

**PROPUESTA PARA FORTALECER EL SISTEMA DE SEGURIDAD
INFORMÁTICA Y CIBERSEGURIDAD FRENTE A ATAQUES CIBERNÉTICOS A
LOS SERVICIOS WEB DENTRO DE LA CAR CUNDINAMARCA**

Autores:

Edwin Alexander Gutiérrez Cely

Jeison Jair González Vargas

Ricardo Andrés Mikán Fajardo

Directores

German Macías Muñoz

Diego Osorio Reina

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
ESPECIALIZACIÓN EN GESTIÓN DE SERVICIOS DE TI
BOGOTÁ, AÑO 2022

Dedicatoria

Familia y equipo de trabajo del presente documento.

GUÍA CONTENIDO

1. PROBLEMA	12
1.1. ARBOL DE PROBLEMAS	14
1.2. QUE SE QUIERE SOLUCIONAR	15
2. IDEACIÓN DE LA SOLUCIÓN	16
2.1 POR QUÉ SE PLANTEA AHORA LA SOLUCIÓN	16
2.1.1. SECTOR OBJETIVO	17
2.1.2. DEFINIR EL SECTOR	18
2.1.3. DESCRIPCION DEL SECTOR	19
2.1.4. APLICACIONES DEL SECTOR.	20
2.1.5. LA RELACIÓN DE LAS APLICACIONES CON LA PROPUESTA.	21
2.1.6. TENDENCIAS DEL SECTOR	27
2.1.7. ANÁLISIS DE MERCADO	28
2.2. ARBOL DE OBJETIVOS	29
3. SITUACIÓN DESEADA	31
3.1 INTRODUCCIÓN A LA SITUACIÓN DESEADA	32
3.2 PROPUESTA DE VALOR	34
3.2.1. PERFIL DEL CLIENTE	35
3.2.2. MAPA DE VALOR	37
3.2.3. CLASIFICACIÓN DE TRABAJOS, FRUSTRACIONES Y ALEGRÍAS	37
3.2.4. LIENZO DE LA PROPUESTA DE VALOR	38
3.2.5. Definición Propuesta de Valor	39
4. ANÁLISIS DE LAS ALTERNATIVAS TÉCNICAS PARA SOLUCIONAR EL PROBLEMA	40
4.1 DIAGNOSTICO INTERNO PARA APROPIAR LAS TECNOLOGÍAS	40
4.2 ANÁLISIS DEL PROCESO DE TRANSFORMACIÓN DIGITAL	45
4.3. MÓDELOS DE PLATAFORMAS WAF	46
4.3.1. ¿Qué ES WAF?	46

4.3.2. WAF COMO SOFTWARE	46
4.3.2. WAF COMO PLATAFORMA FÍSICA	47
5.PROPUSTA DEL MODELO DE NEGOCIO, VALIDACIÓN DE MODELO NEGOCIO Y PROPUESTA DE LA SOLUCIÓN TECNOLÓGICA.	48
5.1. MODELO DE NEGOCIO	48
5.2. VALIDACIÓN MODELO DE NEGOCIO	52
5.3. PROPUESTA DE LA SOLUCIÓN TECNOLÓGICA	55
5.3.1. EVALUACIÓN Y PREPARACIÓN DE LA SOLUCIÓN	56
5.3.2. PRUEBAS DE LA SOLUCIÓN	57
5.3.3. DESPLIEGUE	59
5.3.4. OPTIMIZACIÓN DE LA SOLUCIÓN	64
6. ASPECTOS LEGALES Y CONTRATACIÓN	65
7. CONCLUSIONES	66
8. REFERENCIAS	67

GUÍA DE ILUSTRACIONES

Ilustración 1. Árbol de Problemas – Fuente Elaboración Propia	14
Ilustración 2 Pro Interno Bruto PIB – Fuente Internet: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi8hcW3ocD7AhWrUjABHfyUDl4QFnoECA8QAw&url=https%3A%2F%2Fwww.dane.gov.co%2Ffiles%2Finvestigaciones%2Fboletines%2Fpib%2Fbol_PIB_Iltrim22_prod	22
Ilustración 3 Crecimiento Pymes y Microempresas – Fuente Internet: Departamento de Estudios Económicos ACOPI https://www.acopi.org.co/estudios-economicos/	23
Ilustración 4 Datos TIC - Fuente Internet: DANE. Cu Satélite de las Tec. de la Información y las Comunicaciones (CSTIC) 2020pr. Consultado en línea marzo de 2021. Disponible en: https://www.dane.gov.co/files/investigaciones/pib/tic/bt-satelite-tic-2021pr.pdf	24
Ilustración 5 Actividades TIC Fuente Internet:DANE . Cuenta Satélite de las Tecno de la Información y las Comunicaciones (CSTIC) 2020pr. Consultado en línea marzo de 2021. Disponible en: https://www.dane.gov.co/files/investigaciones/pib/tic/bt-satelite-tic-2021pr.pdf	24
Ilustración 6 Árbol de Objetivos - Fuente Elaboración Propia	30
Ilustración 7. Pilares de Seguridad de la Información – Fuente Internet: https://www.lisot.com/que-es-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/	33
Ilustración 8 Beneficios de Protección a los Ataques WEB Avanzados – Fuente Internet: https://www.marquesme.com/que-es-un-waf-y-como-te-protege-de-ciberataques-a-tus-aplicaciones-web/	34
Ilustración 9. Perfil de cliente, Perfil del cliente y mapa de valor – Fuente Elaboración propia	36
Ilustración 10. Perfil del cliente mapa de valor – Fuente Elaboración propia	37
Ilustración 11. Clasificación de trabajos, frustraciones y alegrías. Fuente Elaboración propia	38
Ilustración 12. Lienzo de la propuesta de valor - Fuente Elaboración propia	39
Ilustración 13 Topología Base CAR Cundinamarca - Fuente, Elaboración Propia	43
Ilustración 14 Modelo de Sesión de Red - Fuente Internet: https://www.fortinet.com/lat/products/web-application-firewall/fortiweb	47
Ilustración 15. Plantilla Modelo Canvas. Fuente Elaboración propia	48
Ilustración 16: validación modelo de negocio pregunta 1	53
Ilustración 17 Validación modelo de negocio pregunta 2	53

Ilustración 18 Validación modelo de negocio pregunta 3	54
Ilustración 19: Validación modelo de negocio pregunta 4	54
Ilustración 20: Validación modelo de negocio pregunta 5	55
Ilustración 21: Validación modelo de negocio pregunta 6	55
Ilustración 22. Integración nativa plataformas de Seguridad – Fuente Internet: https://www.fortinet.com/lat/products/web-application-firewall/fortiweb	60
Ilustración 23. Modelo Proxy Reverso Ejemplo – Fuente Internet: (https://www.google.com/url?sa=i&url=https%3A%2F%2Fhelp.fortinet.com%2Ffw%2F561%2FContent%2FFortiWeb%2Ffortiweb-admin%2Fha.htm&psig=AOvVaw0v00S6ffwCvVAmvt0ygoCc&ust=1667066622433000&source=images&cd=vfe&ved=0CA0QjhxqFwo)	63

GUÍA DE TABLAS

Tabla 1 Sectores Económicos Colombia - Fuente Internet http://www.banrepcultural.org/blaavirtual/ayudadetareas/economia/econo53.htm	19
Tabla 2 Regulación TIC Seguridad Informática Perimetral - Fuente Internet....	27
Tabla 3 Aplicaciones WEB CAR - Fuente propia, tomado del levantamiento de información	42
Tabla 4 ETHICAL HACKING RESULTADO - Fuente propia, tomado del levantamiento de información	¡Error! Marcador no definido.
Tabla 5 Modelo Tabla de Signature -: Fuente Elaboración Propia.....	62

ACRÓNIMOS

MinTic. Ministerio de las Tecnologías de la Información y Comunicaciones.

Vulnerabilidades. Es un fallo o debilidad de un sistema de información que pone en riesgo la seguridad de esta.

WAF. En una solución tecnológica, que se asocia a los sistemas de seguridad de la información, dedicadas a la protección de servicios WEB, bloqueando amenazas en tiempo real, pero no generando falsos positivos basada en sus funcionalidades de auto aprendizaje.

Ciberseguridad. Práctica que se realiza al interior de las compañías para disminuir los elementos de red como las computadoras y los servidores, entre otros de ataques maliciosos.

Proxi Reverso. Se define como la dirección de destino para los reenvíos

MACHINE LEARNING. Tecnología basada en Inteligencia Artificial que se basa en algoritmos para generar en los computadores la capacidad de aprender y conocer patrones predictivos.

Firewall. software o componentes de hardware que depuran y examinan la información que viaja a través de su conexión a Internet.

IA. La Inteligencia Artificial es la mezcla de algoritmos y código de desarrollo que busca crear máquinas que funcionen similar a la mente humana

Topología. Son las capas física o lógica de la red para intercambiar información

WEB. Conjunto de información que se encuentra en una dirección determinada de internet.

ETHICAL HACKING. Se conoce como pruebas de penetración, se realizan cuando de manera legal se busca encontrar una vulnerabilidad en equipos de

red de manera que se evalúen las defensas con las que cuenta una compañía a nivel de red.

IPS (Intrusion Prevention System): se define como sistema de prevención de intrusos, es una tecnología que vigila una red para descubrir actividades anómalas que intente atacar las vulnerabilidades.

Seguridad Informática: está enfocada a la al manejo correcto de la información y tratamiento que se hace sobre dicha información, con el objetivo de evitar el tratamiento de datos y procesos por usuarios no autorizadas.

Appliance. Dispositivo Componente hardware diseñado específicamente para proporcionar un recurso de computación.

Red Corporativa. red interna de la entidad que brinda soporte tanto a hardware como a software.

RESUMEN

La infraestructura tecnológica de la CAR Cundinamarca (Corporación Autónoma Regional de Cundinamarca) ha presentado un crecimiento exponencial en todos sus frentes, sujeto a la adopción de los lineamientos y normativas, gobernanza de seguridad digital, la identificación de infraestructuras críticas, gestión de riesgos y la respuesta a incidentes de seguridad, modelos de seguridad y privacidad de la información y todos aquellos lineamientos y normativas nacionales de políticas de gobierno digital.

Aunque la CAR cuenta con sistemas y medidas de seguridad perimetral, pueden llegar a ser limitados para nuevas modalidades de ciberdelincuencia y al constante desarrollo de herramientas que facilitan los ciberataques. Con el fin de reducir el riesgo de ataques, mitigar vulnerabilidades de los sistemas de información y fortalecer las medidas existentes en las plataformas de seguridad informática perimetral, se quiere implementar controles que protejan los portales WEB basados en soluciones WAF en modalidad de proxy reverso que mitiguen ataques a estos entornos que puedan afectar los servicios de la corporación, y que adicional cuenten con funcionalidades de supervisión y control de eventos.

La integración tecnológica que abarca la atención de esta necesidad, de protección del entorno de los sistemas de información de la entidad, como adopción de las regulaciones actuales y vigentes emitidos por gobierno, comprenden un desarrollo o actualización tecnológica para la Corporación. La integración nativa de la solución WAF con la solución de Firewall perimetral actual entregará información de estadísticas reales que comprenden el soporte de sustento a la necesidad, pero es necesario que, acompañado a este proceso de actualización tecnológica, se generen pruebas de vulnerabilidades a estos sistemas de información como servidores físicos o virtuales en los cuales se alojan las aplicaciones, para dar un punto de partida a la remediación a la necesidad general de proteger los sistemas de información WEB.

ABSTRAC

The CAR's technological infrastructure Cundinamarca (Corporación Autónoma Regional de Cundinamarca) has shown an exponential increase, all of this aligned with regulations, digital security, risk management, and satisfy in security, security models and information privacy and whole guidelines and national rules.

Although, La CAR has perimeter security measures, these measures can be insufficient and restricted for new cyber-attacks methods and continuous development of tools that help to cybercriminals to infringe all security measures. To reduce the attack risk, reduce information system vulnerabilities and strengthen existing measures inside the security web platforms, the technical team propose tools that protect web sites base on WAF solutions which reduce attacks on web environments and can affect the corporation's services, in addition tools that be able to supervise and monitor events.

The implemented measures bring technological upgrade inside of organization, with the integration of WAF with currently perimeter security take information and statistics in real time that accomplish the need, on the other hand it is necessary that the team make test vulnerabilities to start the protection whole web infrastructure.

INTRODUCCIÓN

Las áreas de tecnología de las entidades de gobierno deben estar en capacidad de asegurar que la infraestructura, y los servicios de TI internos como externos no estén expuestos a ataques que comprometan la información que manejan ni el funcionamiento integral de las aplicaciones.

Dentro del documento, se propone una solución que cuenta con tecnología actual para ayudar a prevenir el riesgo de fuga de información la cual afecta el buen desempeño de las TICs en los procesos de la entidad, permitiendo a la CAR ofrecer a sus usuarios mejorar la experiencia de los servicios actuales mediante ayudas tecnológicas.

Desde la CAR Cundinamarca se tiene claro que dentro de la transformación digital se cuentan con activos sumamente importantes como los bienes físicos y digitales como la infraestructura TI, pasando por a la información, los datos, los servicios WEB, entre otros, conociendo que con la misma transformación digital estos elementos pueden ser consultados, almacenados y modificados desde y en cualquier sitio, y es de suma importancia preservar la integridad y la seguridad de estos elementos.

Adicionalmente el sector público ha promovido el uso de tecnologías, estándares y normas aplicables, asegurando con estas una gestión ajustada al manejo que requiere la información, con el fin de hacer más eficiente la utilización de los recursos físicos, humanos, financieros y demás que manejan las entidades, con lo cual se ha guiado esfuerzos hacia la ampliación y modernización de la infraestructura tecnológica, y el fortalecimiento de los esquemas de seguridad informática.

Del mismo modo la ciberseguridad ha crecido y evolucionado respondiendo a los retos planteados por la sociedad en los últimos años. Constantemente estamos viendo nuevos desafíos a la protección de la confidencialidad, disponibilidad e

integridad de la información, así como a la protección de la infraestructura que la soporta.

Dentro del presente documento se plantea la necesidad de implementar un WAF que permitan aumentar el nivel de seguridad de los servicios WEB y del mismo modo genere madurez en cuanto a ciberseguridad de la entidad logrando que se proteja la información, activos críticos y a los usuarios de los posibles ataques de los cuales puedan ser víctimas, y de las consecuencias que traen estos ataques.

Posteriormente se muestran algunas de las vulnerabilidades que han sido reconocidas en los escaneos de seguridad, y con los cuales se genera un precedente de los ataques que pueden comprometer los servicios WEB a través de ataques avanzados de malware (programa maligno), o ataques de día cero como lo puede ser Rasonware. De igual forma, es de suma importancia tener en consideración lo recomendado en las directrices del gobierno nacional, mediante el ministerio TIC y las recomendaciones de fabricantes y normas ISO aplicables a ciberseguridad.

1. PROBLEMA

La CAR Cundinamarca [1] actualmente tiene un débil sistema de seguridad informática y ciberseguridad frente a ataques cibernéticos a los servicios WEB, situación que se refleja en la ausencia de plataformas dedicadas a esta funcionalidad de protección específica, y que adicional entregue funcionalidades de automatización que permitan el análisis de información y generación de información y de remediación basado en tecnologías de transformación digital como IA y MACHINE LEARNING [2]. Esta información se relaciona en el documento anexo a este proyecto, que se nombra “*Levantamiento de información.pdf*” y que parte de su contenido como justificación será desarrollada también en este documento en el numeral 3.1 DIAGNOSTICO INTERNO PARA APROPIAR LAS TECNOLOGÍAS.

El incremento de logs (historial de eventos cibernéticos, en este caso capturados por el Firewall perimetral), de los ataques informáticos, que se encuentran dentro de la información correlacionada, muestra una etapa inicial de escaneo sigiloso con el uso de plataformas de enumeración de puertos y búsqueda de vulnerabilidad a los sistemas operativos, como los motores de ejecución de la aplicación, información que se encuentra en el anexo “*logs de escaneos.xlsx*”.

Así mismo, la desactualización informática que existe en la infraestructura respecto a las versiones de motores de las BD (bases de datos), como en los sistemas operativos de fabricantes Linux como Windows Server, que ya no cuentan con soporte ante los fabricantes, y que no es tema ajeno al conocimiento general del equipo de TI (equipo de ingenieros de tecnologías de información de la OTIC CAR). Lo anterior, ha generado a la Corporación, que en medio de la ejecución de las pruebas de ETHICAL HACKING, se aumente significativamente el número de vulnerabilidades, lo cual se asocia a los parches de sistema

operativo, parches de seguridad y otros componentes que ligan al componente de software.

Todos estos resultados cuantificables, son parte integral del estudio técnico de apalancamiento que busca suplir la necesidad que se relaciona en este documento, en el cuál, la necesidad de proteger los sistemas de información del entorno WEB, se cobijan en la adopción de buenas prácticas enmarcadas en un Hardening (fortalecimiento de sistemas informáticos) [8] a todo el entorno de WEB services, que garantice la estabilidad y protección anhelada.

La reputación de la CAR Cundinamarca, respecto a la protección y garantía del uso de los sistemas de información para el acceso interno como externo, a los usuarios internos y públicos, genera la necesidad de fortalecer la infraestructura, de modo que se omitan las posibles fugas, encriptado o robo de información misional, así como, la necesidad de omitir que ciberdelincuentes editen los portales WEB de la CAR motivados por los bajos controles y sistemas de seguridad. Lo anterior se sustenta en el anexo *“Levantamiento de información.pdf”*.

1.1. ARBOL DE PROBLEMAS

Actualmente la CAR Cundinamarca presenta la necesidad de proteger sus portales WEB, sistemas de información, en su entorno interno como externo.

En la siguiente ilustración se presenta la identificación del problema general identificado, respecto a la exposición de los aplicativos WEB, partiendo en la partiendo inferior de las causas que inherentemente generan vulnerabilidad a estas plataformas de información de manera indirecta y directa, y hacia la parte superior se presentan los efectos que inicialmente se presentan como posibles eventos que si llegan a materializar afectan la integridad de la CAR en sus ámbitos tecnológicos como reputacionales.

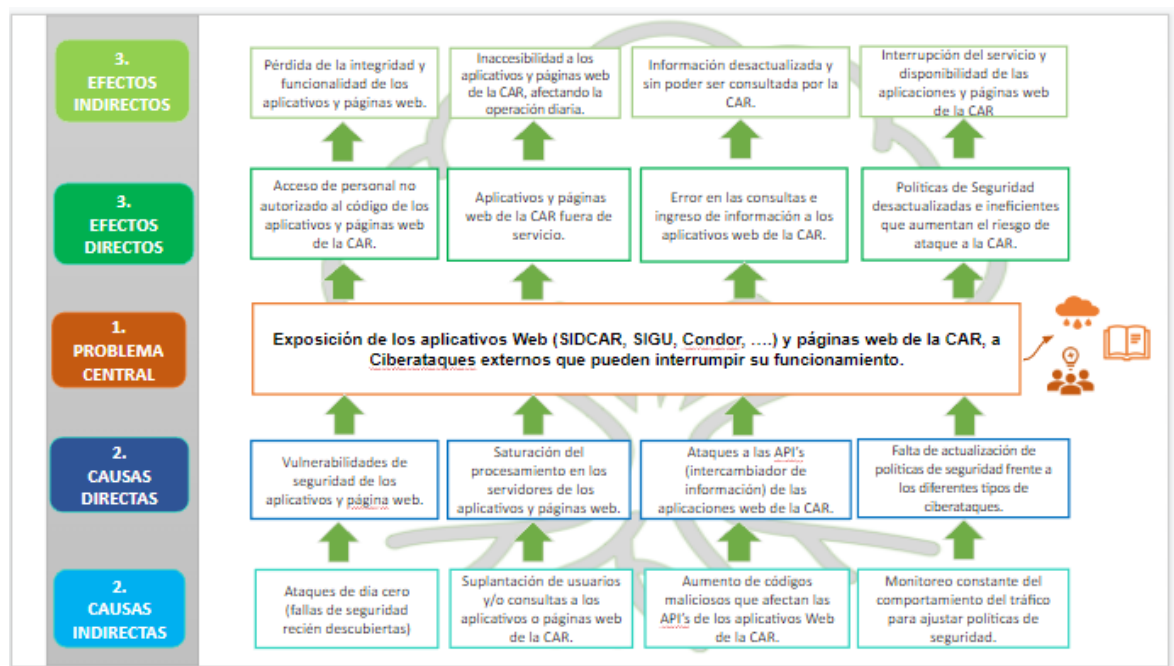


Ilustración 1. Árbol de Problemas – Fuente Elaboración Propia

1.2. QUE SE QUIERE SOLUCIONAR

En la creciente transformación digital, que está presente en la actualidad tecnológica de la humanidad, se evidencia como la ciberdelincuencia se actualiza en un grado similar o mayor a la transformación y/o actualización tecnológica.

La exposición de los aplicativos Web (SIDCAR, SAE, ORION, Página WEB de la CAR, NegociosVerdes, Geoambiental, EVA, Singelia, SIGU, Condor y otras) y páginas web de la CAR, a Ciberataques, son el problema principal que el presente proyecto busca atacar brindando una solución a la Corporación, en donde sean mitigados los riesgos contenidos en la vulnerabilidad o exposición tecnológica que como evento interrumpirán el funcionamiento, generarán posibles fugas o robos de información, así mismo, posibles ingresos de virus que encripten información alojada en los entornos WEB, y que como solución a la necesidad se logre mitigar la vulnerabilidad asociada a la reputación de la Corporación respecto a la exposición de los sistemas de información.

El fin común del presente proyecto, ataca el dimensionamiento técnico propuesto para la protección de los portales WEB de la CAR, respecto al diseño, implementación y apropiación de plataformas que en su característica técnica acoja tecnologías de inspección de código en los cuales automáticamente en tiempo real se liste falencias de las aplicaciones y por medio de tecnologías de machine Learning e inteligencia artificial se cuente con el autoaprendizaje del comportamiento y uso de las plataformas, para así, emitir protección de tiempo respecto a las sesiones TCP/IP que se establecen hacia el usuario final.

2. IDEACIÓN DE LA SOLUCIÓN

2.1 POR QUÉ SE PLANTEA AHORA LA SOLUCIÓN

Los riesgos a los que está expuesta la infraestructura de TI y los sistemas por las amenazas internas y de Internet en la red de datos de Corporativas obliga a monitorear y responder con servicios inteligentes para contrarrestar el tráfico de ataques e interferencia que afecte la operación de los servicios informáticos. Las amenazas desde internet han evolucionado a formas complejas de ataque que requieren del uso de inteligencia artificial para el aprendizaje del comportamiento y la identificación de actividad maliciosa.

Para contar con una nueva capacidad de respuesta inteligente ante actividad maliciosa o sospechosa se plantea disponer de los servicios de inteligencia en el tráfico de red por accesos WEB para identificar variaciones de patrones de tráfico de cada sistema que le permitan mejorar el aseguramiento el cual reduzca el riesgo de afectaciones a la operación y con repercusiones en los servicios misionales de la CAR Cundinamarca.

Por lo tanto, es necesario contar con una plataforma que enfoque su funcionamiento en inteligencia artificial y aprendizaje no supervisado que se enfoque cien por ciento a esta funcionalidad. Esta plataforma no depende de gestión o administración, respecto al aprendizaje y control de la plataforma.

El administrador de estas plataformas utiliza las funcionalidades de auto aprendizaje cuando realiza la etapa de inclusión del sistema de información a la protección WEB, así genera una configuración inicial basado en las

características del sistema de información y activan perfiles de protección web que mediante Machine Learning [3] escucha el comportamiento de la aplicación, y va conociendo el monitoreo del tráfico entrante basado en las conexiones de usuarios finales, para pasar posteriormente a un ambiente de control en el ambiente seguro.

En el ambiente de monitoreo luego de todo el aprendizaje hecho por la solución sobre la aplicación, será usada en su fase segura para mitigar o realizar análisis en tiempo real. Con la adopción de esta plataforma, la CAR podrá atender sus responsabilidades en cuanto a ciberseguridad para mejorar su capacidad de prevenir y detectar oportunamente los incidentes y ataques de seguridad y contrarrestar de forma efectiva la indisponibilidad de los servicios de los sistemas que soportan los servicios misionales de la entidad que pueden surgir como resultados de amenazas cibernéticas internas y desde Internet, que se amparan como evidencia en el anexo “*Levantamiento de información.pdf*” [3].

2.1.1. SECTOR OBJETIVO

A nivel del manejo de la información, control de acceso a la información y datos abiertos en el sector Gobierno, se crea la necesidad en las entidades de contar con un sistema de control y manejo de la información basado en la normatividad estándar que comprende la norma ISO 27032 de 2014, el cual para contar con sus políticas establecidas es necesario complementar con una arquitectura de seguridad informática perimetral. El presente documento detalla el diseño tecnológico propuesto para la protección de los portales WEB de la CAR Cundinamarca (Corporación Autónoma Regional de Cundinamarca), respecto a la presentación de la información misional de la entidad hacia la Internet, como en su Red Corporativa interna.

Con el conocimiento de la necesidad de la CAR, en el cual se ataca la necesidad de corregir la vulnerabilidad y protección ante ciberdelincuencia de los servicios WEB, y el objeto del proyecto se ha tipificado como *“PROPUESTA PARA FORTALECER EL SISTEMA DE SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD FRENTE A ATAQUES CIBERNÉTICOS A LOS SERVICIOS WEB DENTRO DE LA CAR CUNDINAMARCA”* y con el estudio de los sectores económicos así como el estudio hecho bajo el levantamiento de información de la gestión administrativa de la CAR Cundinamarca que es regida bajo el control ambiental del Ministerio del Medio Ambiente.

La actividad económica en nuestro país se divide básicamente en tres sectores, y cada uno esta enfocado en actividades de objetivo comunes, que se pueden entender como una unidad, mientras que su división se realiza de acuerdo con los procesos de producción con los que se cuenta al interior de cada uno.

2.1.2. DEFINIR EL SECTOR

Los sectores de la economía son los siguientes, como se muestra en la siguiente ilustración:

SECTORES ECONOMICOS	DEFINICION	ACTIVIDADES DEL SECTOR
SECTOR PRIMARIO O AGROPECUARIO	Es el sector que obtiene el producto de sus actividades directamente de la naturaleza, sin ningún proceso de transformación. Dentro de este sector se encuentran la agricultura, la ganadería, la silvicultura, la caza y la pesca. No se incluyen dentro de este sector a la minería y a la extracción de petróleo, las cuales se consideran parte del sector industrial	Agropecuario, caza y pesca
SECTOR SECUNDARIO O INDUSTRIAL	Comprende todas las actividades económicas de un país relacionadas con la transformación industrial de los alimentos y otros tipos de bienes o mercancías, los cuales se utilizan como base para la fabricación de nuevos productos. Se divide en dos sub-sectores: industrial extractivo e industrial de transformación: INDUSTRIAL EXTRACTIVO: Extracción minera y de petróleo. INDUSTRIAL DE TRANSFORMACIÓN: Envasado de legumbres y frutas, embotellado de refrescos, fabricación de abonos y fertilizantes, vehículos, cemento, aparatos electrodomésticos, etc	Sector Minería
		Sector Construcción
		Sector Industria manufacturera
		Sector eléctrico, gas y vapor
SECTOR TERCIARIO O DE SERVICIOS	Incluye todas aquellas actividades que no producen una mercancía en sí, pero que son necesarias para el funcionamiento de la economía. Como ejemplos de ello tenemos el comercio, los restaurantes, los hoteles, el transporte, los servicios financieros, las comunicaciones, los servicios de educación, los servicios profesionales, el Gobierno, etc.	Sector Transportes
		Sector comunicaciones
		Sector comercio, restaurante y hoteles
		Sector Financiero

Tabla 1 Sectores Económicos Colombia - Fuente Internet
<http://www.banrepcultural.org/blaavirtual/ayudadetareas/economia/econo53.htm>

En razón a esta ilustración anterior, el Sector Terciario involucra aquellas actividades que no necesariamente generan mercancía en sí, pero que, en su desarrollo, genera implícitamente el apoyo necesario para el funcionamiento de la economía; para este caso específico podemos hablar de capas inferiores como de las comunicaciones y las telecomunicaciones, respecto al apoyo en la transferencia de información, los servicios de educación, los servicios profesionales, el gobierno en los campos informáticos de toda índole, entre otros. [4]

2.1.3. DESCRIPCION DEL SECTOR

La información presentada en la decisión del sector hace parte integral de la consignación para la contratación pública regida en Colombia Compra. Esta información incorpora un análisis de los aspectos generales, una contextualización de la oferta y una descripción de la demanda presentes en el sector terciario.

En este desarrollo se revisarán los aspectos del mercado relacionados con el sector de servicios de apoyo de Tecnologías de Información y Comunicaciones – TIC, para lo cual se revisan los siguientes contextos:

- **Económico:** Esta es una breve descripción del sector, que comprende los agentes, gremios y asociaciones que lo componen, y como las variaciones pueden ocasionar impacto.
- **Técnico:** Se describen las principales características de los servicios de Tecnologías de Información y Comunicaciones - TIC, y que presentan injerencia en el desarrollo tecnológico.
- **Regulatorio:** Son identificados en el marco de regulación aplicable al proceso de contratación, que es aplicada al presente documento o al objeto del Contrato que se ampara en la Ley 80. [5]

2.1.4. APLICACIONES DEL SECTOR.

El desarrollo dentro del Sector Terciario abarca un campo de acción enorme, respecto a servicios.

Para este caso, todo el desarrollo del estudio técnico, como económico, basado en su injerencia y afectación en los campos de acción permiten abarcar de manera global la implementación de plataformas de seguridad en razón a activos fijos de adquisición de la CAR Cundinamarca, para su campo TIC, y de esto modo, de manera conjunta incluir servicios de ingeniería de implementación como su licenciamiento y parches de firmware de ejecución respecto a las funcionalidades necesitadas en atención de implementación de la solución presentada, como objetivo de solución a la necesidad encontrada.

2.1.5. LA RELACIÓN DE LAS APLICACIONES CON LA PROPUESTA.

La sociedad se enfrenta hoy en día cada vez más a la evolución y el desarrollo de las tecnologías de la información y las comunicaciones, que se ligan a factores de protección de datos. El desarrollo de la tecnología permite facilitar la conexión o comunicación en tiempo real en ubicaciones geográficas muy retiradas. Así mismo, el avance tecnológico en el almacenamiento y procesamiento de la información ha permitido darle mayor uso a la información, desarrollando análisis cada vez más complejos y permitiendo aumentar la productividad de la economía, basado en la transformación de procesos, por medio de los avances tecnológicos, que vienen sujetos a las tecnologías emergentes de la industria 4.0. [5]

La transformación digital que usa tecnologías de analítica de datos genera el soporte verificable de las estadísticas y datos que confirman que las TIC incrementan el índice de crecimiento de la productividad y cumplimientos de objetivos, que han permitido mejorar la vida y desarrollo organizacional de las empresas, del mismo modo las administraciones públicas y el desarrollo de los ciudadanos en general. Es tan importante el avance tecnológico que su papel relevante en la sociedad actual, ha generado que diversos autores denominen esta como la era de la información o la sociedad de la información, que se liga para el presente estudio en la protección de la información y reputación de la CAR Cundinamarca, respecto al acceso y presentación de la información.

Como soporte al presente documento de estudio del sector económico, se han tomado los siguientes aportes del IPC (índice de Precios al Consumidor), PIB (resultado de la actividad productiva de las unidades de producción), para 2022, que son tomados de los estudios del DANE.

Para el campo económico, de acuerdo con el Boletín técnico del DANE, Producto Interno Bruto (PIB) II Trimestre 2022, de fecha 16 de agosto de 2022, las cuentas trimestrales se soportan en los estándares internacionales de medición económica definidos por la Organización de Naciones Unidas y el Fondo Monetario Internacional. [6]

La información estadística que se indica a continuación fue consultada a agosto de 2022 así:

II trimestre 2022 preliminar
Gráfico 1. Producto Interno Bruto (PIB)
Tasas de crecimiento en volumen1
2016-I / 2022pr -I

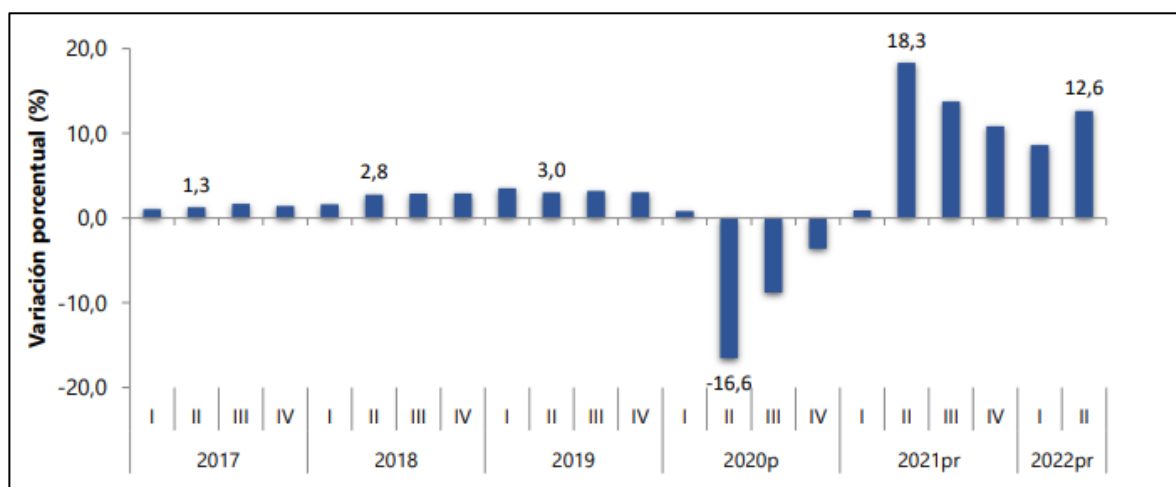


Ilustración 2 Pro Interno Bruto PIB – Fuente Internet:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi8hcW3ocD7AhWrUjABHfyUDI4QFnoECA8QAw&url=https%3A%2F%2Fwww.dane.gov.co%2Ffiles%2Finvestigaciones%2Fboletines%2Fpib%2Fbol_PIB_Iltrim22_prod

La Asociación Colombiana de las Micro, Pequeñas y Medianas Empresas – ACOPI, presentó los resultados de la Encuesta de Desempeño Empresarial, para el primer trimestre del año 2020. Algunos de los indicadores analizados son capital humano, comercio exterior, empleo, inversión, productividad y ventas. De la misma forma, se genera un sondeo con los afiliados del gremio en los temas relevantes y se hace posteriormente el comparativo de indicadores con respecto al mismo periodo del año anterior.

- El 74% de pequeñas y medianas empresas no invirtió durante el primer trimestre de 2020, si se compara con el mismo trimestre del 2019, de esta forma siguen mostrando un decrecimiento en la inversión, dado que el mismo trimestre del año anterior se observó inversiones un 37% mayores.
- Dado el periodo de pandemia, el 35% de pymes y el 33% de microempresarios afirmaron que el nivel de afectación en sus ventas e ingresos por causa del COVID-19 superaron el 75%, mientras que el 32% considera que el nivel de desface puede oscilar entre un 51% y 75%. El país cumplió en ese momento un mes de permanecer en cuarentena obligatoria, las actividades comerciales estuvieron limitadas por lo tanto las estadísticas de deterioro llegaron a un estado difícil de revertir. [7]



Ilustración 3 Crecimiento Pymes y Microempresas – Fuente Internet: Departamento de Estudios Económicos ACOPI <https://www.acopi.org.co/estudios-economicos/>

Dentro del campo técnico, según la Cuenta Satélite de las Tecnologías de la Información y las Comunicaciones (CSTIC), el valor agregado de las TIC ascendió a 40.2 billones de pesos, presentando un crecimiento total de 10.1% en el año 2021 mientras que en 2020p el valor agregado fue de 36,5 billones de

pesos, con un crecimiento de 2,5% con respecto a 2019. Así mismo el sector TIC en los últimos años se ha venido teniendo un comportamiento ascendente en lo que se refiere a la participación al valor agregado nacional 4, tal como se observa en el siguiente gráfico [8].

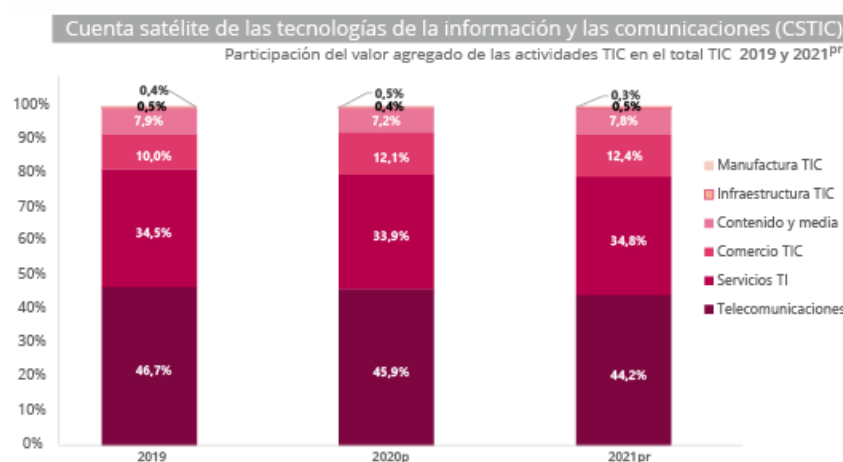


Ilustración 4 Datos TIC - Fuente Internet: DANE. Cu Satélite de las Tec. de la Información y las Comunicaciones (CSTIC) 2020pr. Consultado en línea marzo de 2021. Disponible en: <https://www.dane.gov.co/files/investigaciones/pib/tic/bt-satelite-tic-2021pr.pdf>

El sector TIC para 2021pr registró una participación de 3,8% con respecto al valor agregado nacional, para 2020p esta participación fue de 4,0% mientras que para el período 2019 – 2021pr en promedio participó con el 3,8% del valor agregado nacional. [8]

Actividad Característica TIC	2019	2020 ^P	2021 ^{Pr}
Telecomunicaciones	46,7	45,9	44,2
Servicios TI	34,5	33,9	34,8
Comercio TIC	10,0	12,1	12,4
Contenido y Media	7,9	7,2	7,8
Manufactura TIC	0,5	0,4	0,5
Infraestructura TIC	0,4	0,5	0,3
Total Sector TIC	100,0	100,0	100,0

Fuente: DANE - Ministerio de Tecnologías de la Información y Comunicaciones. Cuenta Satélite TIC

^P provisional

^{Pr} preliminar

Ilustración 5 Actividades TIC Fuente Internet: DANE . Cuenta Satélite de las Tecno de la Información y las Comunicaciones (CSTIC) 2020pr. Consultado en línea marzo de 2021. Disponible en: <https://www.dane.gov.co/files/investigaciones/pib/tic/bt-satelite-tic-2021pr.pdf>

Basado en este estudio, y con la información levantada en la red de la CAR, se detalla la necesidad de crecimiento y protección de los activos de información, respecto al permiso de acceso a los recursos tecnológicos internos como externos.

La arquitectura de seguridad informática corresponde a la base de seguridad por capas. La capacidad de contar con una solución que permitiera a la entidad correlacionar los diferentes eventos y registros de seguridad que se generan en la red, en una única ventana de monitoreo.

Dentro del ámbito regulatorio en la siguiente tabla se presenta la información que abarca el sector económico escogido, y la regulación que los abarca:

NORMATIVIDAD	DETALLE
Ley 80 de 1993 [9]	Estatuto General de la Contratación. [9]
Decreto 1151 de 2008 - MINTIC / Gobierno en Línea [9]	se comprenden los lineamientos generales del plan estratégico para el desarrollo del Gobierno en Línea, bajo Ley 962 de 2005. En el CONPES 3650 de 2010 / Gobierno en Línea. [9]
Ley 1150 de 2007 [9]	Comprende la ley de transparencia, en la ley 80 de 1993. [9]
Ley 1273 de 2009 [9]	Se comprende “la ley de protección de la información y de los datos”. [9]
Ley Estatutaria 1581 de 2012 (Reglamentada parcialmente por el Decreto Nacional 1377 de 2013) [9]	“Se dictan disposiciones generales para la protección de datos personales”. [9]
Decreto 1082 de 2015 [9]	"sector administrativo de planeación nacional" [9]
Decreto 415 DE 2016 [9]	comprende la función pública decreto N° 1083 de 2015, para el fortalecimiento institucional en la materia de tecnologías información y las comunicaciones. [9]
Decreto 1360 De 1989 [9]	Se reglamenta la inscripción al Registro Nacional del Derecho de Autor. [9]

Gobierno en línea [9]	Comprende las metas ○ Meta 1: Gobierno para el ciudadano ○ Meta 2: Un gobierno interconectado ○ Meta 3: Un sistema estadístico y un mapa nacional de registros ○ Meta 8: Incentivar la generación, difusión y uso de la información. [9]
Ley 1221 de 2008 / Teletrabajo. [9]	Normatizar el teletrabajo. [9]
CONPES 3670 de 2010 - DNP / Acceso y Servicio Universal. [9]	Promover el acceso, uso y aprovechamiento de las TIC, de manera coordinada entre los programas del Ministerio de Tecnologías de la Información y las Comunicaciones. [9]
VISIÓN COLOMBIA 2019 [9]	Comprende: Meta 6: Desarrollar capacidades en la población para el uso y la apropiación de las TIC [9]
Ministerio de Tecnologías de la Información y las Comunicaciones. Decreto 338 de 2022 8 marzo 2022: [9]	Fortalecer la Gobernanza de la Seguridad Digital, Gestión de Riesgos y la Respuesta a Incidentes de Seguridad Digital. [9]
Ministerio de Tecnologías de la Información y las Comunicaciones. Resolución 746 de 2022. 11 de marzo de 2022 [9]	Se Fortalece el [9] Modelo de Seguridad y Privacidad de la Información
Ministerio de Comercio, Industria y Turismo Decreto 255 de 2022 23 de febrero de 2022 [9]	Certificación de buenas prácticas en protección de datos personales [9]
Presidencia de la Republica Directiva Presidencial 02 de 2022 24 de febrero de 2022 [9]	Implementar estrategias de seguridad digital con políticas, procedimientos, guías y lineamientos para la gestión de la información de la seguridad digital de conformidad con el modelo de seguridad y privacidad de la información (MSPI) dispuesto por MINTIC. [9]
Ley 3 de 1961 y 99 de 1993 [9]	Mediante las cuales se crea y reglamenta la Corporación Autónoma Regional de Cundinamarca – CAR, se establece que entre sus funciones legales se encuentran las de ejecutar, administrar, operar y mantener proyectos y programas de desarrollo sostenible para la recuperación del medio ambiente y los recursos naturales renovables en el área de su jurisdicción. [9]
Resolución 2710 de 3 de octubre de 2017	Adopción del protocolo IPv6". [9]

Ministerio de Tecnologías de la Información y Las Comunicaciones [9]	
Decreto 1008 de 2018 de 14 de junio de 2018 del Ministerio de Tecnologías de la Información y Las Comunicaciones [9]	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" [9]

Tabla 2 Regulación TIC Seguridad Informática Perimetral - Fuente Internet

2.1.6. TENDENCIAS DEL SECTOR

El auge de la industria 4.0 como la transformación digital, traen consigo el desarrollo de tecnologías como la IA (Inteligencia Artificial) y Machine Learning, que al ser usados como complemento en las plataformas de seguridad crean soluciones de alta relevancia y valor administrativo, generando productos de autoaprendizaje y auto remediación y en un grado aún más eficaz, logrando consolidaciones tecnológicas eficaces en los entornos corporativos.

Los términos que empiezan a ser usuales cuando se habla de ciberseguridad se enfocan en cero confianza (ZERO TRUST), XDR (Extended Detection & Response), y algunas herramientas de Cyber IA, como Next-Gen Security [3] [10] Operations, Profile Web Protection, Bot, Anomaly detection, y Content Routing, empiezan a ser más comunes en el entorno de ciberseguridad.

La protección en tiempo real genera la necesidad de automatizar los procesos, omitiendo gestiones administrativas por usuarios del rol de administrador, basado en la necesidad de contener las amenazas que se transportan en medio de una Red Corporativa, y que explotan vulnerabilidades sin ningún control, dejando solo un rastro en el log del evento o acción realizada, más no contenida. La actualidad tecnológica, como ya lo indicamos, integra tecnologías a los servicios de seguridad informática perimetral, que están activas en modelo de

protección de tiempo real buscando los vectores de vulnerabilidades en términos [3] como Bot detection, Machine Learning templates, anomaly detection, Bot Mitigation, HTTP Flood Prevention. [3] [10]

Al final del día, el ámbito tecnológico, sin importar el sector económico de desarrollo, demandan en todos los aspectos la implementación de soluciones de seguridad que garanticen o brinden confianza en el entorno de acceso a la información bajo la intención de cumplir con los pilares fundamentales de la seguridad de integridad, disponibilidad, confidencialidad y autenticidad de la información. [3] [10]

2.1.7. ANÁLISIS DE MERCADO

Teniendo en cuenta las características que presta la solución presentada para brindar seguridad en aplicativos Web usando WAF, es válido decir que el campo de implementación es amplio dado que puede ser ejecutado en cualquier compañía que cuente con altos estándares de seguridad TI y protección a sus servicios Web:

- **Mercado Objetivo**

El mercado objetivo para la implementación es en entidades dentro del sector público que tengan las mismas capacidades de tecnología, seguridad, personal y presupuesto similar a la CAR Cundinamarca, y del mismo modo con las MiPymes, y empresas donde se tenga constantemente servicios Web expuestos a Internet, con alto volumen de tráfico y que requieran alto nivel de seguridad de la información como pueden ser: MINTIC (Ministerio de las Tecnologías de la Información y las Comunicaciones de Colombia), FEDESOFTEC La Federación Colombiana de la Industria del Software y Tecnologías Informáticas

Relacionadas, y CINTEL (Centro de Desarrollo Tecnológico orientado a la investigación aplicada),entre otros.

- **Donde se ubica el cliente**

Para la descripción puntual del cliente, esta se encuentra en el numeral 3.3 PERFIL DEL CLIENTE.

Sin embargo, cabe resaltar que se puede implementar en compañías establecidas en varios campos de trabajo como: Sector TIC público y privado, compañías de software, sector bancario, y demás compañías que requieran altos niveles de seguridad.

2.2. ARBOL DE OBJETIVOS

Evitar la exposición de los aplicativos Web (SIDCAR, SAE, ORION, Página WEB de la CAR, NegociosVerdes, Geoambiental, EVA, Singelia, SIGU, Condor y otras) y páginas web de la CAR, a ciberataques que pueden interrumpir su

funcionamiento y el acceso a la información en donde la reputación de la Corporación e información misional sea expuesta.

En la siguiente ilustración se presenta el árbol de objetivos general del presente proyecto, en el cual de manera ascendente los deseos indirectos y directos, que nos llevan abarcar el propósito general.

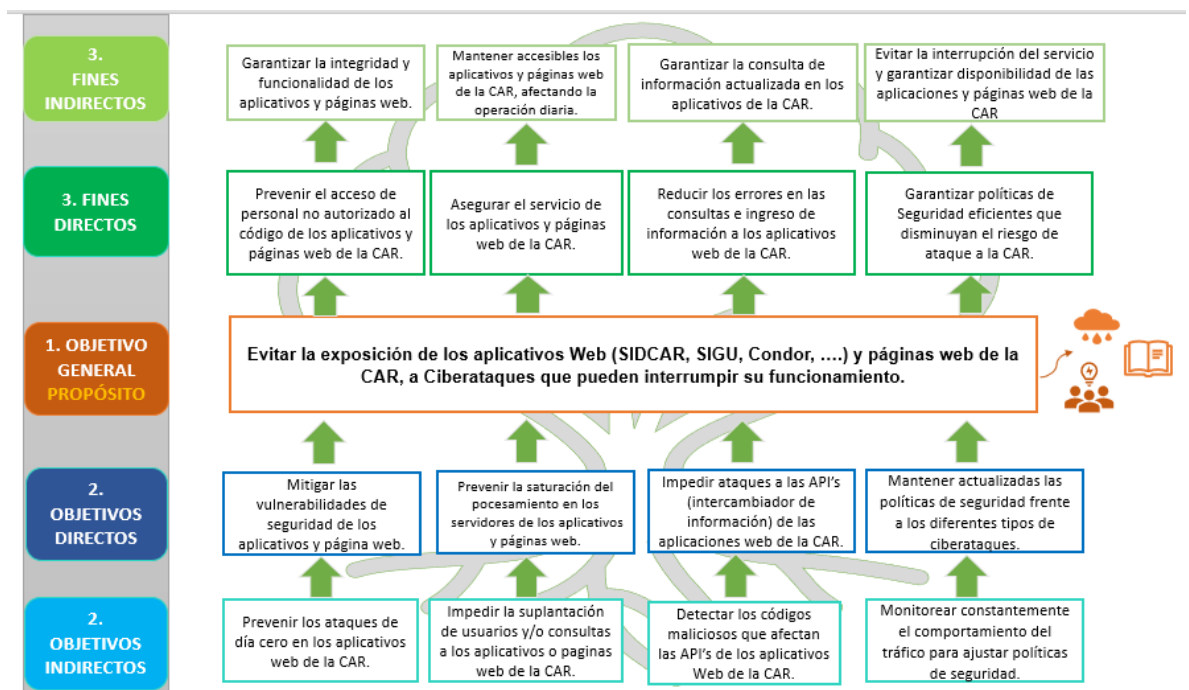


Ilustración 6 Árbol de Objetivos - Fuente Elaboración Propia

3. SITUACIÓN DESEADA

Dentro del campo de TI siempre se quiere tener el máximo nivel de seguridad que proteja los activos de la compañía, tanto equipos, servicios e información, debido a las vulnerabilidades existentes.

En este caso, dentro de la CAR Cundinamarca requiere mitigar al máximo las vulnerabilidades y la exposición de los aplicativos WEB a ciberataques, usando WAF Fortinet que se integre nativamente al Firewall FORTIGATE 1100 E perimetral, que ya existe en la Corporación, el cual ofrece protección en aplicaciones Web y en APIs, y mitigación de BOT.

En el caso ideal, las características que presta el WAF [3] de forma general se encuentra el bloqueo de las amenazas en tiempo real sin afectar a los usuarios legítimos y sin generar falsas alarmas (falsos positivos). A nivel de API proporciona una puerta de enlace que presta un único punto de entrada para el acceso. De igual forma mantiene oculta la estructura interna de la API de posibles atacantes, protegiendo el código. Para el nivel de usuario ofrece una experiencia mejorada en diferentes dispositivos sin poner en riesgo la seguridad. A nivel Web bloquea las amenazas mediante protección de ataques DDOS (Denegación de Servicio), validación de protocolos de red, entre otras características, mientras escanea vulnerabilidades en los aplicativos o en tiempos programados anteriormente.

Realiza la detección y bloqueo de intentos de modificación no autorizada de líneas de código de la web. Todo lo anterior es el objetivo que se quiere alcanzar, para mitigar en el máximo porcentaje posible las vulnerabilidades y la exposición de los servicios. De esta manera se esboza una idea clara de lo que se quiere conseguir, teniendo en cuenta el problema principal y el objetivo que se quiere

alcanzar de manera que se observe aumento en la seguridad informática de la corporación.

Partiendo de todo lo expuesto anteriormente, podríamos identificar como principales ventajas que para la Corporación se tendrá, encontrando una solución definitiva, respecto a los tiempos de atención de incidentes, como mitigación de los mismos, basados en las funcionalidades que se tendrá bajo la solución WAF (Web Application Firewall).

3.1 INTRODUCCIÓN A LA SITUACIÓN DESEADA

Específicamente en la seguridad informática, se debe tener actualizaciones que generen confianza en el cliente dadas las constantes amenazas que surgen en cualquier lugar del mundo y que pueden afectar el funcionamiento de los servicios Web expuestos en la red. Así como las actualizaciones de rendimiento se realizan periódicamente, las de seguridad tienen igual o más importancia, dado el riesgo que presenta la afectación de servicios Web [11] [12].

Debido a esto el ideal dentro de una organización que tiene tráfico alto y constante cambio de usuarios es el de mantener sus servicios, en este caso los servicios WEB, dentro de un estado sano, transparente y donde la información no tenga riesgo de ser afectada, es decir se cumplan los tres pilares de la seguridad de la información. La situación deseada en este caso es contar con un sistema dentro de la infraestructura de TI capaz de prevenir, detectar y disminuir los ataques externos que puedan afectar el normal funcionamiento de las aplicaciones, y de esta forma reducir el riesgo interno dentro de la compañía a nivel de TI. [13]



Ilustración 7. Pilares de Seguridad de la Información – Fuente Internet: <https://www.lisot.com/que-es-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/>

Los usuarios finales internos, que en ocasiones son los que presentan más riesgo de ingreso de ataques debido a su falta de conocimiento, pueden llegar a tener cierto nivel de tranquilidad con la ayuda de la implementación sugerida dentro de este documento, esto teniendo en cuenta que las capacitaciones al personal siempre deben ser periódicas y referentes al tema de seguridad informática. Más allá de que probablemente no existe un sistema que mitigue el 100% de las vulnerabilidades de manera indefinida, ni que rechace completamente el total de ciberataques externos que se puedan sufrir dentro de la organización, lo deseado es disminuir al máximo este riesgo para mitigar afectaciones dentro de los servicios, manteniendo la información resguardada, el código protegido y a los usuarios resguardados de amenazas.



*Ilustración 8 Beneficios de Protección a los Ataques WEB Avanzados – Fuente Internet:
<https://www.marquesme.com/que-es-un-waf-y-como-te-protege-de-ciberataques-a-tus-aplicaciones-web/>*

Como resumen a lo expuesto, en el modelo CANVAS usado, en donde identificamos las ventajas que atienden la necesidad de la CAR Cundinamarca, podemos resaltar:

- ✓ Reducción del tiempo de protección de eventos que afectan la seguridad de los sistemas de información.
- ✓ Adopción de una transformación digital que atiende la necesidad de mejora reputacional, frente a los adversarios cibernéticos.
- ✓ El producto y/o servicio presentado, WAF, cumple con la necesidad de la Corporación, y se acopla nativamente a la infraestructura tecnológica actual.
- ✓ La propuesta de valor actual reduce gastos administrativos.
- ✓ La propuesta de valor presentada genera una actualización tecnológica, que, en razón a sus beneficios, permite una apropiación consciente y responsable.

3.2 PROPUESTA DE VALOR

Teniendo en cuenta los objetivos y el problema que se requiere afrontar, el valor se refleja en la disminución de la afectación de los servicios y la estabilidad que observa el cliente final cuando los utiliza. Estos beneficios son clave cuando

generan mejor percepción en el usuario y cuando disminuyen los incidentes asociados a la infraestructura, desarrollo, y elementos de TI incluidos en la arquitectura del flujo del proceso, y de esta forma mantener a salvo la seguridad, integridad y disponibilidad de la información. Si se afronta de frente al problema planteado, no solo gana TI sino el usuario, el cliente, y las demás áreas que dependen de los servicios expuestos.

Estos servicios comprenden la integración tecnológica de conexión a usuario final de capas superiores del modelo OSI, en donde se presentan soluciones a la medida que buscan satisfacer la necesidad de interacción del usuario con el acceso a la información.

A diferencia de la experiencia tenida en el acceso a la información por los usuarios finales, la escalabilidad de software garantiza la seguridad y la confianza en la información entregada, bajo la analítica y custodia de los datos, como la respectiva generación de informes a la medida que obedece la necesidad general de las áreas jurídica como de gestión documental.

La propuesta de Valor en el Modelo Canvas, se enfoca en fortalecer los entornos web de la CAR implementando herramientas basadas en Inteligencia Artificial y Machine Learning que ayuden en la toma de decisiones al equipo de seguridad de TI estén en la capacidad de analizar y tomar medidas frente a posibles vulnerabilidades por medio de patrones de seguridad.

3.2.1. PERFIL DEL CLIENTE

En la identificación del perfil de los usuarios que interactúan en la Red Corporativa de la CAR Cundinamarca, se logra identificar que los usuarios buscan en su desempeño general en la necesidad de proteger su información respecto al uso de los sistemas de información.

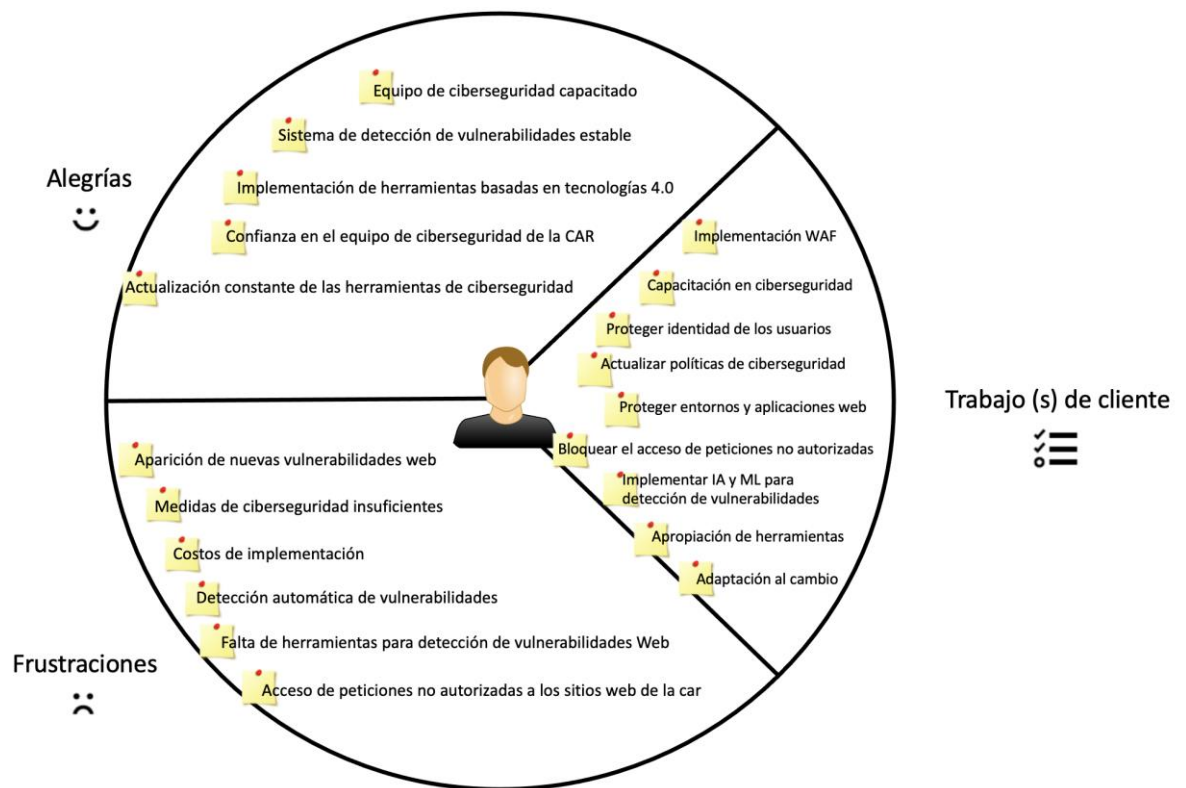


Ilustración 9. Perfil de cliente, Perfil del cliente y mapa de valor – Fuente Elaboración propia

• Segmento de clientes

La propuesta de la solución está dirigida a los clientes internos de la red corporativa la Corporación Autónoma Regional, así como los usuarios externos que hacen consultas a los sistemas de información, dentro ellos:

- Funcionarios Internos
- Contratistas
- Usuarios externos de la Corporación, respecto a consultas, quejas, trámites (Derechos de petición, PQR).
- Entes de control.

3.2.2. MAPA DE VALOR

Se identifica que, a nivel general, es de interés para la Corporación generar la capacitación de los usuarios de la CAR respecto a todos los roles, situación, que genera tranquilidad respecto al uso seguro de los sistemas de información.

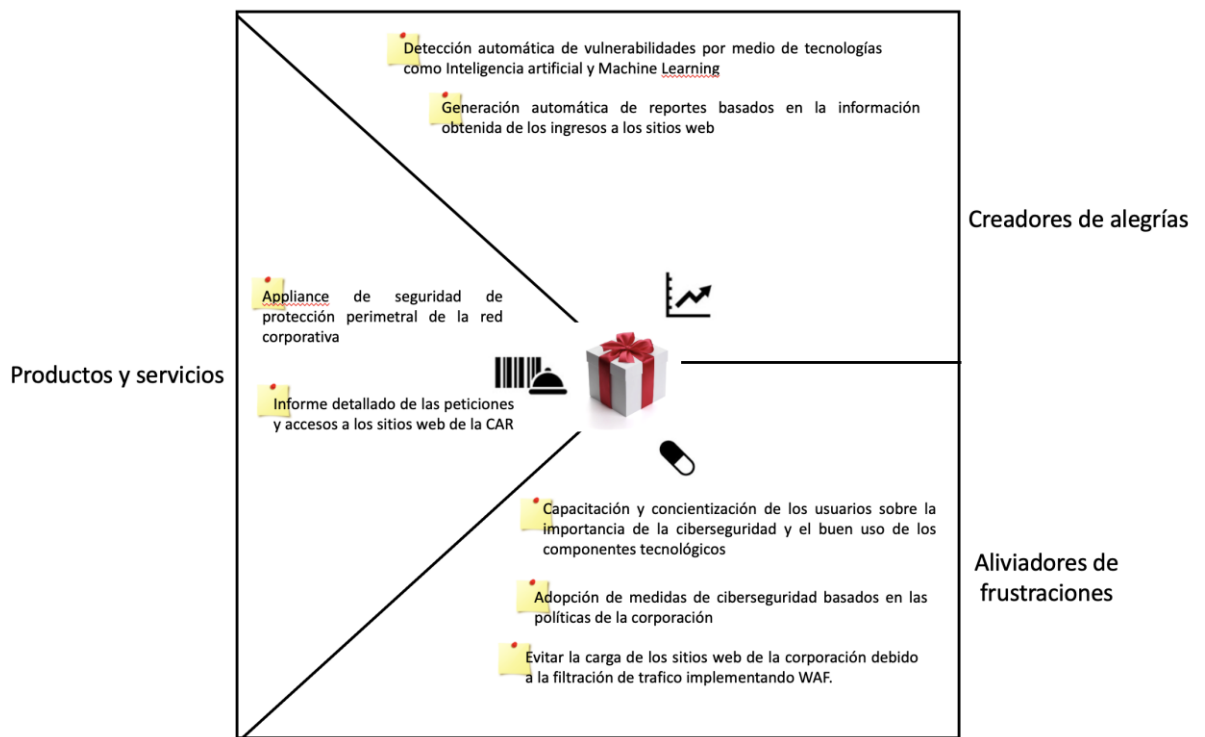


Ilustración 10. Perfil del cliente mapa de valor – Fuente Elaboración propia

3.2.3. CLASIFICACIÓN DE TRABAJOS, FRUSTRACIONES Y ALEGRÍAS

Se enmarca como atención a la necesidad de la Corporación, la implementación de sistemas de protección y mitigación de ambiente inseguros, en donde el uso de los sistemas de información de los usuarios finales cumplan con estándares que seguridad, que a pesar de ser transparentes para los usuarios, permiten al área de OTIC (Oficina de las Tecnologías de la Información y Comunicaciones), contar con un soporte tecnológico robusto, que sustentará el nivel de madurez y

estabilidad de la Corporación en la adopción del marco normativo y regulatorio de ciberseguridad.

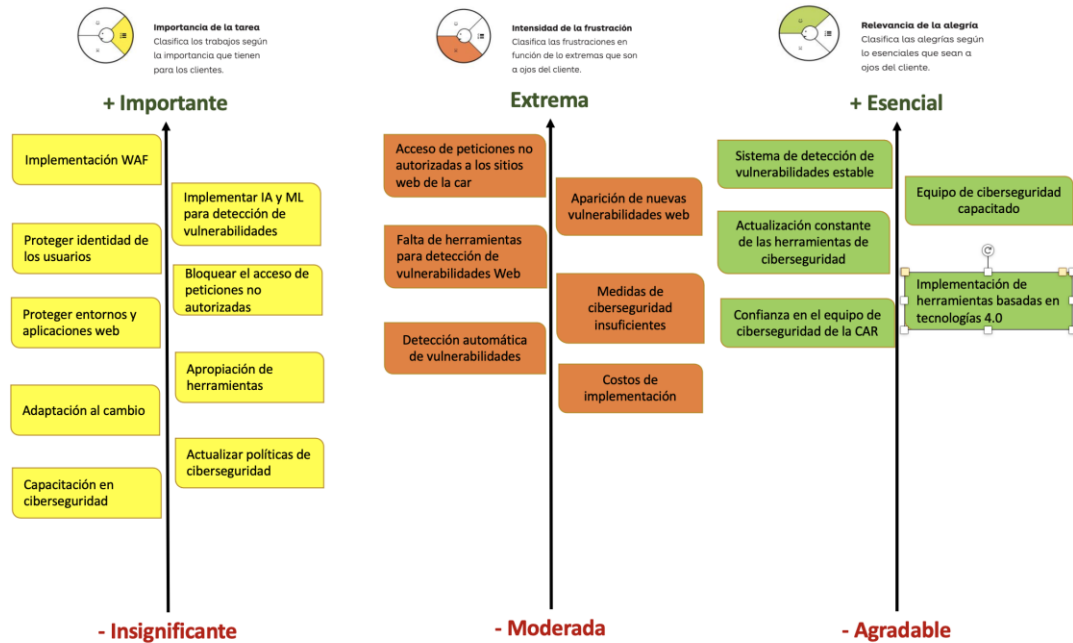


Ilustración 11. Clasificación de trabajos, frustraciones y alegrías. Fuente Elaboración propia

3.2.4. LIENZO DE LA PROPUESTA DE VALOR

Se logra el enfoque general de entendimiento del problema de la Corporación, como la apropiación de un ambiente WEB seguro, que se logra un nivel de madurez tecnológico frente los avances tecnológicos de atención a ciberamenazas.

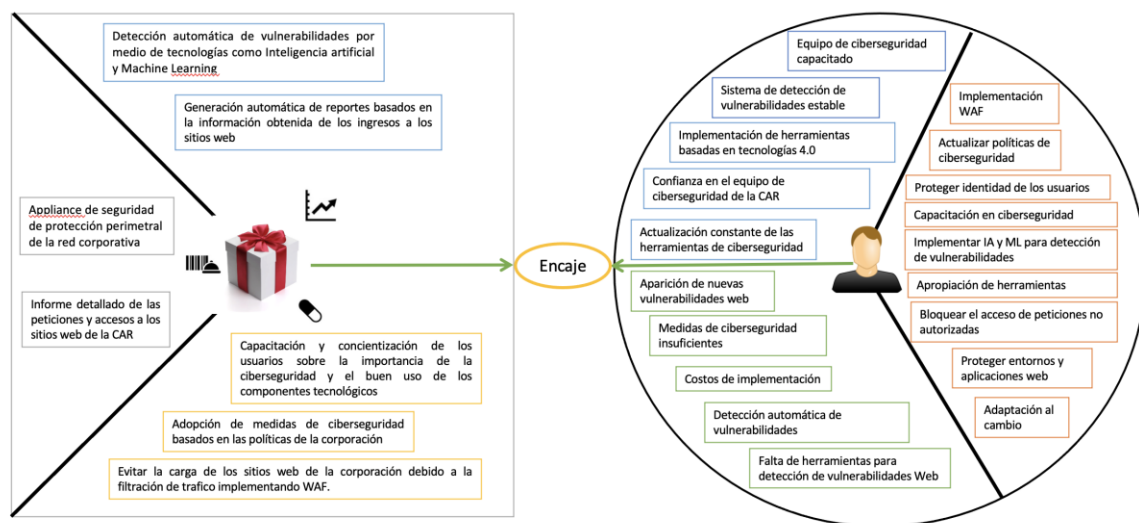


Ilustración 12. Lienzo de la propuesta de valor - Fuente Elaboración propia

3.2.5. Definición Propuesta de Valor

Implementación de servicios de servicios de seguridad de la información, que abarcan el ámbito de seguridad informática perimetral, como el abordamiento de las normas ISO 27001 y 27032, para así, encerrar el campo de acción de la ciberseguridad basado en la normatividad descritos en el numeral “2.6LA RELACIÓN DE LAS APLICACIONES CON LA PROPUESTA”.

Los usuarios finales, en este caso, como los que usan los recursos tecnológicos de la Red Corporativa, de la CAR Cundinamarca, demandan que se les garanticen la protección de los datos usados, basados en los pilares de seguridad de la información confidencialidad, integridad, disponibilidad, autenticidad y legalidad. [13].

Nuestro diseño y servicio presentado, comprende servicios profesionales especializados en un cumplir la expectativa actual, y permitirá corregir falencias tecnologías ya identificados respecto a vulnerabilidades en los sistemas de información, bajo el modelo proxy reverse que será implementado.

4. ANÁLISIS DE LAS ALTERNATIVAS TÉCNICAS PARA SOLUCIONAR EL PROBLEMA

4.1 DIAGNOSTICO INTERNO PARA APROPIAR LAS TECNOLOGÍAS

Basados en la necesidad de implementar unas plataformas dedicadas a la protección de los portales de acceso WEB, bajo los protocolos HTTP y HTTPS de la CAR Cundinamarca, en donde su funcionalidad genera confianza en la protección y que adicional sumen procesos de analítica en tiempo real, bajo servicios tecnológicos de Machine Learnig de cuarta revolución industrial. [12]

Se ha realizado una revisión detallada del entorno actual, como arquitectura del acceso a la información que realizan los usuarios internos como externos a estos servicios. Así mismo, se han identificado el listado de aplicaciones WEB de la Corporación, las cuales, como indicación de los administradores de la Red Corporativa y el equipo de Desarrollo se encuentran proyectadas para incluir dentro de una capa de seguridad, basados en las pruebas de vulnerabilidades realizadas bajo el modelo de Ethical Hacking controlada, por plataformas MALTEGO, NESSUS y NMAP. [3] [13]

Adicional a la tabla relacionada, a continuación, como anexo a este proyecto esta la evidencia en el archivo, “Levantamiento de información.pdf”.

Servicios WEB a proteger:

NOMBRE WEB/APP	APLICACIÓN,	DESCRIPCIÓN APLICACIÓN	URL: Si tiene más de un acceso incluirlo
CONDOR		Control de Obras Responsables	https://condor.car.gov.co/
NEGOCIOS VERDES		PORTAL NEGOCIOS VERDES Y SOSTENIBLES	http://negociosverdes.car.gov.co
PARQUES CAR, WEB		PAGINA DE PARQUES JURISDICCION CAR	https://parques.car.gov.co/

SIDCAR	SISTEMA DE GESTION DOCUMENTAL DE LA CAR	https://sidcar.car.gov.co/ ; <a href="https://sidcar.car.gov.co/api/<controller>...">https://sidcar.car.gov.co/api/<controller>... ; https://sidcar.car.gov.co/WSIntegracion.aspx ; https://sidcar.car.gov.co/WSRadicado.aspx ; https://sidcar.car.gov.co/WSSIGU.aspx ; https://sidcar.car.gov.co/WSVisitaTecnica.aspx
SAE	SISTEMA DE ADMINISTRACION DE EXPEDIENTES AMBIENTALES	https://sae.car.gov.co/
SIDCAR AMBIENTAL	PROCESOS AMBIENTALES SIN EXPEDIENTE	sidcarambiental.car.gov.co apisidcaramb.car.gov.co
SGIP	SISTEMA DE GESTION PREDIAL DE LA CAR (SOLO PREDIOS CAR)	http://sgip.car.gov.co/
Banco de Proyectos de Confinanciación	Registro y seguimiento para Proyectos de Confinanciación	http://bancoproyectos.car.gov.co/
SIGU	Aplicativo para administrar cuentas de usuario en los diferentes sistemas de CAR.	http://sigu.car.gov.co/
GEOAMBIENTAL	Sistema de Información Geográfico en ambiente Web para uso de los funcionarios y contratistas de la CAR	http://geoambiental.car.gov.co
SIGCI	Sistema de Gestión del Conocimiento y la Innovación Ambiental	https://sigci.car.gov.co
AMBIENSQ	sistema laboratorio ambiental	-
CARTOGRAFIA EN LINEA		-
SICLICA / ZIPA		-
Intranet - SharePoint 2010	Intranet corporativa.	http://intranet.car.gov.co
App CAR Móvil (APLICAR)		-
KOFAX Express 3.1		-
SINGELIA	Sistema de información y gestión de la DLIA	singelia.car.gov.co
EVA	Escuela virtual ambiental, cursos CAR	http://elearning.sigci.car.gov.co
SIRFAC	SISTEMA DE FACTURACION Y RENTAS	http://sapwlbogpru.car.gov.co/
SGC	SISTEMA DE GESTION CONTRACTUAL	http://sgc.car.gov.co/forms/frmservlet?config=sgc

PORTAL WEB	Publicación de información e interacción con los usuarios de la Corporación	https://www.car.gov.co/
ORION	Sistema Administrador de Procesos Judiciales	http://orion.car.gov.co/
ORION DISCIPLINARIOS	Sistema Administrador de Procesos Disciplinarios	http://disciplinario/login/login.orion
REVISTA LABORATORIO	Publicación de artículos especializados e información de la Dirección de Laboratorio Ambiental	https://ittpa.car.gov.co/

Tabla 3 Aplicaciones WEB CAR - Fuente propia, tomado del levantamiento de información

En el archivo anexo “logs de escaneos.xlsx”, se encuentra el detalle de tabla indicada anteriormente.

Adicional a esta evidencia, se presenta la arquitectura de comunicaciones general que se levantó del entorno de la CAR Cundinamarca respecto al ambiente cliente-servidor en servicios WEB HTTP y HTTPS, en el cual se detalla un Firewall perimetral Core, que es el centro de toda la Red Corporativa de la CAR en el cual se identifica la existencia de dos super redes de servidores denominadas DMZ (desmilitarizada) y MZ (militarizada), en donde la red DMZ es la que contiene todas las aplicaciones a proteger respecto la necesidad planteada por la Corporación. Respecto a la conexión de los usuarios hacia estas zonas de servidores, se identifica que se encuentran separados como una zona de red diferente y del mismo modo, la conexión de los usuarios externos ingresa por una interfaz del Firewall que va hacia la Internet, en una conexión redundante de dos operadores de servicios de Internet, Telefónica Movistar y ETB (Empresa de Telecomunicaciones de Bogotá). Esta información se encuentra relacionada en el anexo a este proyecto, que se nombra “Levantamiento de información.pdf”.

En la siguiente ilustración, se presenta la topología basé de la red de la Corporación, que surtirá modificaciones, cuando sea intervenida la

infraestructura de la capa de seguridad y sea integrado a la protección de las aplicaciones WEB, un Firewall WEB:

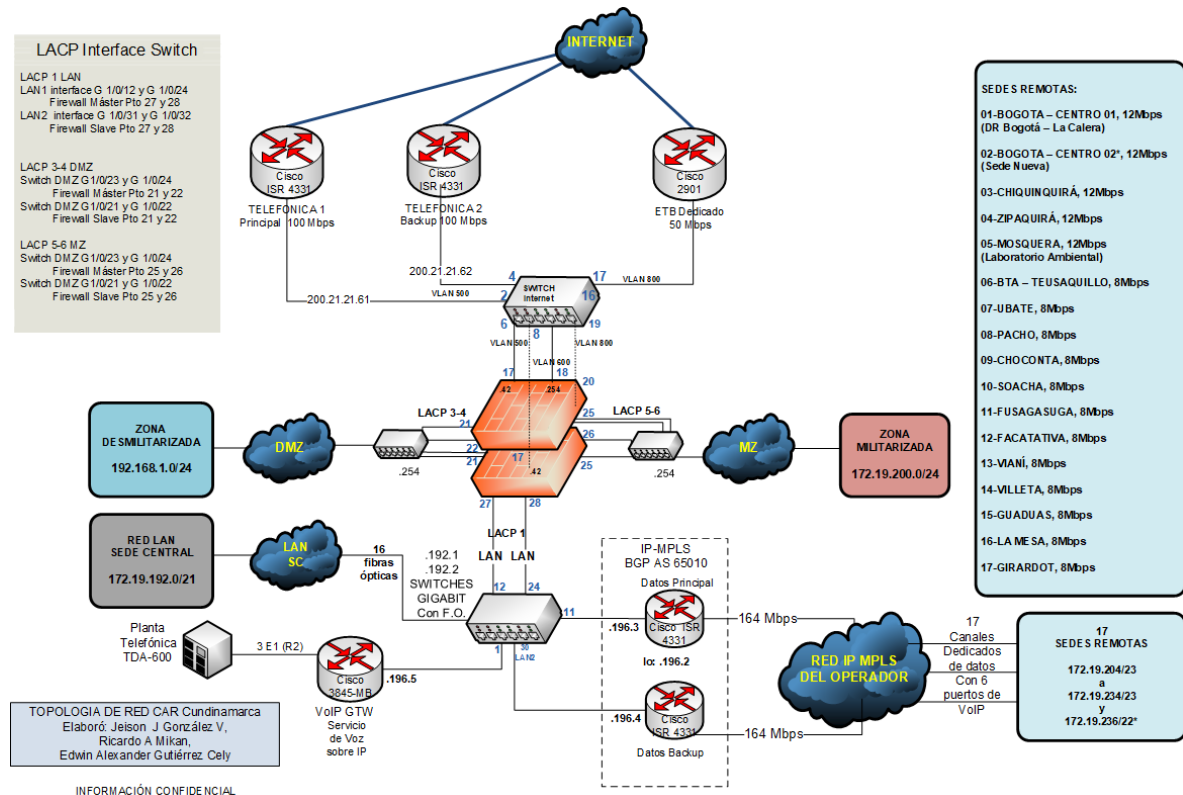


Ilustración 13 Topología Base CAR Cundinamarca - Fuente, Elaboración Propia

Al revisar con los administradores de estas plataformas se obtiene el siguiente resumen técnico de las actuales soluciones de seguridad informática, que juegan un papel importante dentro de la arquitectura, desde el punto de vista de los periféricos.

Se confirma la existencia de la una consola de antivirus de marca McAfee bajo la solución ePolicy Orchestrator, que se encuentra desplegada en los usuarios finales internos como en todos los servidores de la Corporación.

Así mismo, se confirma con el administrador del Firewall, que es de la marca FORTINET, de modelo 1100E, indica que el acceso a los servicios WEB

contenidos en el presente documento esta desplegado por ZONAS, en los cuales se hace una comunicación de zona a zona por medio reglas de Firewall en los cuales solo son permitidos los puertos específicos que requiere cada comunicación, así mismo, se cuentan con perfiles IPS (Intrusion Prevention System) en las aplicaciones, en donde se detalla o se resalta que estos perfiles que monitorean el tráfico que pasa hacia a la aplicación se basan a nivel de firmas conocidas y actualizadas por los fabricantes tal como ocurre con el antivirus, pero que no logran detectar ataques desconocidos o de comportamientos anómalos, que solo se puedan identificar en tiempo real por tecnologías de machine Learning e inteligencia artificial. En la conexión de los usuarios externos, para el protocolo IPv4 se evidencia las respectivas reglas de comunicación con NAT y para el protocolo IPv6, se observan que las conexiones en IPv6 pasan directo peer to peer (punto a punto), con direccionamiento Global Unicast del prefijo /48 de la entidad, situación que expone al servidor directo a Internet en su IIS.

Para los usuarios internos que se encuentran fuera de la Red Corporativa se confirma la existencia de portales VPN SSL, que son administrados bajo la conexión del AD (directorío activo), con integración del protocolo LDAP (protocolo ligero de acceso a directorios, TCP 389), así mismo, se detalla que todos los usuarios internos cuentan con su propio usuario del directorío activo, con una clasificación por grupos de Gold, Blanco y unos generales que se divide en verde y violeta. En el anexo a este proyecto, que se nombra “Levantamiento de información.pdf”.

A medida que la tecnología de las aplicaciones sigue avanzando rápidamente, las amenazas también proliferan en la capa de aplicaciones (capas superiores del modelo OSI). Debido a lo accesibles que pueden ser las aplicaciones a través de Internet, las plataformas WEB se encuentran constantemente expuestas a posibles delitos cibernéticos. Los firewalls de red tradicionales, los NGFW e

incluso los NIPS más avanzados sólo pueden proporcionar, como mucho, un nivel de capa 4 de protección, pero no en las capas de aplicación. Sólo un firewall de aplicaciones web puede cubrir de forma exhaustiva esta nueva lista de vulnerabilidades, conocida como OWASP top 10 [14].

4.2 ANÁLISIS DEL PROCESO DE TRANSFORMACIÓN DIGITAL

La adopción e implementación de nuevas tecnologías es un proceso constante que adquieren las compañías del sector público y privado para tener sus servicios de TI a la vanguardia. Generalmente se adquieren software y hardware que ayudan a actualizar la infraestructura y el licenciamiento para renovar las capacidades de respuesta de los servicios de TI que prestan a los usuarios.

Algunas veces se confunde la compra de elementos nuevos como si fuera Transformación Digital, y lo que requiere entender el término como tal es la adopción en todos los niveles de personas y tecnología, de aspectos de evolución constante que permita a la compañía el cambio tecnológico que el mundo exige, como pasó en los últimos años con el uso del Cloud y la disminución del On Premise cuando se habla de infraestructura de TI.

En nuestro caso particular, la adopción del WAF para la seguridad de los servicios WEB de la CAR, hace parte de esa Transformación Digital dado que permite a los usuarios tener más seguridad al usar los servicios, conservar la integridad de la información, y agilizar labores que anteriormente tomaban más tiempo realizar, como la mitigación de riesgos asociados a seguridad, como ataques de denegación de servicio, entre otros.

Visión y Liderazgo

Es importante entender que la transformación digital no se genera desde los cargos directivos hacia abajo, sino se aprende e implementa transversalmente

en todos los niveles, para generar cultura de innovación donde ninguna persona se sienta aislada del flujo de trabajo. Se debe contar con las capacitaciones necesarias que aporten valor a las personas y procesos en cada elemento participativo dentro de la transformación que se quiere alcanzar, teniendo claro los objetivos. Lo que sí se requiere es generar transformación donde cada persona pueda sentirse líder de los procesos en los que participa.

Transformación Digital de las Personas Y Procesos

Como se mencionó anteriormente, es importante que las personas se sientan incluidas en la transformación digital. Es decir, hacer partícipes a todos los involucrados desde cada área, sin desestimar el usuario final el cual usa los servicios web, a involucrarse y aprender cuando se adquiere una nueva tecnología, se modifica algún proceso, o se sustituyen métodos manuales por procesos de TI que generan más eficiencia y menos tiempo de ejecución.

4.3. MODELOS DE PLATAFORMAS WAF

4.3.1. ¿Qué ES WAF?

En una solución tecnológica, que se asocia a los sistemas de seguridad de la información, dedicadas a la protección de servicios WEB, bloqueando amenazas en tiempo real, pero no generando falsos positivos basada en sus funcionalidades de auto aprendizaje.

WAF: Web Application Firewall.

4.3.2. WAF COMO SOFTWARE

Requiere un ambiente virtualizado para su despliegue, ejemplo, hyperv, vmware y otros. Es escalable en cuanto las capacidades que se pueden aprovisionar por el administrador de servidores e infraestructura de Datacenter.

Como solución no se acopla a la presente necesidad, ya que los servicios de la CAR Cundinamarca están en ambiente físico de Datacenter on premise, en el cual se busca que esta solución actúe como un Gateway, puerta de enlace, que sea el frente a todas las consultas.

4.3.2. WAF COMO PLATAFORMA FÍSICA

Se presenta como un dispositivo físico que interviene o se integra en arquitectura física de la solución.

Este diseño acoge técnicamente la necesidad contemplada por la Corporación.

Se dispone de múltiples funcionalidades que atienden el impacto de vulnerabilidades a mitigar y aíslan los ciber ataques, permitiendo el tráfico de red como paquetes de información limpios, para ser entregados al servidor de los sistemas de información.

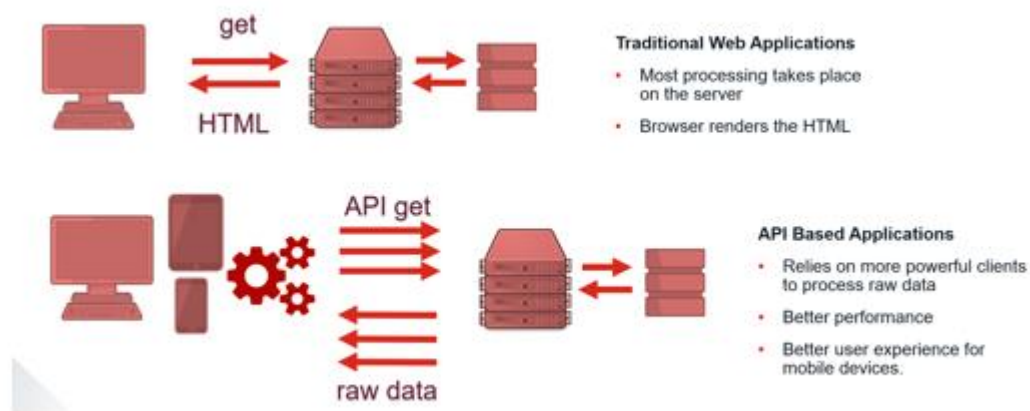


Ilustración 14 Modelo de Sesión de Red - Fuente Internet: <https://www.fortinet.com/lat/products/web-application-firewall/fortiweb>

5.PROPUESTA DEL MODELO DE NEGOCIO, VALIDACIÓN DE MODELO NEGOCIO Y PROPUESTA DE LA SOLUCIÓN TECNOLÓGICA.

5.1. MODELO DE NEGOCIO

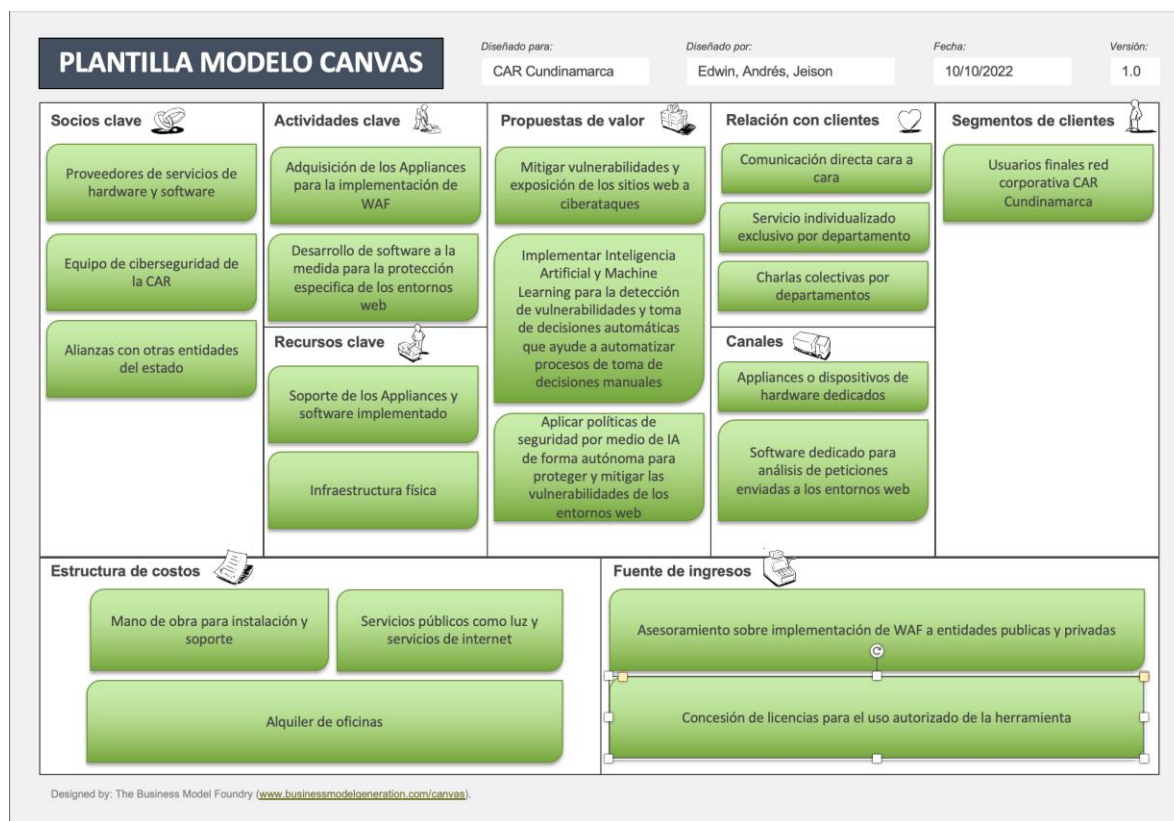


Ilustración 15. Plantilla Modelo Canvas. Fuente Elaboración propia

- **Canales**

La propuesta de valor será entregada a los usuarios finales por medio de acceso WEB seguro en modalidad de proxy reverso bajo los protocolos HTTP y HTTPS, respecto al acceso local y externo por medio de una red virtual denominada VIP que será el frente hacia las consultas de las aplicaciones de sesiones TCP/IP, en donde el WAF será quien ante la aplicación genere la consulta.

- **Relación con los clientes**

Para garantizar una implementación efectiva de la propuesta de valor se plantea una comunicación directa entre el equipo de seguridad de TI quienes son los encargados de gestionar el uso de las herramientas para garantizar la seguridad y las demás áreas de la corporación quienes serán los usuarios finales a quien va dirigida la solución que se está proponiendo. Lo anterior, partiendo del precedente del auto aprendizaje de la plataforma WAF hacia la aplicación y análisis técnico con los líderes funcionales de las mismas, quienes de primera mano conocen el funcionamiento y fin de uso de la aplicación.

- **Flujo de ingresos**

Este modelo de arquitectura segura se integra con más entidades gubernamentales como privadas, en razón, a que esta plataforma en modelo de software como dispositivo físico permitiría mitigar el riesgo de vulnerabilidades y ciberataques a los sistemas de información.

Se concluye, que los equipos WAF se dedican 100% a la protección de servicios WEB respecto a sus características técnicas.

Adicional a la implementación, se cuenta con servicios de Soporte tecnológico del diseño de la protección de datos en plataformas seguras.

Por lo anterior, el modelo de negocio para el flujo de ingresos comprende un sector robusto, ya que se mitigan y corrigen falencias en la seguridad informática perimetral. Por lo anterior, se dispone de participación en procesos contractuales tanto del sector público y privado, dentro y fuera de Colombia.

- **Recursos clave**

Infraestructura tecnológica como servidores de aplicaciones, servidores de bases de datos y licenciamiento de herramientas de seguridad perimetral y la integración de las tecnologías con los servicios web.

- **Actividades clave**

Levantamiento de información, entendimiento de la arquitectura, seguido de la enumeración de los portales WEB a incluir en el WAF, identificación de vulnerabilidades de las aplicaciones, levantamiento de información de las características de las aplicaciones, respecto a su motor de ejecución y base de datos, generación de las reglas de capa 3 y capa 4 del modelo OSI de la red virtual de modalidad de proxy reverso, inclusión al WAF de las aplicaciones WEB de la Corporación en modo monitor de auto aprendizaje de las funcionalidades de Machine Learning por un tiempo corto, para en una ventana contrada pasar a modo seguro.

- **Socios clave**

- Usuarios Finales
- Usuarios Funcionales de las aplicaciones
- Equipo de desarrollo interno
- Equipo de QA
- Equipo de redes y seguridad de TI (Tecnologías de la Información) interno de la Corporación o entidad o compañía

- **Estructura de costos**

La Corporación Autónoma Regional cuenta con estructura de costos fijos y variables enfocados al área de seguridad de TI.

- **Costos Fijos:**

Adquisición de la solución WAF (Firewall de aplicaciones WEB), con todo su esquema de licenciamiento, respecto a funcionalidades como Security Service, Antivirus, IP Reputation, IP Reputation, Credential Stuffing Defense y otros. En el ITEM técnico se debe dimensionar el soporte por el fabricante, en el cual se detalla la modalidad de atención como canales de atención, es así, que se dimensione el periodo a contar con este servicio. Como ejemplo un modelo de 7*24*365 por 2 años.

Adicional a estos costos fijos, es importante detallar los servicios de ingeniería profesionales, como los perfiles de gerencia de proyectos y líderes técnicos que comprenden el desarrollo general de este modelo de proyectos.

- **Costos Variables:**

Mantenimiento de los ambientes los cuales pueden variar de acuerdo con el soporte que se necesite, por otro lado, existe la mano de obra que puede variar de acuerdo con las tareas que se vayan necesitando durante el afinamiento de la solución tecnológica.

5.2. VALIDACIÓN MODELO DE NEGOCIO

Para la validación del modelo de negocio se ha seleccionado las encuestas ya que por medio de estas se permite analizar las diferentes perspectivas de los consultados y tomar decisiones más acertadas para la implementación de la propuesta de solución propuesta.

De la encuesta realizada se consultó un grupo de 20 personas las cuales trabajan dentro de la CAR Cundinamarca en diferentes áreas esto con el fin de conocer que tanto conocen sobre la seguridad que ofrece la entidad y la importancia que esta tiene para garantizar el correcto funcionamiento de los entornos web de la entidad.

Dentro de la encuesta se diseñaron 6 preguntas relacionadas a temas de seguridad y dispositivos de protección web y de las cuales se obtuvo el siguiente análisis y resultados:

- Se puede concluir que el 70% de los encuestados conocen la importancia de proteger los sitios web para garantizar el correcto funcionamiento de los entornos web de la entidad
- El equipo de seguridad de la información se encarga de brindar capacitaciones oportunas que contribuyen a la prevención y disminución de ataques por fallas humanas
- Para el 85% de los encuestados es más importante que las personas estén capacitadas sobre los riesgos antes que dejar todo en manos de herramientas de protección, sin embargo, el 80% de los encuestados también consideran que la entidad debería implementar medidas y dispositivos de seguridad para mejorar los indicadores de seguridad.

¿Conoce usted sobre las medidas implementadas a nivel de seguridad sobre los servidores web, aplicaciones y APIs?

20 respuestas

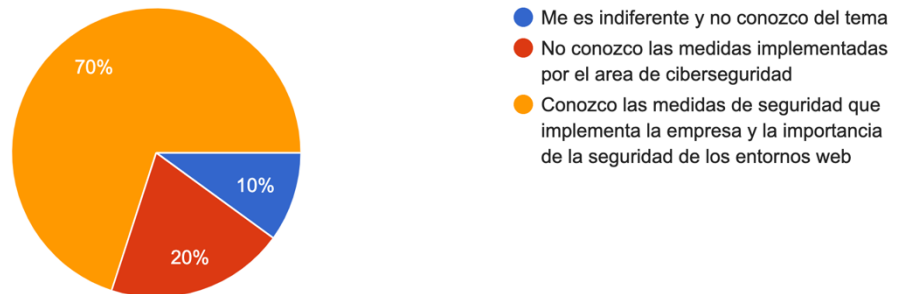


Ilustración 16: validación modelo de negocio pregunta 1

¿La capacitación que he recibido por parte del equipo de ciberseguridad en cuanto a la importancia de la seguridad de los entornos web es?

20 respuestas

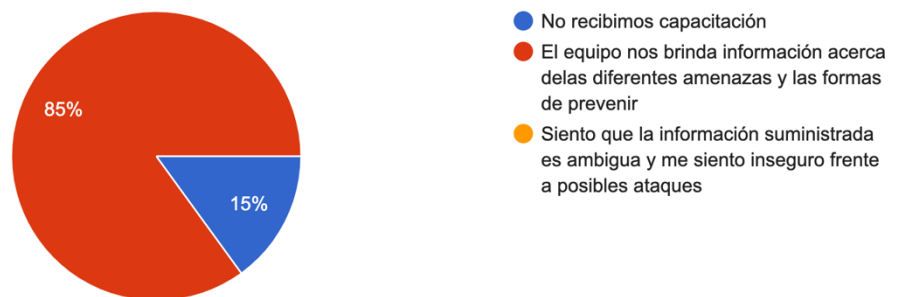


Ilustración 17 Validación modelo de negocio pregunta 2

Seleccione la afirmación o afirmaciones que considere más precisas.

20 respuestas

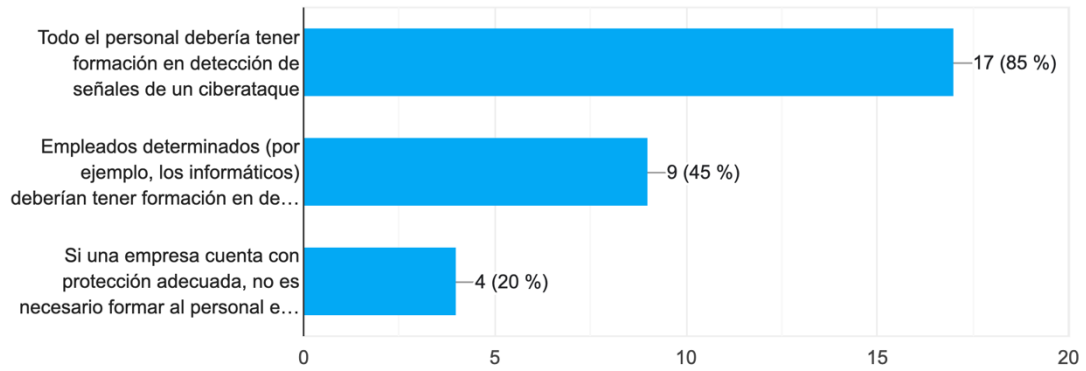


Ilustración 18 Validación modelo de negocio pregunta 3

Conoce usted que es WAF (firewall de aplicaciones web)

20 respuestas

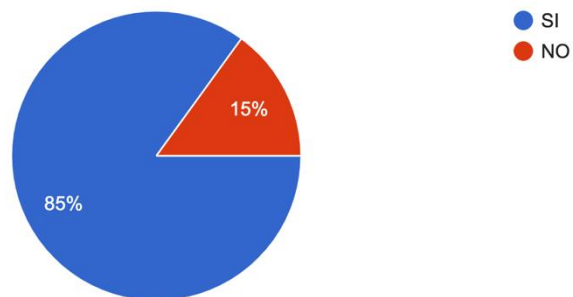


Ilustración 19: Validación modelo de negocio pregunta 4

¿Cuáles de los siguientes aspectos considera más importantes para la ciberseguridad de las empresas? Seleccione todas las opciones que considere desde su conocimiento.

20 respuestas

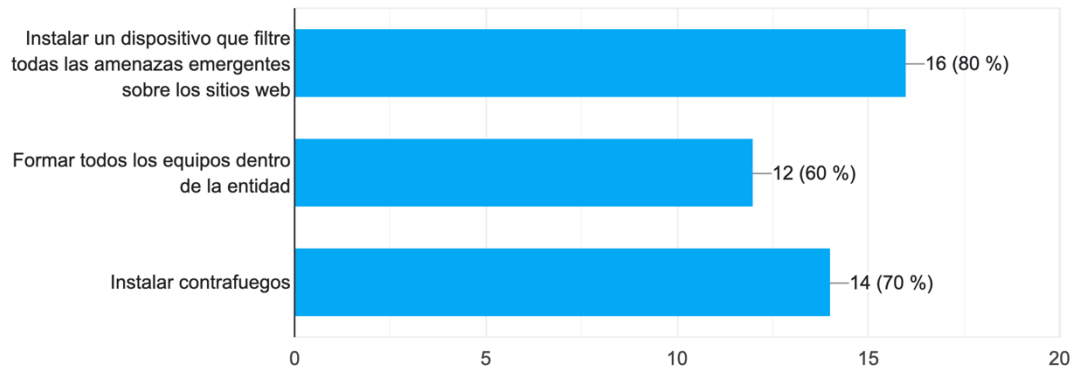


Ilustración 20: Validación modelo de negocio pregunta 5

Que percepción tiene usted acerca de los entornos y sitios web de su compañía

20 respuestas

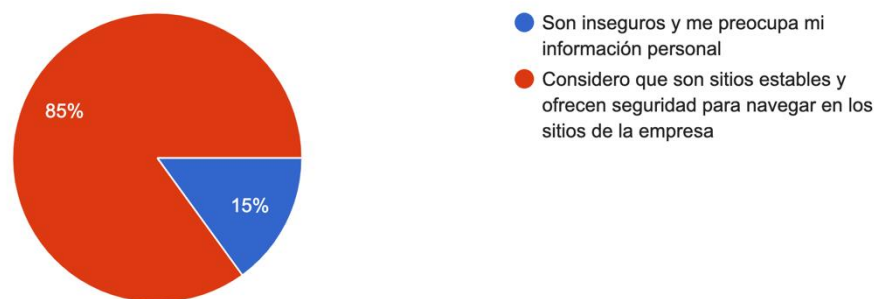


Ilustración 21: Validación modelo de negocio pregunta 6

5.3. PROPUESTA DE LA SOLUCIÓN TECNOLÓGICÁ

Con base a la información levantada, la cual se ha presentado en el numeral anterior, desde el punto de vista del presente proyecto se deduce que su proceso de transformación y actualización tecnológica va por un buen camino, ya que el principio del control de acceso está enmarcado en la separación de dominios de broadcast. Del mismo, se cuenta con el control de usuarios bajo niveles de

privilegios, y que todo esto se integra con directorio activo hacia el perímetro por LDAP. También se evidencia la existencia de un antivirus vigente, que controla las terminales finales como servidores, y así mismo, se observa que sus sistemas operativos se encuentran actualizados tanto en las terminales de usuarios como servidores de aplicaciones y bases de datos.

La disposición de plataformas de control de acceso dispuestas por la Corporación, respecto a la solución FORTIGATE como su consola de antivirus, respecto a la necesidad general presentada en el presente documento de protección de los portales WEB, no cubren ni un pequeño porcentaje de la necesidad, basado al modelo internacional de comunicaciones OSI, en el cual el problema de protección de los portales WEB está en capas superiores de integración al motor de desarrollo y características específicas de cada aplicación.

El creciente desarrollo de amenazas cibernéticas demanda un desempeño y generación de atención de eventos en tiempo real, que se integre y entienda o capture cambios en el tráfico, que se ligan al comportamiento de la interfaz del usuario con el acceso y uso de los servicios tecnológicos.

El despliegue de plataformas dedicadas cien por ciento a estas funcionalidades de protección se presentan en las soluciones WAF (WEB APPLICATION FIREWALL), en donde todas las funcionalidades requeridas por la CAR CUNDINAMARCA, son acogidas en el software de gestión de estos appliance físicos. Dichas plataformas asumirán el rol supervisión, filtrado y bloqueo de tráfico en puertos de servicios y aplicaciones WEB.

5.3.1. EVALUACIÓN Y PREPARACIÓN DE LA SOLUCIÓN

Al conocer la infraestructura de la Corporación, y conocimiento lo que integra su sistema de seguridad, se llega a la decisión de viabilizar la adquisición del appliance para disponer en el datacenter, o por el contrario, confiar en las funcionalidades del Firewall, confiar en los antivirus locales del servidor o confiar en tener los sistemas operativos como parches totalmente activos y que esto nos permita confiar y esperar que todo estará bien en cuanto a la protección de los sistemas de información de la Corporación.

Adicional a esta duda, también se debe evaluar el impacto topológico que se generará con la inclusión de esta nueva plataforma, ya que se genera el impacto de crear nuevos dominios, creación de una red virtual para el servicio de proxy reverso, según el diseño, y el impacto a nivel de tráfico de red que esto generará.

Como complemento, la CAR en su equipo TI, y equipos de infraestructura, desarrollo y gerencial, definir si el alcance hecho, basado en la cantidad de aplicaciones que buscan proteger se mantendrán, o si por el contrario, se planificará dejar un crecimiento respecto a las capacidades del WAF, migrando todas las demás aplicaciones a este entorno seguro, y si en su migración, se dejarán solo para consulta internas, como externas.

5.3.2. PRUEBAS DE LA SOLUCIÓN

Con la decisión tomada, respecto a la inclusión del WAF como esquema de seguridad de los servicios WEB de la CAR, se ahonda en sus beneficios.

El Firewall de Aplicaciones Web (WAF) posee motores de detección dual compuesto por coincidencia de reglas y análisis semántico basado en el auto aprendizaje de funcionalidades de IA (inteligencia artificial).

Esta plataforma bloqueará las amenazas en tiempo real sin bloquear a los usuarios legítimos y sin generar los falsos positivos que generan los gastos administrativos, resaltando que las aplicaciones interactúan con bots benignos y maliciosos, y necesitan bloquear los maliciosos mientras permiten el acceso administrado para los benignos, en donde, los bots maliciosos buscan minería de datos competitiva, recolección de datos personales y financieros, adquisición de cuentas, fraudes publicitarios digitales y en casos extremos fraudes de transacciones.

Los servicios WEB para proteger de la Corporación cuentan con API contenidas como de consulta en otros sitios, para lo cual, las plataformas WAF cuentan con funcionalidades que benefician y que proporcionan puertas de enlace seguras en donde se gestionan los usuarios de API, se verifica la clave API, Control de acceso a la API, se controla el límite de tasa, se reescriben las llamadas a las API en donde los beneficios de control a este complemento se destaca que se oculta la estructura interna de la API de posibles atacantes y se ofrece una experiencia de usuario mejorada para los usuarios en una amplia gama de dispositivos sin sacrificar la seguridad.

En pro de la solución de la problemática sobre la solución WAF, se cuentan con las metodologías de CI/CD (Integración Continua / Despliegue Continuo), que garantizará la integración continua en el despliegue, en donde el machine learning reduce la fricción o problemas de la implementación de las aplicaciones WEB de la CAR Cundinamarca.

Estas plataformas WAF cuentan con las técnicas tradicionales que bloquean el tráfico malicioso en donde se encuentran la reputación por IP, la protección de DDOS, la validación de los protocolos como inspección, características específicas de los ataques conocidos como los desconocidos con interacción a los modelos sandboxing (ambiente aislado), así como lo más conocido y

genérico como firmas de antivirus y servicios de DLP (perdidas de datos o funcionalidades de fuga de información, estas funcionalidades son básicas, ya que el WAF no está dedicado a este servicio).

5.3.3. DESPLIEGUE

Con la base de la arquitectura de la CAR, en su Red Corporativa, en donde el Firewall perimetral obedece a un FORTINET Fortigate 1100E, la propuesta contemplada dentro el alcance a la solución de la necesidad, de protección de los portales WEB de la Corporación, genera una integración nativa a su plataforma, encaminada a un crecimiento homogéneo. La integración de plataformas de manera nativa, administrativamente a la CAR, brindará manejo de información de correlación e integración, para un análisis como seguimiento a incidentes de manera centralizada.

Con base a lo expuesto se presenta la plataforma FORTIWEB WAF, en donde se cumple técnicamente con la atención y corrección de la necesidad planteada y de igual forma se detallan las características técnicas a las cuales se acude como propuesta valor a la solución en donde como resumen se destaca que la CAR Cundinamarca no cuenta con plataformas que se dediquen a proteger cien por ciento (100%), portales WEB, sino que estas, solo mitigan el perímetro de acceso, bajo firmas o ataques conocidos sin servicios de autoprotección a vulnerabilidades que se encuentran en el tráfico de red.

En la siguiente ilustración se presenta el modelo de interacción de tráfico de las plataformas de seguridad.

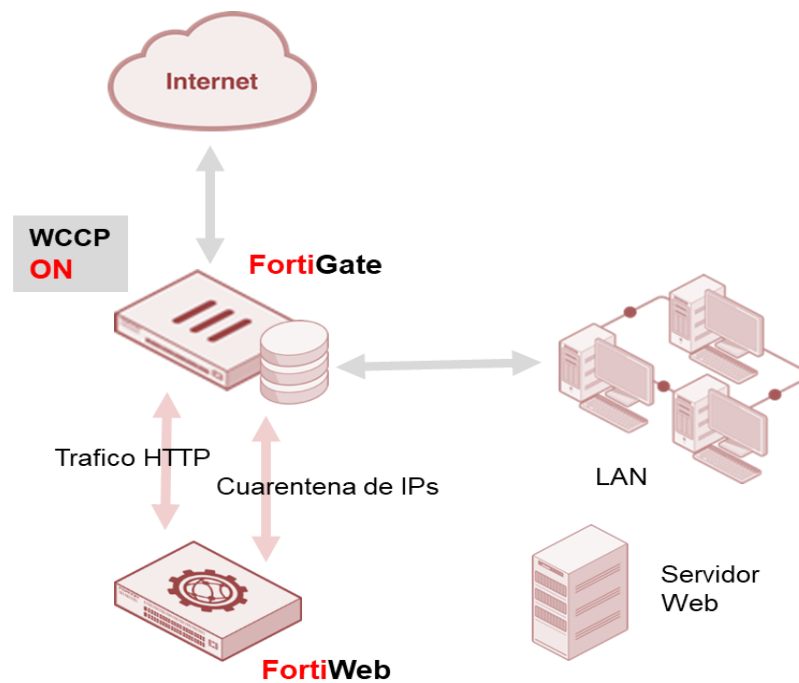


*Ilustración 22. Integración nativa plataformas de Seguridad – Fuente Internet:
<https://www.fortinet.com/lat/products/web-application-firewall/fortiweb>*

En tiempo real se contará con servicios de escaneos de vulnerabilidades WEB bajo servicios HTTP y HTTPS o puertos en modalidad de Forward hacia TCP/80. [2] Servicios de balanceo de aplicaciones que se podrían manejar en restricciones de acceso a sitios protegidos en la modalidad de autenticación, modalidad de caching en el cual se disminuirá la saturación del ancho de banda de Forwarding. La modalidad de compresión en la cual se acelera el rendimiento y son mejorados los tiempos de respuesta y por último la modalidad de SSL offloading en el cual se reducen el tráfico en servidores backend, los servicios comunes de antimalware de las firmas de antivirus, los servicios de la capa 7 presentación, también anti-defacement y Anti-DDOS [10] contando la detección y bloqueo de intentos de modificación del código con la inserción de script en los portales WEB, por lo cual protege la capa superior del modelo OSI de presentación del portal WEB, y [11] protegerá la imagen de la Corporación. Se requiere protección y denegación, de manera redundante a la Denegación de Servicios Distribuido a nivel de HTTP, teniendo validación de la reputación de

las direcciones IP públicas provenientes de la Internet, y por último servicios de implementaciones flexibles, con alta disponibilidad en razón al balanceo indicado, con integración nativa con el Core tecnológico de marca FORTINET y apoyo a la entidad en la transición del protocolo IPv6 como protección a los servicios de IIS, sujeto a las comunicaciones peer to peer permitidas por este protocolo. [10]

En la siguiente ilustración se presenta el modelo de transición del protocolo IPv6.

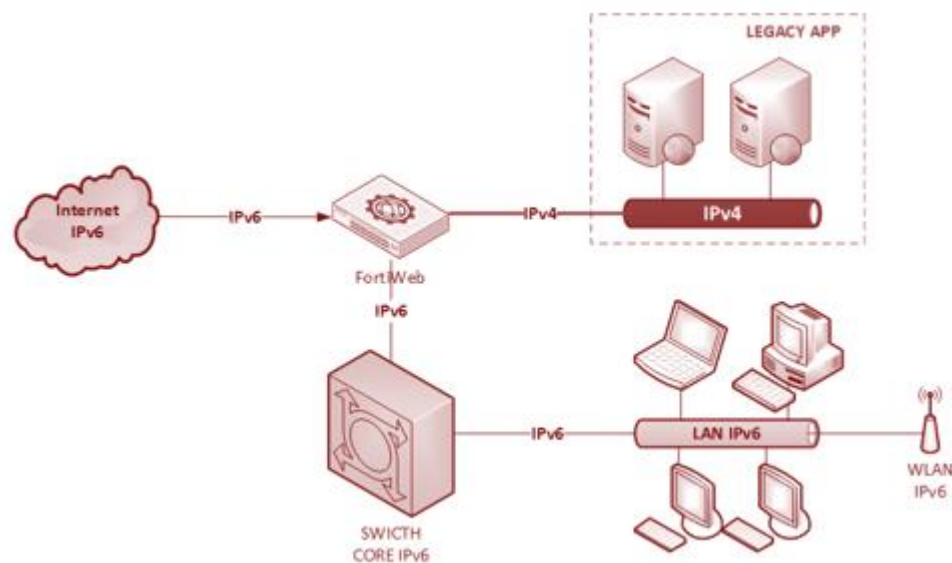


Ilustración 3 Transición IPv6 – Fuente Internet: <https://www.fortinet.com/lat/products/web-application-firewall/fortiweb>

Dentro del ambiente físico y lógico de implementación, la plataforma FORTIWEB ofrece los modelos de implementación e integración, tales como inspección transparente y proxy real transparente. El proxy reverso fuera de línea le permite al FortiWeb ajustarse a cualquier entorno. [15]

Con el conocimiento de la necesidad de la Corporación, el modelo de integración se plantea en dos fases de implementación e integración a las plataformas WEB. En esta fase se tendrá que desarrollar la etapa 1 que corresponde a monitoreo

y reconocimiento de las características de cada portal WEB, en la cual el responsable de cada aplicación entregará una tabla con las características de cada aplicación, para integrar al WAF, y no generar un impacto alto en el acceso de los usuarios.

En la siguiente tabla se presenta el ejemplo propuesto del diseño de la tabla que recogerá las características de cada servicio WEB que será migrada a la solución WAF.

	Oracle	MySQL	MSSQL	DB2	Sybase	PostgreSQL	¿Otro, cuál?						
Base de Datos	X												
	IIS	Apache	Apache Tomcat	Netscape Enterprise Server	IBM Lotus Domino	Nginx	IBM Websphere	Lighttpd	Jboss	Caucho Resin	Jrun Web Server	WebLogic	¿Otro, cuál?
Web Server	x												
	WordPress	Drupal	Struts	SharePoint	Otro, ¿cuál?								
Web Application					.Net C#								
	PHP	ASP	JSP	Otro, ¿cuál?									
Lenguaje				.Net C# e Interfaz: Js									

Tabla 4 Modelo Tabla de Signature -: Fuente Elaboración Propia

Dentro del desarrollo se deberá tener en cuenta que el modelo de proxy reverso al cual se acude, se tendrá una arquitectura de trafico de red lógico en el cual el WAF será quien reciba las peticiones del usuario final (interno como externo), lo cual demanda la creación de un ambiente virtual, que para este documento llamaremos VIP, en donde se tendrá un direccionamiento nuevo dentro de la red para los protocolos IPv4 como IPv6. [13]

Dicho direccionamiento virtual tanto a nivel de las reglas del Firewall como los NAT

de los virtual IP de las reglas serán los que existirán en el destino desde los usuarios, y se generarán unas nuevas reglas y zonas desde la arquitectura lógica del Firewall en donde la nueva zona VIP se comunicará hacia la Red física de los servidores, en su segmento DMZ, que conocemos con el levantamiento de información. [10]

En la siguiente ilustración se platea la topología final de la integración.

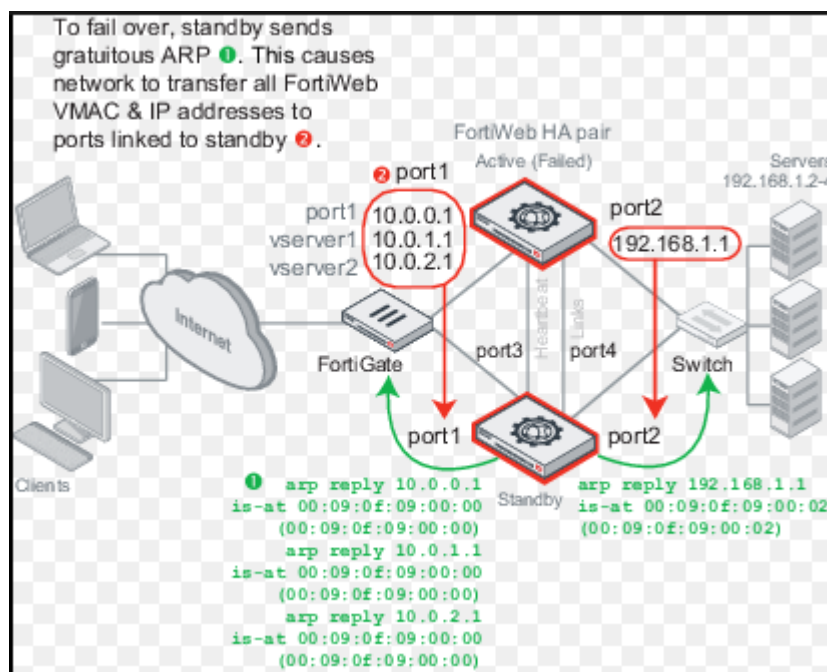


Ilustración 23. Modelo Proxy Reverso Ejemplo – Fuente Internet:
(<https://www.google.com/url?sa=i&url=https%3A%2F%2Fhelp.fortinet.com%2Ffwweb%2F561%2FContent%2FFortiWeb%2Ffortiweb-admin%2Fha.htm&psig=AOvVaw0v00S6ffwCvVAmvt0ygoCc&ust=1667066622433000&source=images&c&d=vfe&ved=0CA0QjhqFwo>)

En la etapa 2, posterior al monitoreo y autoaprendizaje hecho por la plataforma WAF, en cuanto a las funcionalidades de Machine Learnig, se desactivará el

modo MONITOR en las reglas del WAF, para cada servidor pool creado que se asociará a los servidores WEB relacionados en la “*Tabla 3 Aplicaciones WEB CAR - Fuente propia, tomado del levantamiento de información*”.

5.3.4. OPTIMIZACIÓN DE LA SOLUCIÓN

Por último, dentro del desarrollo de un proyecto en esta envergadura se prevé el desarrollo de una etapa de estabilización en la cual este comprendido el monitoreo, afinamiento de la solución y cierre, que garanticen a la CAR Cundinamarca la confianza buscada respecto al servicios prestados por sus portales WEB, en cuanto al acceso a la información y cumplimiento de los pilares de seguridad de la información.

En su alcance mínimo se contempla:

- Monitorear el consumo y estado de procesamiento de la plataforma WAF, procurando su buen desempeño.
- Analizar los eventos e información capturada, para afinar constantemente las reglas y políticas que se asocian a cada sistema de información.
- Analizar el costo y apropiación de la plataforma por el equipo de TI de la CAR.

6. ASPECTOS LEGALES Y CONTRATACIÓN

El presente proyecto se basa en la naturaleza, características y objeto a contratar y con el propósito de solucionar la necesidad de la CAR, desde la emisión del presente documento se confía procedente el uso de Licitación Pública regulado por la ley 1150 de 2007 artículo 2º numeral 1º y el Capítulo 2 DISPOSICIONES ESPECIALES DEL SISTEMA DE COMPRAS Y CONTRATACION PUBLICA, de la Sección 1 – MODALIDADES DE SELECCIÓN, y Subsección 1 - LICITACIÓN PÚBLICA, el artículo 2.2.1.2.1.1.1. y siguientes del Decreto 1082 de 2015 y la Ley 1882 de 2018. [1]

En este sentido, el numeral 1 del artículo 2 de la Ley 1150 de 2007, dispone: [5]

“ARTICULO 2 DE LAS MODALIDADES DE SELECCIÓN. La escogencia del contratista se efectuará con arreglo a las modalidades de selección de licitación pública, selección abreviada, concurso de méritos y contratación directa, con base en las siguientes reglas: 1. Licitación pública.

Con lo expuesto, se precisa, que al consultar con la secretaria general se confirma que la menor cuantía para la Corporación Autónoma Regional de Cundinamarca CAR [1] es de \$100.000.001 hasta \$1.000.000.000, que fue establecido por la Corporación según Circular de sistema de información SIDCAR.CAR.GOV.CO con No. 20224000164 del 12 de mayo de 2022. [5]

CONCLUSIONES

El presente documento nos ha permitido comprender que las soluciones perimetrales como un Firewall o un antivirus no están dedicadas a la protección de portales WEB, ya que su alcance está en capas inferiores del modelo OSI respecto al acceso a la Red mas no a protección a capas superiores, en donde la interfaz de usuario está ligadas al código de la aplicación y protocolos HTTP y HTTPS.

Se reconoce que la necesidad de una Red Corporativa de proteger los servicios WEB demanda el trabajo en equipo de los integrantes de una oficina general, ya que la inclusión de seguridad a los servicios WEB requiere un conocimiento especializado, en cuanto a los motores de la aplicación como de los motores de las bases de datos, y servicios integrados como API para las líneas de conexión.

El uso de nuevas tecnologías, agilizan los procesos de control de la seguridad informática y ciberseguridad, respecto a la automatización y agilidad en la protección de tiempo real como mitigación de riesgos.

REFERENCIAS

- [1] CAR Inc., «Corporación Autónoma Regional Cundinamarca,» 2020. [En línea]. Available: <https://www.car.gov.co>. [Último acceso: 7 Octubre 2022].
- [2] G. Gartnet Inc., «"Las principales tendencias tecnologicas estratégicas de Gartner para 2023",» 2022. [En línea]. Available: <https://www.gartner.es/es/tecnologia-de-la-informacion/insights/principales-tendencias-tecnologicas..> [Último acceso: 11 Octubre 2022].
- [3] J. T. Tejedor, «"¿En qué consiste el hardening?",» 3 Marzo 2022. [En línea]. Available: <https://es.linkedin.com/pulse/en-qu%C3%A9-consiste-el-hardening-jose-tejedor-leyva>. [Último acceso: 11 Octubre 2022].
- [4] Banco de la Republica Inc., «Sectores Económicos,» 2022. [En línea]. Available: <https://www.banrepcultural.org/blaavirtual/ayudadetareas/economia/econo53.htm>. [Último acceso: 17 Noviembre 2022].
- [5] C. C. E. Colombia Compra Eficiente Inc., «Guía para la elaboración de estudios de sector. Manual CCE-EIGP-GI-18._gees_v.2,» 27 Diciembre 2013. [En línea]. Available: <https://www.colombiacompra.gov.co/manuales-guias-y-pliegos-tipo/manuales-y-guias/guia-para-la-elaboracion-de-estudios-de-sector>. [Último acceso: 21 Noviembre 2022].
- [6] D. DANE Inc., «"Producto Interno Bruto (PIB) II trimestre de 2022", Boletín Técnico Preliminar,» 16 Agosto 2022. [En línea]. Available: https://www.dane.gov.co/files/investigaciones/boletines/pib/bol_PIB_IITrim22_produccion_y_gasto.pdf. [Último acceso: 17 Noviembre 2022].
- [7] Acopi Inc, «"Estudios Economicos", Doc Tech,» 2022. [En línea]. Available: <https://www.acopi.org.co/estudios-economicos/>. [Último acceso: 17 Noviembre 2022].
- [8] D. DANE Inc, «"Cuenta satélite de las tecnologías de la información y las comunicaciones", Boletín Técnico 2021,» 18 Marzo 2022. [En línea]. Available: <https://www.dane.gov.co/files/investigaciones/pib/tic/bt-satelitet-2021pr.pdf>. [Último acceso: 17 11 2022].
- [9] Bahamón-Jara, M. L, «Análisis de la normatividad en contratación pública,» Colección Jus Público No. 26, Bogotá: Universidad Católica de

- Colombia, 2018. [En línea]. Available:
https://repository.ucatolica.edu.co/bitstream/10983/20285/1/Elementos-y-presupuestos-de-la-contratacion-estatal_Cap04.pdf.
- [10] PCI Security Standard Council Inc, «Application Reviews and Web Application Firewalls Clarified,» 2008. [En línea]. Available:
<https://listings.pcisecuritystandards.org>. [Último acceso: 8 Octubre 2022].
 - [11] Akamai Inc, «"Análisis de la nueva era de la seguridad de la información", Tech Doc Estado de Internet,» 2021. [En línea]. Available:
<https://www.akamai.com/es/our-thinking/the-state-of-the-internet/global-state-of-the-internet-security-ddos-attack-reports>. [Último acceso: 2 Diciembre 2022].
 - [12] DOI Inc. , «"Penetration Testing", Tech Doc.,» U.S. Department of the Interior, [En línea]. Available:
<https://www.doi.gov/ocio/customers/penetration-testing>. [Último acceso: 8 Octubre 2022].
 - [13] Tecon Inc., «"Seguridad de la Información", Blog,» 2018. [En línea]. Available: <https://www.tecon.es/la-seguridad-de-la-informacion/>. [Último acceso: 2 Diciembre 2022].
 - [14] B-Secure Inc., «"Firewall de aplicaciones Web - WAF, Tech Doc,» 2022. [En línea]. Available: <https://www.b-secure.co/estrategias/aplicaciones/firewall-aplicaciones-web>. [Último acceso: 2 Diciembre 2022].
 - [15] Min-Tic Inc, «"Lineamientos y estándares para la estrategia de seguridad digital", Ministerio de Tecnologías de la Información y las Comunicaciones Resolución 00500,» 10 Marzo 2021. [En línea]. Available: https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf. [Último acceso: 8 Octubre 2022].
 - [16] D. DANE Inc, «"Índice de precios al consumidor", Boletín Técnico Septiembre 2020,» 5 Octubre 2022. [En línea]. Available:
https://www.dane.gov.co/files/investigaciones/boletines/ipc/bol_ipc_sep20.pdf. [Último acceso: 17 Noviembre 2022].
 - [17] Min-Tic Inc, «"Modelo de Seguridad y Privacidad de la Información", Ministerio de Tecnologías de la Información y las Comunicaciones, Resolución 000746,» 11 Marzo 2022. [En línea]. Available:
https://www.mintic.gov.co/portal/715/articles-208143_recurso_1.pdf. [Último acceso: 8 Octubre 2022].
 - [18] x|

