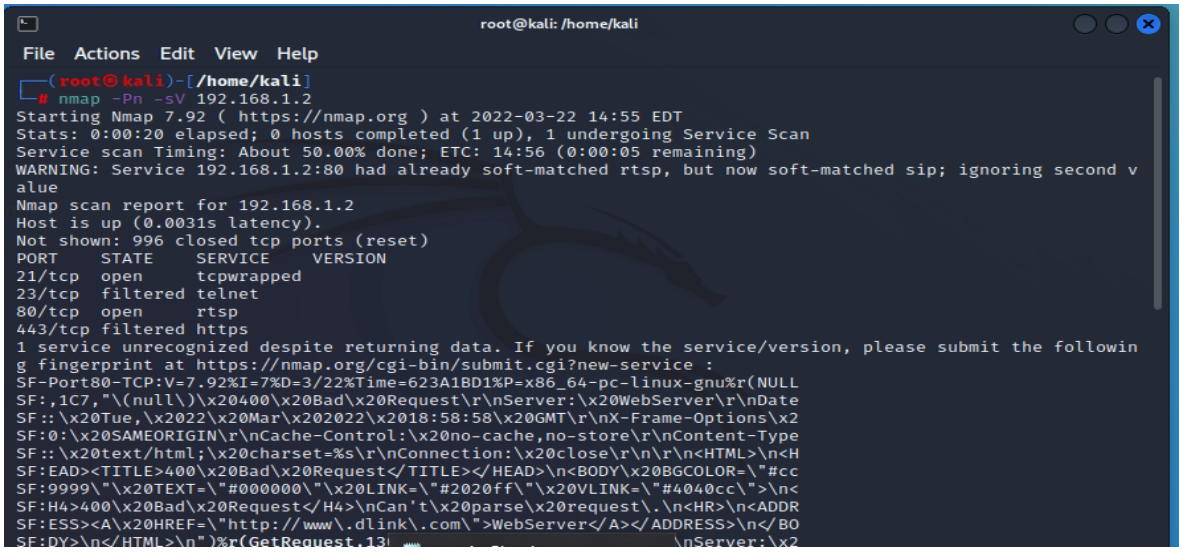
**Ilustración 28.** Escaneo de vulnerabilidades con NMAP




**Fuente:** elaboración propia

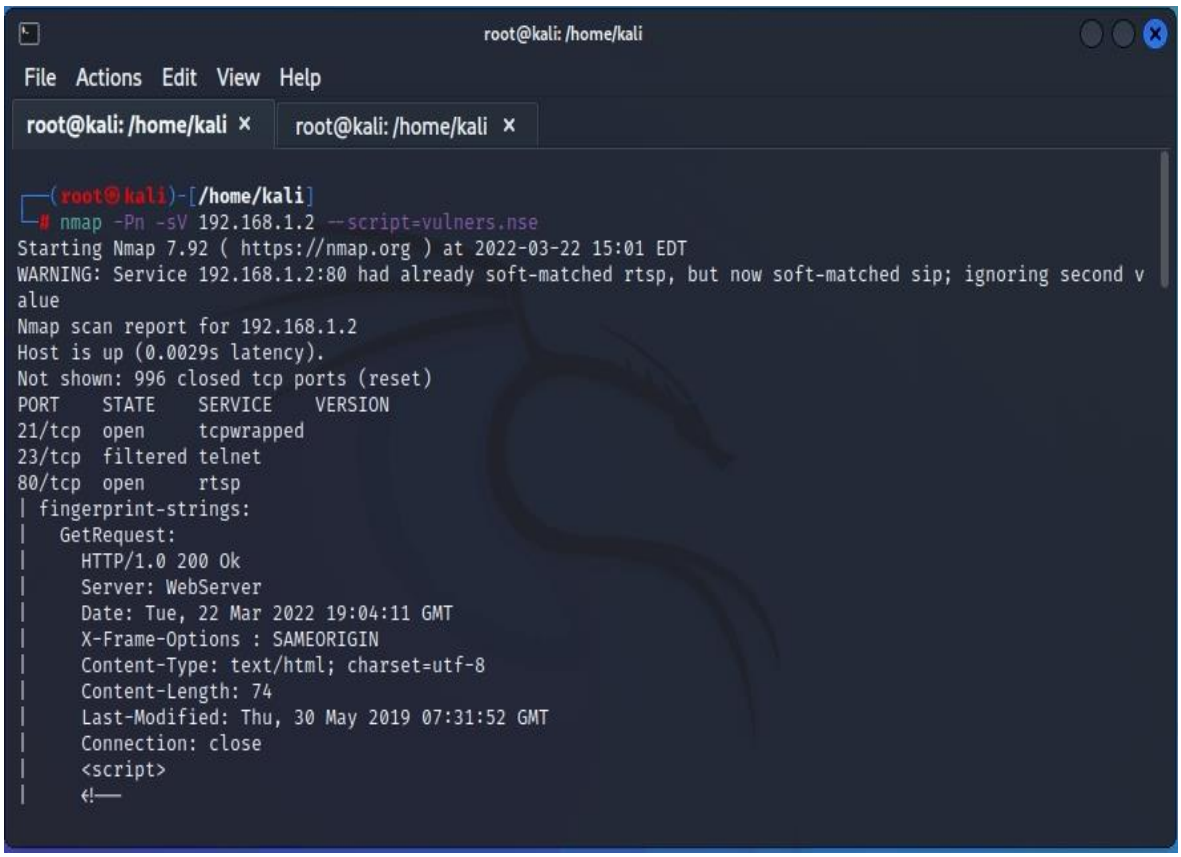
De la misma manera hacemos un análisis al *router* de borde, tanto el escaneo de puertos simple como un análisis de vulnerabilidades, se observa que el router utiliza un protocolo como TELNET que actualmente se encuentra obsoleto. De igual manera con una inspección simple se observa que no es administrable por lo que no se podrían aplicar protecciones a nivel de red. Las figuras 29 y 30 ilustran este procedimiento.

**Ilustración 29**. NMAP al *router*




**Fuente:** elaboración propia

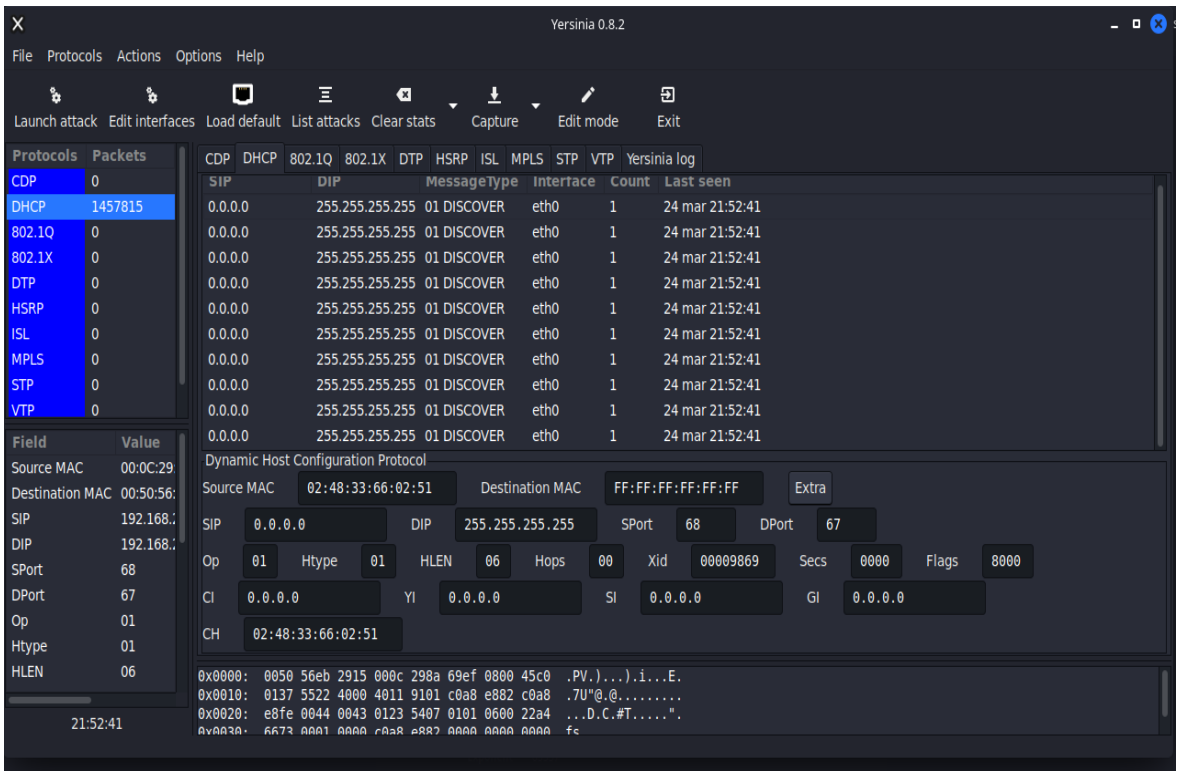
**Ilustración 30.** NMAP con el *script* de *vulners* al *router* de borde




**Fuente:** elaboración propia

A nivel de seguridad en la infraestructura de red al ser una red plana no segmentada por VLANs y el switch al no ser administrable dificultan la configuración de características como el DCHP *snopping*. Un ataque simple de DHCP *starvation* con la herramienta YERSINIA agota las direcciones IP dejando sin servicio a otros clientes. En la figura 31 se observa este procedimiento.

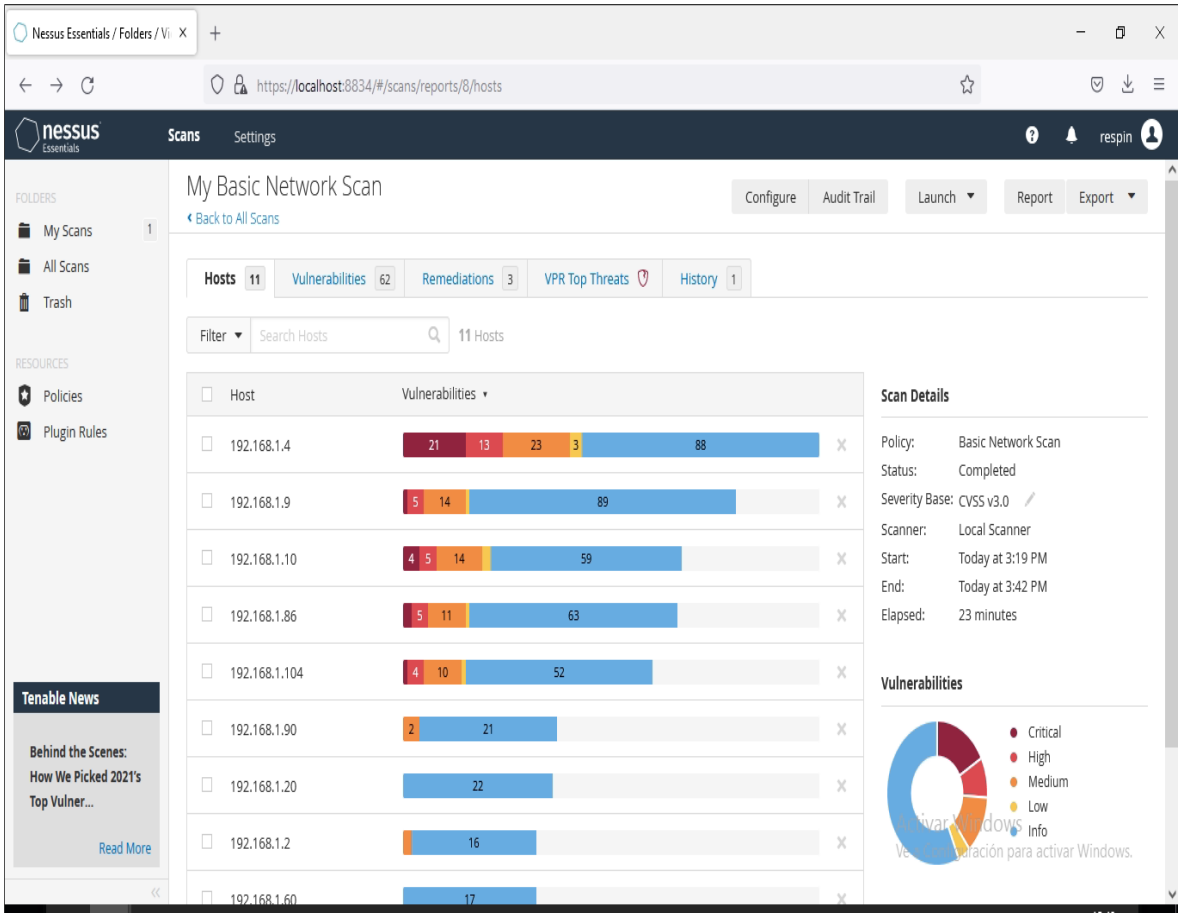
**Ilustración 31.** Ataque con Yersinia




**Fuente:** elaboración propia

La herramienta denomina NESSUS tiene como objetivo el análisis de vulnerabilidades dentro de redes privadas y corporativas, NESSUS es un *software* privativo por lo que limita el número de activos analizables a 16. Un escaneo de toda la red es necesario puesto que finalmente los activos de *harwdare* de cliente final también será un vector de ataque, sistemas operativos desactualizados o sin parchar son un gran riesgo para la organización. En la figura 32 está el resultado de la herramienta mencionada.

**Ilustración 32.** Escaneo con NESSUS a los activos.




**Fuente:** elaboración propia

Culminado el análisis de vulnerabilidades del sistema y de sus activos relacionados. Los resultados son resumidos en la siguiente tabla 7.

**Tabla 8.** Vulnerabilidades de activos

| **Vulnerabilidad** | **CVE/OSBVA** | **Criticidad** | **Herramienta** | **Activo** | **IP** |
|---|---|---|---|---|---|
| Detección de versión no compatible de *Microsoft SQL Server* (comprobación remota), la versión que tiene el sistema es 12.0.2000.0. | N/A | Crítico | NESSUS | A1<br>A2<br>A3<br>A5<br>A6<br>A7 | 192.168.1.2 |
| Certificado SSL firmado con algoritmo *hash* débil. | N/A | Alto | | | |
| Detección de protocolo SSL versión 2 y 3. | N/A | Alto | | | |
| Compatible con suites de cifrado de fuerza media SSL (SWEET32) | N/A | Alto | | | |
| El servidor sigue soportando TLS 1.0 | N/A | Medio | | | |
| SMB sin autenticación | N/A | Medio | | | |
| SSL auto firmado (Puede omitirse, debido a que la mayoría accede usando el dominio externo) y usa una llave RSA menor a 2048 bits. | N/A | Medio | | | |
| Probable inyección de SQL, la información es susceptible a filtrarse debido a un manejo inadecuado de errores durante el cifrado. | OSVDB-10107 | Medio | Nikto | | |
| Potencial RCE y posible revelación de información sensible a través de peticiones HTTP con consultas específicas. | OSVDB-12184 | Bajo | | | |
| Permite listado de directorios del sistema. | OSVDB-13404 | Bajo | | | |

| | | | | | |
|---|---|---|---|---|---|
| El archivo WS_FTP presenta información sensible. | OSVDB-13405 | Bajo | | | |
| Posible llamada a procedimientos remotos sin autorización (smssend) | OSVDB-14329 | Bajo | | | |
| *My Photo Gallery* inferior a la versión 3.6 contiene múltiples vulnerabilidades, incluido un cruce de directorios y acceso a la interfaz de administración remota. | OSVDB-2695 | Medio | | | |
| *Musicqueue* 1.20 es vulnerable a *buffer overflow.* | OSVDB-2735 | Medio | | | |
| MPM Guest Book 1.2 y sus versiones inferiores son vulnerables a ataques XSS. | OSVDB-2754 | Alto | | | |
| Immobilier agentadmin.php contiene múltiples vulnerabilidades de SQL *injection.* | OSVDB-35876 | Alto | | | |
| Múltiples *plugins* desactualizados presentan varias vulnerabilidades como acceso a archivos sin autenticación o contienen revelan información sensible. | OSVDB-42680<br>OSVDB-4314<br>OSVDB-6656<br>OSVDB-8103 | Medio | | | |

| | | | | | |
|---|---|---|---|---|---|
| DotBr 0.1 configuration *file includes usernames and passwords.* | OSVDB-5092 | Alto | | | |
| No presenta mecanismos para ataques de fuerza bruta o diccionario. | N/A | Medio | Análisis manual | | |
| Es una red plana por lo tanto todos los dispositivos tienen acceso al servidor y cualquier dispositivo puede conectarse. | N/A | Alto | Análisis manual | A8<br>A9 | N/A |
| El dispositivo no es administrable por lo que es vulnerable a ciertos ataques. | N/A | Medio | | | |
| El acceso al cuarto de servidores y la institución no está controlado. | N/A | Medio | Verificación manual. | A1 | N/A |

**Fuente:** elaboración propia

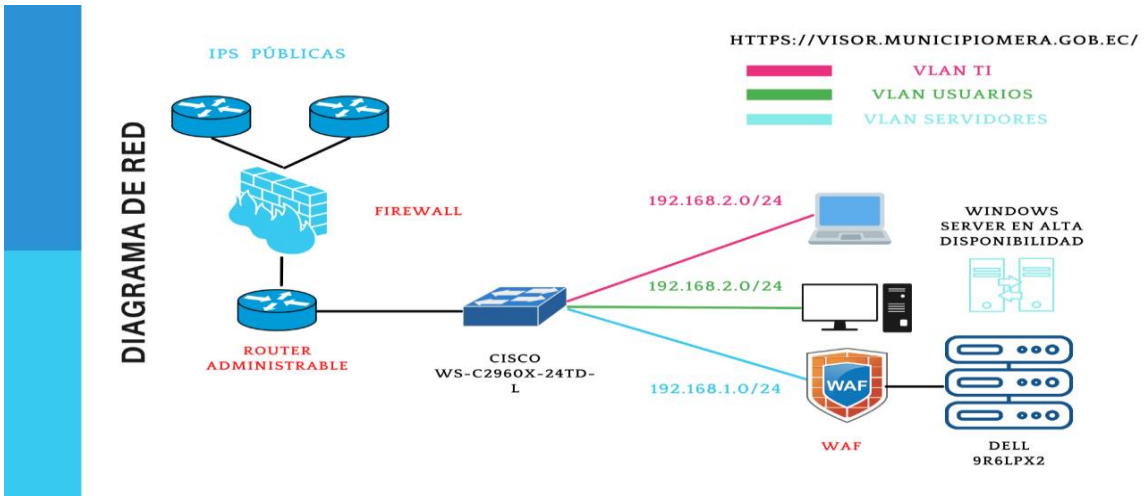
## 2.3. Elección de mecanismos de seguridad adecuados para el sistema de información catastral del cantón Mera

### Topología de red propuesta

Como parte de la implementación de mecanismos para mejorar la seguridad dentro del sistema catastral se propone reemplazar, actualizar configuraciones y añadir ciertos dispositivos o *software* dentro de la infraestructura. Añadir un *firewall* perimetral es clave dentro de la seguridad no solo del sistema sino de toda la institución a nivel informático, de igual manera para resguardar la continuidad de los servicios al añadir alta disponibilidad en diferentes puntos de fallo donde existe un único punto de servicio como, por ejemplo, el servidor o el enlace datos y también añadir un servicio de virtualización.

Para el *hardware* se toman varios aspectos como el de monitorear los dispositivos de red, esto es clave dentro de una seguridad integral porque dentro de la infraestructura virtualizada existirá un sistema para llevar un control e inventario. Otro aspecto es la reingeniería de ciertos dispositivos como el del *switch* en el que se propone segmentar en VLANs y agregar un *router* administrable para reemplazar el anterior con el fin de realizar el enrutamiento entre VLAN. En la ilustración 34 se muestra el diagrama de red propuesto.

**Ilustración 33.** Diagrama de red propuesto




**Fuente:** elaboración propia

Con el fin de apegarse a la realidad económica de la institución se pretende priorizar el uso de herramientas de código abierto, sin embargo, se plantean alternativas de pago para el caso del WAF, en la siguiente tabla se listan las herramientas y el *software* propuesto.

**Tabla 9.** Mecanismos de ciberseguridad propuestos

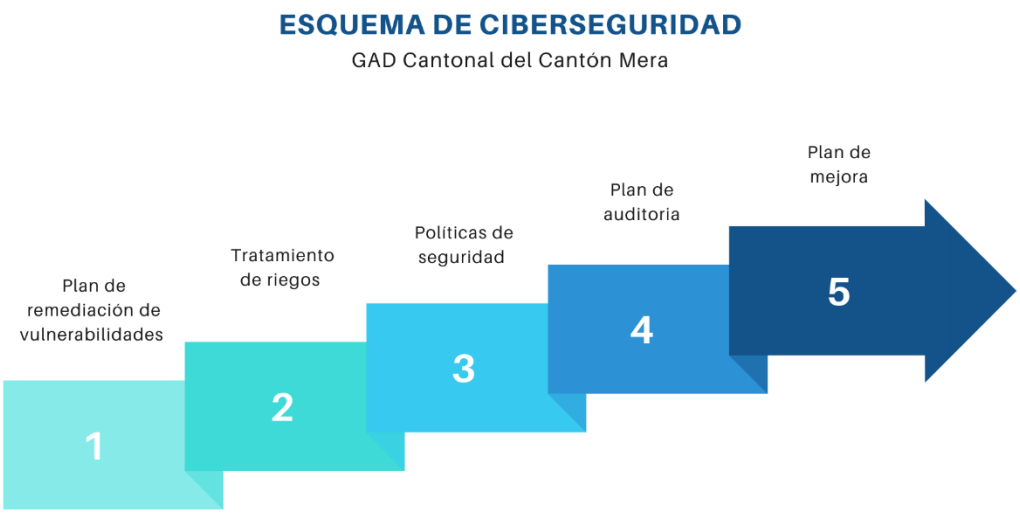
| **Activo** | **Solución** | **Licenciamiento** | **Descripción** |
|---|---|---|---|
| *Firewall* | *pfsense* | *Opensource* | *Firewall* de código abierto. |
| Sistema de monitoreo | *Zabbix* | *Opensource* | Sistema de monitoreo de dispositivos de red. |
| Virtualización | VMWare ESXi 6.5 Free | Gratuito con limitaciones. | *Hypervisor* gratuito con limitación al número de procesadores. |
| *Router* | Cisco smb Sf500-24 | N/A | *Switch Cisco* smb sf500-24-k9 administrable l3 de 24 puertos 10/100 MBPS |
| Enlace secundario | Servicio de internet secundario. | N/A | Servicio de internet IP Publica estática para la alta disponibilidad. |
| WAF | F5 *advanced* WAF | De pago. | F5 WAF es un servicio *onpremise,* es decir se despliega dentro del ambiente virtualizado (*Advanced WAF*, s/f), previene los 10 ataques más comunes a servicios web dentro del OWASP. |

**Fuente:** elaboración propia

## 2.4. Desarrollo de un prototipo de ciberseguridad

Con el diagnóstico de la situación del sistema catastral se tiene una amplia visión de lo que se ejecutará como mecanismos de ciberseguridad. El levantamiento de activos de información, su posterior evaluación de riesgos y el análisis de vulnerabilidades técnicas, permite diseñar un esquema de seguridad apropiado y ajustado a la realidad del GAD sin que este afecte económica, ni administrativamente. En la ilustración 33 se muestra la propuesta como modelo de ciberseguridad.

**Ilustración 34.** Diagrama de flujo implementación de un prototipo de ciberseguridad




**Fuente:** elaboración propia

## Plan de remediación de vulnerabilidades

La ciberseguridad consiste en asegurar la confidencialidad, integridad y disponibilidad de un sistema información. Si bien es cierto, ningún sistema se encuentra seguro en su totalidad, se busca la manera de evitar o prevenir posibles riesgos existentes a través de acciones que permitan evitar esas situaciones de riesgo. Es por esto por lo que de acuerdo con la información obtenida en el análisis de vulnerabilidades se plantean las medidas que se tomarán para eliminar o mitigar el riesgo que actualmente está latente dentro del sistema catastral. En la tabla 8 se plantea el plan de mitigación aplicable a las vulnerabilidades de los sistemas.

**Tabla 10.** Plan de remediación de vulnerabilidades

| **Vulnerabilidad** | **CVE/OSBVA** | **Solución** |
|---|---|---|
| Detección de versión no compatible de *Microsoft SQL Server* (comprobación remota), la versión que tiene el sistema es 12.0.2000.0. | N/A | Instalar la versión 12.0.6024.0. |
| Certificado SSL firmado con algoritmo *hash* débil. | N/A | Al ser un certificado auto firmado se generará otro con un algoritmo superior tal como SHA-256. |

| | | |
|---|---|---|
| Detección de protocolo SSL versión 2 y 3. | N/A | Volver a configurar la aplicación afectada para evitar el uso de cifrados de intensidad media. |
| Compatible con suites de cifrado de fuerza media SSL (SWEET32) | N/A | Volver a configurar la aplicación afectada para evitar el uso de cifrados de intensidad media. |
| El servidor sigue soportando TLS 1.0 | N/A | Deshabilitar el soporte para TLS 1.0 en el servidor. |
| SMB sin autenticación | N/A | Habilitar la autenticación SMB. |
| SSL auto firmado (Puede omitirse, debido a que la mayoría accede usando el dominio externo) y usa una llave RSA menor a 2048 bits. | N/A | Al ser un certificado auto firmado se generará otro con una llave de RSA 2048. |
| Probable inyección de SQL, la información es susceptible a filtrarse debido a un manejo inadecuado de errores durante el cifrado. | OSVDB-10107 | Solicitar al proveedor una reingeniería del código fuente de la aplicación utilizando estándares de seguridad y calidad. |
| Potencial RCE y posible revelación de información sensible a través de peticiones HTTP con consultas específicas. | OSVDB-12184 | Solicitar al proveedor una reingeniería del código fuente de la aplicación utilizando estándares de seguridad y calidad. |
| Permite listado de directorios del sistema. | OSVDB-13404 | Solicitar al proveedor una reingeniería del código fuente de la aplicación utilizando estándares de seguridad y calidad. |
| El archivo WS_FTP presenta información sensible. | OSVDB-13405 | Solicitar al proveedor una reingeniería del código fuente de la aplicación utilizando estándares de seguridad y calidad. |
| Posible llamada a procedimientos remotos sin autorización (smssend) | OSVDB-14329 | Solicitar al proveedor actualizar las librerías utilizadas. |

| | | |
|---|---|---|
| *My Photo Gallery* inferior a la versión 3.6 contiene múltiples vulnerabilidades, incluido un cruce de directorios y acceso a la interfaz de administración remota. | OSVDB-2695 | Solicitar al proveedor actualizar las librerías utilizadas. |
| *Musicqueue* 1.20 es vulnerable a *buffer overflow*. | OSVDB-2735 | Solicitar al proveedor actualizar las librerías utilizadas. |
| *MPM Guest Book* 1.2 y sus versiones inferiores son vulnerables a ataques XSS. | OSVDB-2754 | Solicitar al proveedor actualizar las librerías utilizadas. |
| Immobilier agentadmin.php contiene múltiples vulnerabilidades de SQL *injection.* | OSVDB-35876 | Solicitar al proveedor actualizar las librerías utilizadas. |
| Múltiples librerías desactualizadas presentan varias vulnerabilidades como acceso a archivos sin autenticación o contienen revelan información sensible. | OSVDB-42680<br>OSVDB-4314<br>OSVDB-6656<br>OSVDB-8103 | Solicitar al proveedor actualizar las librerías utilizadas. |
| DotBr 0.1 *configuration file includes usernames and passwords.* | OSVDB-5092 | Solicitar al proveedor actualizar las librerías utilizadas. |
| No presenta mecanismos para ataques de fuerza bruta o diccionario. | N/A | Implementar un WAF o reingeniería del código para implementar mecanismos contra múltiples solicitudes a nivel de programación. |
| Es una red plana por lo tanto todos los dispositivos tienen acceso al servidor y cualquier dispositivo puede conectarse. | N/A | Adquirir un *switch* administrable con el fin de crear VLANs. |
| El dispositivo no es administrable por lo que es vulnerable a DHCP starvation lo que agota las direcciones IP. | N/A | Adquirir un *switch* administrable con el fin de definir protecciones como un |

**Fuente:** elaboración propia

## Tratamiento de riesgos

El tratamiento de riesgos propone controles aplicados a los riesgos con el fin de mitigarlos, en la tabla 9 se muestra el tratamiento propuesto.

**Tabla 11.** Controles para el tratamiento de riesgos

| **Descripción del riesgo** | **Control para implementar** | **Fecha de cumplimiento** | **Medio de verificación.** |
|---|---|---|---|
| No se cuentan con copias de seguridad automatizadas periódicas. | Implementar respaldos diarios fuera de sitio en una nube privada. | 01/06/2022 | Bitácora de respaldos |
| No se realizan copias de seguridad completas del sistema. | Definir copias completas de sistema en discos duros externos bajo un procedimiento documentado. | 01/06/2022 | Procedimiento documentado. |
| No existe un inventario de información confidencial | Inventariar la información confidencial y clasificarla según criticidad. | 01/06/2022 | Listado maestro de información confidencial. |
| No elimina los datos confidenciales o sistemas a los que la organización no accede regularmente | Definir un procedimiento documentado para eliminar información dentro del sistema catastral. | 15/06/2022 | Procedimiento documentado. |
| Se permiten dispositivos USB | Bloquear el acceso a USB no federados a los equipos de cliente final. | 01/06/2022 | Política aplicada |
| No cuentan con autenticación multifactor. | Aplicar a los administradores de sistema métodos de doble factor de autenticación. | 01/06/2022 | Política aplicada |
| No limita el acceso a las herramientas de *script* en el servidor | Bloquear la ejecución de scripts en el servidor. | 01/06/2022 | Política aplicada |
| No controla o monitorea cuentas asociadas con pruebas de penetración. | Instalar *zabbix* para monitorear a los dispositivos. | 01/06/2022 | *Zabbiz* desplegado |

| | | | |
|---|---|---|---|
| No usa herramientas de análisis de vulnerabilidades y pruebas de penetración. | Usar herramientas de manejo de vulnerabilidades de *software* libre. | 01/06/2022 | Herramientas y agentes desplegados. |
| No se implementa *firewalls* de aplicaciones web (WAF) | Implementar un WAF en la nube. | 01/07/2022 | WAF desplegado |
| El personal no cuenta con capacitación acerca de: manejo de datos confidenciales, sobre las causas de la exposición no intencional de datos, notificación de incidentes de ciberseguridad, ingeniería social y autenticación segura. | Capacitar a los usuarios dentro de buenas prácticas dentro del uso de la información manejada dentro del sistema catastral, así como el uso de contraseñas, etc. | 15/07/2022 | Documentación de capacitación generada. |
| No tiene un plan de contingencia, como un enlace secundario o un servidor para alta disponibilidad. | Virtualizar el servidor o en su lugar un segundo servidor en alta disponibilidad, a su vez, contratar un enlace de internet secundario en modo activo-pasivo. | 15/07/2022 | Servidor virtualizado, servidor secundario desplegado y enlace de datos contratado y configurado. |
| Los equipos de red no cuentan con un respaldo de sus configuraciones. | Montar un servidor de GITLAB para versionar las configuraciones de los equipos de comunicaciones. | 01/08/2022 | Sistema de versionamiento desplegado. |
| No se cuenta con un equipo de seguridad perimetral, ni con *endpoint.* | Adquirir un sistema de seguridad de perímetro. | 15/08/2022 | *Software* de perímetro desplegado |

**Fuente:** elaboración propia

Como parte de la remediación de vulnerabilidades y el tratamiento de riesgos se plantea un nuevo esquema de red aplicando mejoras y cambios dentro de este. Para evitar costos se tiene como prioridad usar herramientas *opensource*. Los principales cambios para aplicar son:

- Tener redundancia a nivel de *router* de borde, pues su ausencia representa un riesgo de pérdida de conectividad con los enlaces externos al no existir alta disponibilidad el dispositivo que actualmente está operando presentaría fallos y no tener un medio al cuál conmutar para mantener la disponibilidad del servicio.
- Aplicación de *software* de seguridad perimetral. Implementar una solución de seguridad de perímetro para asignar permisos de navegación y administrar el tráfico entrante, realizar reglas de NAT, etc.
- Enlace redundante. Contratar un enlace de respaldo con un proveedor y aplicar balanceo de carga y alta disponibilidad.
- Virtualización para tener alta disponibilidad a nivel de servidor se virtualizará el servidor y tener una réplica en modo activo-pasivo.
- Reingeniería del *Switch* para segmentar las redes a nivel de capa 2 y aplicar protecciones para ataques a nivel de infraestructura de red.

**Políticas de seguridad para el uso del sistema ANZU**

La información es un recurso de carácter estratégico para el GAD Cantonal de Mera y, por lo tanto, su protección de garantizarse. Esto no quiere decir que la protección de la información sea un fin en sí mismo, sino que, será protegida en la medida que el cumplimiento de la misión del GAD depende de ella. El sistema catastral forma parte de los procesos del valor agregado por lo que contará con mecanismos de seguridad. Una parte fundamental es la aplicación de políticas que los usuarios que utilizan el sistema seguirán. Apegarse a estas normas ayudará al buen uso de la plataforma. Estas políticas serán aprobadas por alcaldía y distribuidas al personal involucrado.

**Tabla 12.** Política de confidencialidad y difusión de información del sistema ANZU

| **DECLARACIÓN DE LA POLÍTICA** |
| --- |
| Todos los candidatos, aspirantes, contratistas involucrados con el sistema catastral firmarán un acuerdo de confidencialidad.<br>La información que contenga datos personales (cédula, teléfonos, nombres, etc.) no puede ser difundida ni divulgada. |
| **OBJETIVO** |
| Reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información del sistema. |

**Fuente:** elaboración propia

**Tabla 13.** Política de medios removibles ANZU

| **DECLARACIÓN DE LA POLÍTICA** |
| --- |
| El uso de medios de almacenamiento removibles será autorizado por el jefe departamental y monitoreado por el departamento de tecnologías de la información. Para el caso del servidor solo TI está autorizado a insertar medios removibles dentro del servidor.<br>El uso de servicios de almacenamiento en la nube será aprobado por el jefe inmediato y no se almacenará información de terceros. |
| **OBJETIVO** |
| Reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información del sistema. |

Fuente: elaboración propia

**Tabla 14.** Política de uso de activos ANZU

| **DECLARACIÓN DE LA POLÍTICA** |
| --- |
| Se permite a los usuarios: la descarga de archivos desde internet, únicamente con fines institucionales. De igual manera está prohibido la navegación en sitios que contengan pornografía, música ilegal, *torrents* u otros considerados peligrosos.<br>Los usuarios no están autorizados a instalar o modificar *software*, solo TI está autorizado a hacerlo.<br>Los equipos y servidores involucrados que requieran salir de la institución para mantenimiento u otros motivos no tendrán información confidencial o de terceros. |
| **OBJETIVO** |
| Reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información del sistema. |

**Fuente:** elaboración propia

**Tabla 15.** Política de contraseñas

| **DECLARACIÓN DE LA POLÍTICA** |
| --- |
| Las contraseñas de los usuarios contarán con un mínimo de 12 caracteres que incluyan mayúsculas, minúsculas, números y caracteres especiales, además, será obligatorio cambiar esta cada 3 meses.<br>También está prohibido almacenar las claves de acceso del sistema en lugares visibles como en el computador, escritorios, etc.<br>Las contraseñas del sistema y del computador con el que acceden al mismo son propiedad del usuario asignado y son para uso personal, no serán compartidas.<br>Los usuarios administradores tendrán doble factor de autenticación. |
| **OBJETIVO** |
| Promover el uso de contraseñas seguras y asegurar la confidencialidad de la información. |

**Fuente:** elaboración propia

## Plan de auditoria

Determinar el grado de calidad de los mecanismos de ciberseguridad implementados para el sistema catastral ANZU del GAD Cantonal Mera bajo los siguientes criterios de auditoria:

- Evaluar la capacidad en los mecanismos de ciberseguridad para asegurar el cumplimiento de los requisitos reglamentarios y contractuales del producto y servicio.
- Evaluar la eficacia de los mecanismos aplicados para lograr los objetivos especificados.
- Identificar mecanismos de mejora en los mecanismos implementados.

El auditor será encargado de resolver lo planteado en la tabla y no pertenecerá a la institución.

**Tabla 16.** Actividades del plan de auditoría

| **Actividad** | **Fecha** | **Documento de respaldo** |
|---|---|---|
| Análisis de vulnerabilidades con el fin de verificar si se remediaron. | 20/07/2022 | Reporte de vulnerabilidades. |
| Verificación de cumplimiento de políticas. | 20/08/2022 | Reporte de hallazgos |
| Realizar pruebas de penetración al sistema y a los equipos de red | 15/08/2022 | Informe de pruebas de penetración. |
| Se realizará una prueba del correcto funcionamiento de los respaldos. | 15/09/2022 | Informe del procedimiento e incidencias acerca los respaldos. |

**Fuente:** elaboración propia

# CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

## 3.1. Evaluación de mecanismos elegidos

Un software de seguridad perimetral es clave en una infraestructura seria de seguridad, la elección de una herramienta *opensource* como *pfSense* reducen la probabilidad de un ataque directo a la red y al sistema de información, también la posibilidad se proveer permisos de navegación por usuario facilita la gestiona y secciona a usuarios con privilegios.

Un WAF protege de los ataques más comunes descritos en el top ten de *OWASP*, mencionados anteriormente, por lo que a nivel *web* el riesgo de una intrusión se reduce, sumado a la remediación de vulnerabilidades hacen del sistema ANZU bastante robusto.

Segmentar la red, actualizar los equipos de red y configurarlos con mecanismos de seguridad, además de implementar un equipo de seguridad perimetral aplicando los permisos respectivos de navegación, reducen el riesgo de un incidente de ciberseguridad a nivel de infraestructura, sumado a la creación de políticas de seguridad que los usuarios finales están cumplir, cumplen la meta de asegurar el eslabón más débil, es decir, el usuario final que utiliza el sistema ANZU.

La herramienta de monitoreo *Zabbix* permite monitorear el estado de los equipos involucrados en el sistema de información ANZU, lo que alerta de posibles incidentes como consumo excesivo de recursos, temperatura o estado de los enlaces de datos que pueden afectar a la disponibilidad de los servicios, con los reportes y advertencias el administrador puede tomar correctivos para la continuidad de los servicios.

## 3.2. Evaluación del prototipo de ciberseguridad

Cuando se elige una herramienta o mecanismo de ciberseguridad, como por ejemplo el WAF, el fin es minimizar los riesgos o la posibilidad de un incidente, si bien el WAF cumple con su trabajo, es necesario corregir vulnerabilidades y falencias dentro de un sistema de información, con el fin de definir un prototipo completo de ciberseguridad el plan de remediación de vulnerabilidades

encontradas a nivel web se complementa con e WAF haciendo que la probabilidad sea aún menor. De igual manera sucede con el software de seguridad perimetral, por lo que las vulnerabilidades a nivel de infraestructura de red con el prototipo propuesto en el plan de remediación se eliminan, asegurando la integridad de la infraestructura interna del sistema de información y del GAD.

Un tratamiento de riesgos cumple un rol vital dentro de cualquier sistema de información, al tener un sistema de gestión de riesgos se trata de reducir los mismos mediante la aplicación de controles a todos los ámbitos relacionados con el sistema ANZU, por lo que juntamente con el plan de auditoría y mejora aseguran la confidencialidad, disponibilidad e integridad. Entre los controles aplicados se encuentran un plan de respaldos, mejora de los sistemas UPS y un enlace secundario, la virtualización de los servidores en alta disponibilidad, que garantizan la integridad y la disponibilidad; el manejo e inventario de activos de información sensibles, bloqueo de dispositivos USB que asegura la confidencialidad, entre otros.

Si bien el sistema ANZU no ha sufrido un incidente de ciberseguridad el riesgo de que se presente uno siempre estuvo latente, con la aplicación de los mecanismos y el prototipo implementado, este riesgo se reduce considerablemente. Esto asegura el cumplimiento de las leyes aplicables en el ámbito de seguridad de la información del país.

En la tabla 17 se muestra el riesgo luego de aplicar los controles correspondientes, el nivel de madurez es 5, por lo que el riesgo disminuye a 3, que según la tabla 4 se convierte en un riesgo aceptable.

**Tabla 17.** Niveles de riesgos después de aplicar el plan de tratamiento

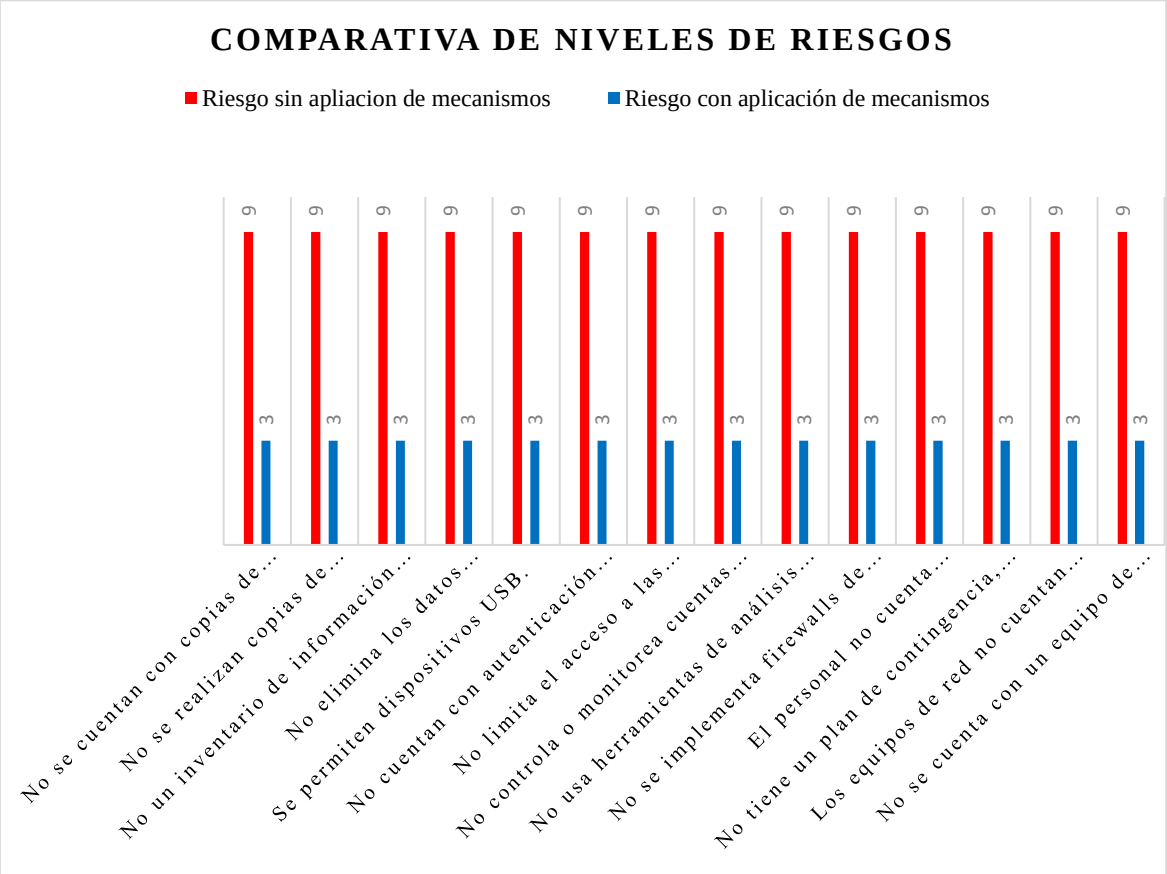
| **Descripción del riesgo** | **Valor** | **Nivel de madurez del control** | **Valor riesgo** |
|---|---|---|---|
| No se cuentan con copias de seguridad automatizadas periódicas. | 15 | 5 | 3 |
| No se realizan copias de seguridad completas del sistema. | 12 | 5 | 3 |
| No un inventario de información confidencial | 12 | 5 | 3 |
| No elimina los datos confidenciales o sistemas a los que la organización no accede regularmente. | 12 | 5 | 3 |
| Se permiten dispositivos USB. | 15 | 5 | 3 |
| No cuentan con autenticación multifactor. | 12 | 5 | 3 |
| No limita el acceso a las herramientas de *script* en el servidor. | 15 | 5 | 3 |
| No controla o monitorea cuentas asociadas con pruebas de penetración. | 15 | 5 | 3 |
| No usa herramientas de análisis de vulnerabilidades y pruebas de penetración. | 15 | 5 | 3 |
| No se implementa *firewalls* de aplicaciones web (WAF). | 15 | 5 | 3 |
| El personal no cuenta capacitación acerca de: manejo de datos confidenciales, sobre las causas de la exposición no intencional de datos, notificación de incidentes de ciberseguridad, ingeniería social y autenticación segura. | 12 | 5 | 3 |
| No tiene un plan de contingencia, como un enlace secundario o un servidor para alta disponibilidad. | 12 | 5 | 3 |
| Los equipos de red no cuentan con un respaldo de sus configuraciones. | 12 | 5 | 3 |
| No se cuenta con un equipo de seguridad perimetral ni con *endpoint.* | 12 | 5 | 3 |

**Fuente:** elaboración propia

En la ilustración 35 podemos ver la comparativa de los riegos de seguridad según la metodología CIS RAM, donde todos los riesgos tiene un valor de 9 puesto que la aplicación de mecanismos tiene un nivel de madurez de 1, mientras que en con el

nivel de madurez 5, es decir controles o mecanismos aplicados, el riesgo se reduce a 3, por lo que, según los criterios elegidos, es un nivel de riesgo aceptable.

**Ilustración 35.** Comparativa de riesgos según el nivel de madurez




**Fuente:** elaboración propia

A partir del análisis de riesgos, el diagnóstico de la situación actual y la investigación de los mecanismos existentes, con la aplicación de estos se forma un prototipo de mecanismos de ciberseguridad para un sistema de información basado en controles, hardware y software. Al implementar mecanismos de ciberseguridad el riesgo se reduce considerablemente, pero no se elimina, pues este es el fin de aplicar dichas herramientas, siempre existe lo denominado como riesgo residual.

Los resultados indican que con los mecanismos de ciberseguridad elegidos y el prototipo desarrollado se cumple con el objetivo de mitigar el riesgo de un incidente cibernético en el sistema catastral ANZU. Priorizar de herramientas de software libre ayuda a mantener un balance entre seguridad y presupuesto para una

institución pequeña sin que se vea afectado el rendimiento, pues con una elección correcta de mecanismos y herramientas se reduce el riesgo a niveles aceptables.

Por último, una etapa clave en el prototipo es la mejora, porque eventualmente se debe evaluar los mecanismos según lo planteado en el plan de auditoria con el fin de mantener la gestión actualizada mejorar los niveles de seguridad relacionados al sistema de información.

## CONCLUSIONES

- En el presente trabajo se abordó la temática de ciberseguridad, con la implementación de una serie de mecanismos de ciberseguridad en el sistema de gestión catastral del GAD cantonal de Mera, consiguiendo mejorar la disponibilidad, la integridad y la confidencialidad de la información.

- Se recopiló información con el fin de conocer los fundamentos teóricos a profundidad que sirven como base para la elaboración de proyectos de ciberseguridad, realizando un análisis bibliográfico acerca de estándares y mecanismos en el área de seguridad de la información.

- Con el análisis de la situación en la que estaba el sistema y sus activos relacionados, así como el levantamiento de activos de información para realizar un análisis de riesgos, se determinaron varias vulnerabilidades críticas a nivel de infraestructura, organización y del sistema de gestión catastral GAD del cantón Mera.

- Con el fin de mejorar la seguridad del sistema de catastral se propusieron una serie de mecanismos mediante el diseño de un prototipo, con diferentes mecanismos aplicables a sistemas de información, llegando a la conclusión de que usar varios mecanismos ya existentes (políticas, herramientas de software, controles de seguridad, reestructuración de la infraestructura) es la forma más eficiente de mantener seguros los activos de información relacionados al sistema catastral.

## RECOMENDACIONES

- Poner en funcionamiento todos los puntos del plan recomendado y evaluarlos anualmente para comprobar la eficiencia del prototipo.
- Elaborar y documentar procedimientos con el fin de reducir el riesgo en las actividades relacionadas al sistema catastral.
- Invertir en capacitaciones en el personal TI a nivel de seguridad de la información y segmentar sus áreas con el fin de evitar que un solo técnico realice todas las actividades.
- Aumentar el presupuesto para el área de TI, con el fin de que no sea visto como un gasto sino inversión.
- Fomentar una cultura de seguridad de la información dentro de todo el personal del GAD.
- Se recomienda tener contactos con diferentes instituciones similares en infraestructura y personal, con el fin de compartir experiencia.

## BIBLIOGRAFÍA

3 Types of Web Application Firewalls: How to Choose? (2020, agosto 3). *Penta Security Systems Inc.* Obtenido de https://www.pentasecurity.com/blog/3-types-web-application-firewalls/

*A01 Broken Access Control—OWASP Top 10:2021* (s/f). Recuperado el 14 de febrero de 2022, Obtenido de https://owasp.org/Top10/A01_2021-Broken_Access_Control/

*Acuerdos. 017-21 Refórmese el Acuerdo Ministerial No. 020-20 de 25 de mayo de 2020* (s/f). vLex. Recuperado el 16 de enero de 2022, Obtenido de https://vlex.ec/vid/017-21-reformese-acuerdo-873603569

*Advanced WAF* (s/f). Recuperado el 24 de abril de 2022, Obtenido de https://www.f5.com/es_es/products/security/advanced-waf.html

Andress, J., & Leary, M., (2016). *Building a Practical Information Security Program*. Syngress.

*ANT presenta quinta denuncia contra ataques informáticos* (2021, julio 21).Obtenido de https://www.lahora.com.ec/pais/ant-denuncia-ataques-informaticos/

Acorte (2019). *Arcotel Informa—Revista Institucional No.20 by ARCOTEL Ecuador—Issuu*.Obtenido de https://issuu.com/arcotelecuador/docs/revista20-comprimido__1_

Bhattacharya, S. M. A. B., Abhishek (2020). *Secure Chains: Cybersecurity and Blockchain-powered automation*. BPB Publications.

Briceño, E. V., (2021). *Seguridad de la información*. 3Ciencias.

Bus de Servicios Gubernamentales MINTEL (2018, octubre 10). *Gobierno Electrónico de Ecuador*. Obtenido de https://www.gobiernoelectronico.gob.ec/bus-de-servicios-gubernamentales/

Calder, A., (2011). *Implementing Information Security based on ISO 27001/ISO 27002*. Van Haren.

Canlas, R., & Price, E., (2021). *ASP.NET Core 5 Secure Coding Cookbook: Practical recipes for tackling vulnerabilities in your ASP.NET web applications*. Packt Publishing Ltd.

CARLOS, C. G., & ANTONIO, C. G., JUAN (2017). *Salvaguarda y seguridad de los datos*. Ediciones Paraninfo, S.A.

Chakraborty, M., Singh, M., Balas, V. E., & Mukhopadhyay, I., (2020). *The "Essence" of Network Security: An End-to-End Panorama*. Springer Nature.

Chou, E., & Groves, R., (s/f). *Distributed Denial of Service (DDoS)*. 89.

Ciampa, M., (2020). *CompTIA Security+ Guide to Network Security Fundamentals* (7th edition). Cengage Learning.

CIS (s/f). *CIS RAM (Risk Assessment Method)*. CIS. Recuperado el 3 de abril de 2022, Obtenido de https://www.cisecurity.org/white-papers/cis-ram-risk-assessment-method/

Crawley, D. R., (2015). *Cisco ASA for Accidental Administrators: An Illustrated Step-by-Step ASA Learning and Configuration Guide*.

*Cross Site Scripting (XSS) Software Attack* | *OWASP Foundation* (s/f). Recuperado el 13 de febrero de 2022, Obtenido de https://owasp.org/www-community/attacks/xss/

Datalinknetworks (s/f). *What is a Web Application Firewall (WAF)? Types & Benefits of Web Application Firewalls [2021 Update]*. Datalinknetworks. Recuperado el 28 de marzo de 2022, Obtenido de https://www.datalinknetworks.net/dln_blog/what-is-a-web-application-firewall

Deane, A. J., (2020). *CCSP For Dummies with Online Practice*. John Wiley & Sons.

*DOM Based XSS Software Attack | OWASP Foundation* (s/f). Recuperado el 13 de febrero de 2022, Obtenido de https://owasp.org/www-community/attacks/DOM_Based_XSS

Ecuador y su primera Ley Orgánica de Protección de Datos Personales (2021, junio 16). *Delegado de protección de datos*. Obtenido de https://dpd.aec.es/ecuador-y-su-primera-ley-organica-de-proteccion-de-datos-personales/

EGSI v2 (s/f). *Gobierno Electrónico de Ecuador*. Recuperado el 16 de enero de 2022, Obtenido de https://www.gobiernoelectronico.gob.ec/egsi-v2/

Fox, R., (2013). *Information Technology: An Introduction for Today's Digital World*.

Gamon, V. P., (2017). Internet, la nueva era del delito: Ciberdelito, ciberterrorismo, legislación y ciberseguridad/ Internet, the new age of crime: cibercrime, ciberterrorism, legislation and cibersecurity. *URVIO. Revista Latinoamericana de Estudios de Seguridad*, *20*, 80–93. Obtenido de https://doi.org/10.17141/urvio.20.2017.2563

Gibson, D., & Igonor, A., (2020). *Managing Risk in Information Systems*.

Guise, P. de., (2017). *Data Protection: Ensuring Data Availability*.

Gupta, B. B., & Chaudhary, P., (2020). *Cross-Site Scripting Attacks: Classification, Attack, and Countermeasures*. CRC Press.

Gupta, B. B., & Dahiya, A., (2021). *Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures*. CRC Press.

Gutiérrez, J., & Ayuso, J. G. T., (2003). *Protocolos criptográficos y seguridad de redes*. Ed. Universidad de Cantabria.

Hartley, D., (2012). What Is SQL Injection? En *SQL Injection Attacks and Defense* (pp. 1–25). Elsevier. Obtenido de https://doi.org/10.1016/B978-1-59-749963-7.00001-3

Heredero, C. de P., Agius, J. J. L. H., Romero, S. M.-R., & Salgado, S. M., (2019). *Organización y transformación de los sistemas de información en la empresa*. ESIC.

*Infografía: ¿Cuántos usuarios de Internet hay en América Latina?* (2018). Statista Infografías. Obtenido de https://es.statista.com/grafico/13903/cuantos-usuarios-de-internet-hay-en-america-latina/

*ISO/IEC 27000 – key International Standard for information security revised* (s/f). ISO. Recuperado el 30 de enero de 2022, Obtenido de https://www.iso.org/cms/render/live/en/sites/isoorg/contents/news/2018/03/Ref2266.html

*ISO/IEC 27003—Guía para la implementación de un Sistema de Gestión de Seguridad de la Información* (2014, enero 17). PMG SSI - ISO 27001.Obtenido de https://www.pmg-ssi.com/2014/01/isoiec-27003-guia-para-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-información/

*ISO/IEC 27005:2018 (en), Information technology—Security techniques—Information security risk management* (s/f). Recuperado el 16 de enero de 2022, Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en

Jarrín, E. J., Cueva, T. P., Sarmiento, T. A., Cevallos, D. G., & Aguirre, J. P., (s/f). *Raquel González Lastre presidenta del Consejo de Participación Ciudadana y Control Social*. 60.

Karamanian, A., (2011). *PKI Uncovered: Certificate-Based Security Solutions for Next-Generation Networks: CertificateBased Security Solutions for NextGeneration Networks ...* (1st edition). Cisco Press. *Learn about the CIS Controls™* (s/f). CIS. Recuperado el 30 de enero de 2022, de Obtenido de https://www.cisecurity.org/controls/v7/

López, P. A., (2010). *Seguridad informática*. Editex.

*Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método* (s/f). 127.

Mera, C., & Areas, Y., (s/f). *SEGÚN NIVELES DE INSTRUCCIÓN. Censo 2001 TOTAL HOMBRES*. 4.

Miessler, D., (2022). *Danielmiessler/SecLists* [PHP]. Obtenido de https://github.com/danielmiessler/SecLists/blob/168584fdc61b44080342291611238585648f08a8/Passwords/Common-Credentials/10-million-password-list-top-10000.txt (Original work published 2012)

Miguel, A. D. P., (2019). *Gestión de archivos*. Ediciones Paraninfo, S.A.

Moallem, A., (2021). *Understanding Cybersecurity Technologies: A Guide to Selecting the Right Cybersecurity Tools*.

Mondesir, C., (2015). *Computer Network Security: Firewall Software*.

Peña Segura, X. A., (s/f). *Sistema de Información Geográfica aplicado al Catastro Predial del Cantón Paute, ECUADOR*. Universidad San Francisco de Quito.

Priyadarshini, I., & Cotton, C., (2022). *Cybersecurity: Ethics, Legal, Risks, and Policies*. CRC Press.

Quito, P. Y. L. 4 de A. de 2021 D., (s/f). *Nuevo ataque cibernético a un organismo estatal ecuatoriano*. infobae. Recuperado el 13 de enero de 2022, Obtenido de https://www.infobae.com/america/america-latina/2021/08/04/nuevo-ataque-cibernetico-a-un-organismo-estatal-ecuatoriano/

Quito, P. Y. L. 19 de J. de 2021 D., (s/f). *Un ataque informático apagó las computadoras de la Corporación Nacional de Telecomunicaciones del Ecuador*. infobae. Recuperado el 13 de enero de 2022, Obtenido de https://www.infobae.com/america/america-latina/2021/07/19/un-ataque-informatico-apago-las-computadoras-de-la-corporacion-nacional-de-telecomunicaciones-del-ecuador/

Rathore, P. S., Dutt, V., Agrawal, R., Sasubilli, S. M., & Swarna, S. R., (2022). *Deep Learning Approaches to Cloud Security*. John Wiley & Sons.

Smith, R. E., (2011). *Elementary Information Security*. Jones & Bartlett Publishers.

Stewart, J. M., & Kinsey, D., (2020). *Network Security, Firewalls, and VPNs* (3rd edition). Jones & Bartlett Learning.

Surianarayanan, C., & Chelliah, P. R., (2019). *Essentials of Cloud Computing: A Holistic Perspective*.

Talabis, M., & Martin, J., (2012). *Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis*.

Terán, D., (2014). *Administración Estratégica de la función informática*. Alfaomega Grupo Editor.

WeLiveSecurity.*¿En qué consiste la vulnerabilidad Cross Site Request Forgery (CSRF)?* (2015, abril 21). Obtenido de https://www.welivesecurity.com/la-es/2015/04/21/vulnerabilidad-cross-site-request-forgery-csrf/

*What Is a Secure Email Gateway (SEG)?* (s/f). Check Point Software. Recuperado el 4 de abril de 2022, Obtenido de https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-email-security/what-is-a-secure-email-gateway-seg/

Williams, W., (2021). *Creating an Information Security Program from Scratch*. CRC Press.

Wu, C.-H., (John), & Irwin, J. D., (2016). *Introduction to Computer Networks and Cybersecurity*. CRC Press.