CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC

INVESTIGADORES

DIEGO ARMANDO GARCIA ALTAMIRANDA

JAIDER VERGARA UTRIA

UNIVERSIDAD DE CARTAGENA

FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS D. T. y C.

2019

CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC

Investigadores

DIEGO ARMANDO GARCIA ALTAMIRANDA

JAIDER VERGARA UTRIA

Directora

YASMÍN MOYA VILLA – UNIVERSIDAD DE CARTAGENA

Asesora

YENIS ALVAREZ JÍMENEZ – BIOFILM S.A.

PROYECTO DE GRADO PRESENTADO COMO REQUISITO PARCIAL PARA OPTAR AL TÍTULO DE INGENIERO DE SISTEMAS

UNIVERSIDAD DE CARTAGENA
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS
CARTAGENA DE INDIAS

2019

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Cartagena de Indias D.T. y C.

2019

DEDICATORIA

La realización de este trabajo, primeramente, es dedica a Dios nuestro creador por ser el camino a la salvación, el dador de perseverancia y quien nos llena de bendiciones cada día.

A nuestros padres quienes son la representación del amor de Dios en la tierra. Ellos son quienes nos impulsan a continuar y perseverar para alcanzar nuestras metas y objetivos, teniendo siempre presente el amor de la familia y, sobre todo, el amor hacia Dios.

También a todas aquellas personas que nos orientaron en el camino universitario. Nuestros profesores y amigos por ayudarnos a adquirir conocimientos constructivos y por estar en disposición de ayudarnos constantemente.

Una dedicatoria muy especial a la Ingeniera y profesora de la Universidad de Cartagena Yasmín Moya Villa, porque además de cumplir su papel de docente, nos sirvió de apoyo incondicional en los momentos más difíciles, y siempre con la mejor disposición. Así mismo, a los Ingenieros de la empresa BIOFILM S.A, Yenis Álvarez Jiménez, Elkin de Castro, Jorge Rivera y Juan Vertel, por confiar en nuestras capacidades y brindarnos las herramientas necesarias para culminar con el trabajo de grado de buena manera. A todos, muchas gracias.

AGRADECIMIENTOS

“Inicialmente agradezco a mi Dios por permitirme alcanzar este gran logro en mi vida, por llenarme de bendiciones diariamente, y por entregarme la fortaleza moral y espiritual para perseverar en las etapas difíciles. Toda la honra y la gloria sea para él.

Del mismo modo, le agradezco por colocar en mi camino, todas esas personas que fueron constructivas en mi vida y, en especial, en mi etapa universitaria. A mi mamá, hermanos y abuela materna, por ser mi motor, mi fuente de inspiración, mi razón de lucha y de superación. A mi papá que, ante cualquier adversidad, es mi ejemplo, mi espejo y mi apoyo.

Especialmente agradezco a mi abuela paterna, la luz de mis ojos, por ser bondadosa y generosa conmigo, pero sobre todo por demostrarme ese amor inmenso e incondicional. Por supuesto, también le agradezco infinitamente a mi tío Isaac por confiar en mí y mis capacidades, por ser mi apoyo, mi ejemplo profesional, e impulsor de mis sueños. Este triunfo es suyo.

Tampoco puedo dejar de lado, al sin número de personas, tíos, primos, amigos, que siempre me ofrecieron apoyo moral con sus buenos deseos y bendiciones. Ellos con pequeños detalles, me demostraron su cariño. A todos ustedes, mis más sinceros agradecimientos.

Esta dicha que hoy me posee, quiero compartirla con todos ustedes. Muchas gracias por su apoyo.”

Diego Armando García Altamiranda.

"*El presente trabajo investigativo lo dedicamos principalmente a Dios, por ser el inspirador y darnos fuerza para continuar en este proceso de obtener uno de los anhelos más deseados.*

A nuestros padres, por su amor, trabajo y sacrificio en todos estos años, gracias por ser los principales promotores de nuestros sueños, por confiar y creer en nuestras expectativas, por los consejos, valores y principios que nos han inculcado.

Así mismo agradecerle a nuestros hermanos, por acompañarnos en este arduo proceso, y siempre brindarnos apoyo moral, con sus palabras que nos hacían sentir orgullosos. De igual forma gracias y mil gracias a nuestros amigos y compañeros, quienes fueron nuestros mayores aliados en este largo proceso, compartiendo sus conocimientos y aportándonos a nuestro crecimiento personal y profesional.

Gracias a nuestra universidad, por habernos permitido formar y en ella, gracias a todos nuestros maestros que fueron participes de este proceso, ya sea de manera directa o indirecta, gracias a todos ustedes, fueron ustedes los responsables de realizar su pequeño aporte, que el día de hoy se vería reflejado en la culminación de este proyecto de grado.

Para finalizar queremos hacer una dedicatoria especial a la directora de este proyecto, YASMIN MOYA VILLA, quien nos apoyó de principio a fin, siempre haciéndolo de la mejor forma, aportándonos muchos conocimientos, que permitieron concluir este proyecto de grado exitosamente. Además agradecerle por contribuir a nuestro crecimiento personal a través de sus buenos consejos. También queremos hacer una dedicatoria especial a la ingeniera YENIS ALVAREZ, quien fue la persona que nos brindó la confianza para ejecutar este proyecto de grado en la empresa BIOFILM S.A, apoyándonos incansablemente en las gestiones pertinentes en la empresa, a lo largo de este proyecto. Finalmente, también queremos agradecer al personal administrativo designado, para apoyarnos en cada una de las diferentes etapas de este trabajo de grado. Gracias a todos ustedes, y sobre todo gracias a BIOFILM S.A, por confiar en nosotros.

Finalmente gracias a la vida por este nuevo triunfo, gracias a todas las personas que nos apoyaron y creyeron en la realización de este proyecto de grado."

Jaider Vergara Utria.

CONTENIDO

LISTA DE FIGURAS.

LISTA DE TABLAS

TABLA DE GRÁFICAS

1. RESUMEN

El proyecto titulado CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC, se realizó con el objetivo de construir dos controles como mecanismos para el fortalecimiento de la seguridad de la información (SdI) y potencializar los procesos operativos concernientes a esta temática, llevados a cabo por los dominios de Telecomunicaciones y Recursos Humanos (RRHH) de la empresa BIOFILM S.A., ubicada en la zona industrial de la ciudad de Cartagena de Indias D. T. y C.

La metodología mixta utilizada para la elaboración del proyecto, permitió la adquisición adecuada de las herramientas y recursos pertinentes para la realización y cumplimiento de los objetivos propuestos para llevar a feliz término la ejecución del proyecto. Esta metodología se basó en el desarrollo por objetivos, para lo cual se hizo necesario la adopción de una investigación aplicada bajo documentos, reuniones, entrevistas, pruebas y la utilización de otros tipos de metodologías puntuales para los objetivos de desarrollo de software. En este proceso, el personal competente puesto a disposición por la empresa, cumplió un papel fundamental por servir de apoyo y acompañamiento de las estrategias adoptadas para el cumplimiento de los objetivos.

Con la utilización de tecnologías para el desarrollo de aplicativos móviles, objetos virtuales de aprendizaje y el uso de herramientas de gestión de redes, se logró la creación de herramientas como controles que fortalecieron los procesos llevados a cabo por los dominios de Telecomunicaciones y RRHH, concernientes con la gestión de la SdI.

La realización de este proyecto, inició una relación directa entre la Universidad de Cartagena y BIOFILM S.A., para la realización de trabajos e investigaciones conjuntas entre ambas instituciones. Lo que permitió aumentar el nivel académico de la Universidad y generar beneficios para la empresa, además de ayudar a cumplir con la intención de la Universidad de Cartagena de formar profesionales competentes al servicio de la ciudadanía y la comunidad en general.

Palabras claves: *Seguridad de la Información, TIC, Controles, Metodología Mixta, Desarrollo por objetivos, Telecomunicaciones, Recursos Humanos, Estrategias, Tecnologías, BIOFILM S.A., Universidad de Cartagena.*

2. ABSTRACT

The project entitled CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS ICT, was held with the aim of building controls as mechanisms for the strengthening of the security of information (SdI) and enhance operational processes concerning this topic, carried out by the domains of Telecommunications and Human Resources (HR) of BIOFILM S.A. company, located on the industry zone in Cartagena de Indias D.T. and C.

The joint methodology for the elaboration of the project, allowed the proper acquisition of the tools and relevant resources for the implementation and fulfilment of the objectives APProved to carry out the purpose of the project. This methodology was based on the development objectives, within which, is comply with them is necessitated the adoption of a research under documents, meetings, interviews and tests, and also the use of others types of specific methodologies for software development. In this process, the staff made available by the company, was instrumental for serving support and accompaniment of the strategies adopted and for the fulfilment of the objectives and methodologies.

Technologies included ICT for the development of APPlications using mobile, virtual learning objects and the use of network management tools was creation of tools such as controls that strengthened the processes carried out by Telecommunications and Human Resources divisions, concerned with the management of SdI.

The realization of this project, start a direct relationship between the University of Cartagena and BIOFILM S.A., for the realization of joint work and investigations between both institutions, what allows to increase the academic level of the company, besides helping to fulfill with the intention of the University of Cartagena to train competent professional to the service of the citizenship.

Palabras claves: *Security of Information, ICT, Human Resources, Strategies, Telecommunications, BIOFILM S.A., University of Cartagena, Technologies, Controls, Mixed Mythology, Development by Objectives.*

3. INTRODUCCIÓN

En la actualidad, las organizaciones constantemente se enfrentan a diversas vulnerabilidades a nivel de seguridad de la información, de ahora en adelante SdI, que ponen en riesgo su patrimonio. En ese aspecto, uno de los puntos críticos es el tratamiento de la información al interior de dicha organización, dado que se requiere mantener muchas veces confidencialidad en los diversos procesos llevados a cabo, a fin de que estos se ejecuten de manera correcta, sin presentar sobresaltos que pongan en riesgo el funcionamiento del sistema en general. Por lo tanto, contar con herramientas y planes adecuados para el tratamiento de la información y fortalecimiento de la SdI, no solo permite que una empresa optimice sus procesos, sino también que ayude a su consolidación.

Por consiguiente, este proyecto fue propuesto como una posible solución a los problemas que traen las nuevas necesidades del mercado, y que estuvieron presentes en la empresa BIOFILM S.A.[1], más específicamente en los dominios de Telecomunicaciones y Recursos Humanos, de ahora en adelante RRHH, concernientes a TI en el ámbito de la SdI. Dentro de los cuales destacó la necesidad de actualizar y fortalecer la infraestructura de red, mediante la implantación de una herramienta SIEM[2] acorde con la industria y sus problemáticas, con la finalidad de poder soportar las exigencias tecnológicas del mercado y la expansión de la empresa. De igual modo, también existió la dificultad sobre el poco conocimiento de las políticas de SdI que la empresa poseía, por parte de los empleados de la planta. La solución a esta última problemática radicó en la creación de una estrategia dividida en dos ítems: 1) Desarrollo de un aplicativo móvil para la plataforma Android; 2) Creación de un Objeto Virtual de Aprendizaje (OVA[3]) desplegado en el Servidor de Archivos empresarial. Ambos tienen la intención de ser una estrategia para la divulgación, concientización y evaluación al personal de trabajo sobre las políticas de seguridad de BIOFILM S.A. En general, la solución a cada uno de los problemas descritos, conformaron los controles para la gestión de la SdI.

[1] BIOFILM S.A.: Empresa fabricante de polipropileno biorientado con más de 20 años de experiencia. < http://www.biofilm.com.co/g>

[2] SIEM: Término utilizado para señalar a las herramientas relacionadas con la seguridad de la información y administración de eventos dentro de un contexto informático. Básicamente consiste en brindar la oportunidad de monitorear en tiempo real, todos los sistemas, componentes de redes, bases de datos y aplicaciones a las cuales esté asociada dicha herramienta.

[3] OVA: Es un conjunto de recursos digitales, auto contenibles y reutilizable, con un propósito educativo.

Los controles planteados en el desarrollo de este proyecto, estuvieron orientados a los dominios de Telecomunicaciones y RRHH, de la planta de producción central de BIOFILM S.A. ubicada en la zona industrial de Cartagena de Indias D.T y C, Colombia.

Como proyecto investigativo, éste se desarrolló bajo la línea de investigación de las Tecnologías de la Información y las Telecomunicaciones del grupo GIMATICA[4], perteneciente al programa de Ingeniería de Sistemas de la Universidad de Cartagena, debido a la afinidad que tiene con los temas de SdI e infraestructura de redes.

[4] GIMATICA: Grupo de Investigación en Tecnologías de la Comunicación e Informática del Programa de Ingeniería de Sistema de la Facultad de Ingeniería de la Universidad de Cartagena.

4. PLANTEAMIENTO DEL PROBLEMA

4.1. DESCRIPCION DEL PROBLEMA

Las organizaciones tanto públicas como privadas, con las exigencias del mercado obtienen necesidades a nivel de las tecnologías de la información que ameritan ser solucionadas. Al interior de las empresas, la infraestructura tecnológica es quizás la que más sufre con estos cambios. Por tal motivo, éstas deben adoptar planes y herramientas tecnológicas que permitan revisar, analizar y mejorar sus controles a nivel de SdI, y de ese modo preservar la integridad, disponibilidad y confidencialidad de la información, para mejorar la prestación de servicios y el fortalecimiento de los procesos operacionales. (Delgado Mendieta & Suárez Asencio, 2015)

Del mismo modo, procesar las grandes afluencias de datos, peticiones y movimientos que atienden las empresas dentro de la red, plantea un reto al momento de gestionar en tiempo real todas estas actividades que se desarrollan en la infraestructura de red, utilizando los dispositivos conectados a la misma, con el fin de identificar problemas de seguridad y de rendimiento, especialmente cuando la infraestructura de hardware es limitada. Los proveedores de servicios de seguridad administrados (MSSP[5]), quienes poseen sus servicios y aplicaciones en la nube, reciben eventos y actividades de forma abrumadora. Por ende, es crítico procesar estos datos eficientemente, de modo que los ataques pudieran ser identificados rápidamente y la respuesta necesaria podría ser iniciada.(Alam, Ihsan, & Khan, 2016)

Por consiguiente, la manipulación y el tratado de todos los movimientos que se presentan en la red, al igual que el constante monitoreo de la infraestructura tecnológica, es trabajo tedioso y complejo que amerita la implantación e implementación de herramientas creadas especialmente para identificar y combatir los movimientos y las amenazas que se presentan en la red, y de ese modo evitar los problemas de seguridad informática para la empresa cada vez que se accede a los servicios alojados en los servidores.

Los problemas de seguridad sobre el robo y/o alteración de la información, generan pérdidas económicas, al igual que el caos interno y la pérdida de credibilidad. Estas son amenazas prioritarias de las cuales se debe cuidar la empresa. Los acontecimientos enunciados

[5] MSSP: Son empresas que participan del mercado de la administración o monitoreo remoto de las funciones de las Seguridad de TI usando recursos compartidos desde centros de operaciones de seguridad.

anteriormente, pueden suceder por las vulnerabilidades que ofrecen los dispositivos asociados a la infraestructura de red y los sistemas de información, al igual que la falta de control sobre ellos por parte de una herramienta de gestión de redes que pueda atender todos los equipos, dispositivos, peticiones y amenazas presentes en la misma. Los hechos se pueden evitar con la correcta implantación de una herramienta de gestión, control y monitoreo de riesgos de seguridad sobre la infraestructura de red, y un permanente seguimiento de la misma.

Por otro lado, el pleno conocimiento de las políticas de seguridad de cada empresa por medio de sus trabajadores, genera confianza y estabilidad interna sobre los procesos y actividades desarrolladas dentro y fuera de ella. Sobre lo cual, el poco conocimiento de las políticas de seguridad por parte de los empleados, se convierte en una problemática para cualquier industria, que debe ser corregida mediante el uso y puesta en marcha de estrategias metodológicas que permitan la divulgación, aprendizaje y evaluación de las políticas de seguridad de la empresa, al igual que un control sobre su cumplimiento.

Estas problemáticas la mayoría de veces son conocidas por la empresa, pero no solucionadas, hasta que un agente externo los instruye sobre el valor del cumplimiento y utilización de las mismas, con el fin de evitar grandes problemas. Escenario ocurrido en la empresa BIOFILM S.A., qué después de una auditoría global desarrollada por terceros contratados, se detectaron dichas problemáticas en los dominios de Telecomunicaciones y RRHH, englobados bajo la norma ISO 27000[6] en el marco de la SdI.

En BIOFILM S.A. en el dominio de Telecomunicaciones, las exigencias del mercado y la modernización constante que sufre como empresa, la impulsan a poseer una infraestructura de red capaz de soportar todas las peticiones sobre los servicios alojados en los servidores y demás dispositivos, y responder de buena forma ante ellas. En este proceso, la red está expuesta a intrusos, virus y cualquier tipo de ataques que buscan entorpecer las labores y prestaciones que normalmente se hacen en cada uno de los dominios de la empresa, donde utilizan la red como medio. Las implicaciones que traen consigo las exposiciones a los ataques y el asecho de los mismos, generan, para mal de la empresa, problemas de toda índole. Por tal motivo, fue importante implantar una herramienta SIEM que permitiera disminuir todos estos riesgos, con el

[6] ISO 27000: Es una serie establecida de normas de seguridad de la información para las empresas y organizaciones de toda índole.

fin de evitar los problemas informáticos y sus similares que tanto daño le podían causar a la empresa.

Anteriormente, el dominio de Telecomunicaciones de la empresa BIOFILM S.A. implementaba como mecanismo de protección contra incidentes de seguridad sobre la infraestructura de red, una herramienta NAGIOS[7] para revisar la disponibilidad y estado de servicios y dispositivos. Esta herramienta en su momento ofrecía una protección completa sobre los equipos y servicios de las redes, pero con el paso del tiempo y la modernización de las herramientas hardware y software de los sistemas de información y de redes, se crea la correlación de eventos para detectar múltiples sucesos anómalos en el sistema, asociarlos a una amenaza y alertar al administrador de la red para que se tomen medidas que los contrarresten. Esta característica no está presente en las herramientas NAGIOS, por lo que ha quedado relegada a un segundo plano al momento de monitorizar, prevenir y contrarrestar grandes afluencias de ataques y movimientos no deseados, sobre los dispositivos que componen la infraestructura de red. Permitiendo de este modo, que existan variados eventos extraños relacionados que pueden afectar el funcionamiento normal de la red, y estos no sean detectados como amenazas, sino como eventos aislados que no representan problema alguno para el funcionamiento de la misma. Por lo anterior, existió la necesidad por parte de la compañía, de cambiar la herramienta NAGIOS de protección contra incidentes de seguridad utilizada en la infraestructura de red.

Por otro lado, no sólo los problemas en el medio de la informática son los que amenazaban a BIOFILM S.A., también existía una problemática presente en el dominio de RRHH generada por la falta de conocimiento y uso de las políticas de seguridad de la empresa por parte de los empleados. Debido a esto, se creó la necesidad de generar una estrategia como mecanismo de conocimiento, concientización y aprendizaje de dichas políticas, que ayudara a disminuir los desaciertos que produce el poco conocimiento de éstas por parte de sus empleados.

La divulgación de las políticas de seguridad que utilizaba el dominio de RRHH de la empresa BIOFILM S.A. no era la más efectiva al momento de fomentar el conocimiento, aprendizaje y la puesta en marcha de esas políticas, debido a que utilizaban los contratos como método de divulgación de las mismas, medio que por lo general sólo se emplea una vez. Igualmente,

[7] NAGIOS: Es un sistema de monitorización de equipos y de servicios de red, creado para ayudar a los administradores a tener el control de la misma.

utilizaban indicativos e instructivos impresos ubicados en los tableros informativos, los cuales son fáciles de desechar y/o hacer caso omiso, lo que directamente incide en un desperdicio de tiempo, dinero y esfuerzo por parte de las personas encargadas de la divulgación por este medio, y directamente sobre la empresa. Por ende, se propuso una estrategia que permitiera y potencializara el aprendizaje de las políticas de la empresa sobre la SdI, disminuyendo el poco conocimiento que tienen los empleados sobre estas políticas. Esta estrategia consistió en la creación de un OVA que fue anexado al LMS de la empresa, como mecanismo de enseñanza/aprendizaje de las políticas de seguridad de la información, y la creación de un aplicativo móvil como medio de evaluación de los conocimientos adquiridos con el uso del OVA. Dicha estrategia está expuesta en el desarrollo de este proyecto como uno de los controles para la gestión de la SdI en la empresa.

4.2. FORMULACIÓN DEL PROBLEMA

¿Cómo fortalecer los procesos desarrollados bajo los dominios de RRHH y Telecomunicaciones para el mejoramiento en la gestión de la seguridad de la información dentro de BIOFILM S.A.?

5. JUSTIFICACION

Para las empresas, el creciente desarrollo del campo de las tecnologías de la información (TI) trae consigo muchos obstáculos que se deben afrontar día tras día para poder estar a la vanguardia de los tiempos. Dentro de este, la SdI es quizás una de las temáticas que a diario se debe estar retroalimentando, debido a las diversas problemáticas que surgen entorno al desarrollo de los sistemas informáticos para el tratamiento de información y sus similares, al igual que las nuevas metodologías y herramientas de ataques utilizadas por terceros para entorpecer las prestaciones de las empresas. Por tal motivo, se debe tener en cuenta la constante búsqueda de soluciones y la actualización de conocimientos para disminuir los inconvenientes que se presenten en cuestiones de TI. Para solventar esta problemática, surgen diversas herramientas software en el mercado que permiten la disminución de los inconvenientes mediante controles de seguridad y creación de sistemas de detección que ayudan a ejercer una gestión más adecuada sobre los diversos sistemas y software asociados a TI, manejados en la organización. Todo con el fin de mejorar la calidad en la prestación de servicios y potencializar la operatividad de la empresa.

Esta necesidad quedó evidenciada en los dominios de Telecomunicaciones de la empresa BIOFILM S.A. ubicada en la zona industrial de Cartagena de Indias D.T. y C., luego de una auditoría general hecha en la misma, enmarcada bajo la norma ISO 27000 en el concepto de SdI. Dicha necesidad es debida a que, BIOFILM S.A. por ser una empresa, siempre se encuentra en constante evolución de su infraestructura tecnológica, razón por la cual está sujeta al mercado y sus exigencias. Por este motivo, existió la necesidad de actualizar las herramientas utilizadas para la gestión de la infraestructura de red, con el fin de fortalecer las operaciones desarrolladas dentro de la planta para una mejor prestación de servicios, agilidad en la operatividad y preservación de la SdI.

Siguiendo este orden de ideas, dentro de los resultados de la misma auditoría enmarcados dentro de la SdI, en la división de RRHH se evidenció la necesidad de potencializar el conocimiento y la ejecución de las políticas que poseen a nivel de SdI, por parte de sus empleados. El desconocimiento de dichas políticas podía acarrear problemas como, impedir el correcto funcionamiento de la planta operacional. Debido a esto, existió la necesidad de crear una estrategia para la divulgación, aprendizaje y concientización de dichas políticas de seguridad, y

de ese modo evitar los inconvenientes presentados a nivel de SdI y sus derivados, por la falta de conocimiento de las mismas.

En este proyecto, se brindó solución a las problemáticas establecidas en los dominios de Telecomunicaciones y RRHH de la empresa BIOFILM S.A., creando dos controles como herramienta para la gestión de la SdI: 1) La implantación de una herramienta SIEM para el monitoreo de la infraestructura de red; 2) Creación de una metodología para la divulgación, aprendizaje y concientización de las políticas de seguridad. A su vez, éste último se conformó por la creación de un Objeto Virtual de Aprendizaje (OVA), que fue anexado al Sistema de Gestión de Aprendizaje (LMS) empresarial, para la enseñanza/aprendizaje de conocimientos concernientes a las políticas de SdI; y la creación de un aplicativo móvil para dispositivos móviles con plataforma Android, con el fin de evaluar los conocimientos de los empleados adquiridos mediante la utilización del OVA.

La creación de estos controles permitió la puesta en marcha de conocimientos actualizados sobre SdI y la gestión de infraestructura de red, orientadas a las empresas. Temáticas de gran interés e importancia para las organizaciones, por permitir la actualización de sus tecnologías y la preservación de la información mediante el fortalecimiento de la seguridad de las mismas.

Otro aspecto tenido en cuenta en el desarrollo de este proyecto, fue la presentación de una nueva forma para fortalecer la SdI para BIOFILM S.A, que a diferencia de la ya utilizada, fue de gran utilidad por el uso de herramientas actualizadas de gestión de redes, es decir, dejó a un lado la utilización de las herramientas NAGIOS por parte de la empresa en el monitoreo de redes, para implantar una herramienta SIEM que cumplió con las exigencias que habían adoptado los sistemas de gestión de redes para garantizar la seguridad de las mismas. La herramienta SIEM que se implantó a través de este proyecto, ofreció al sistema de gestión de redes que utiliza BIOFILM S.A., correlación de eventos para monitorear un conjunto de sucesos, asociarlos a una amenaza y alertar sobre ellos al administrador de la red. La funcionalidad de correlación de eventos de dicha herramienta, permite detectar eventos aislados aparentemente inofensivos y relacionarlos, para que sean detectados como amenazas y, posteriormente, notificar al administrador de la red sobre dichos eventos, logrando de esta manera se tomen las medidas necesarias.

Del mismo modo, para la divulgación, aprendizaje y concientización de las políticas de seguridad de la empresa, se hicieron a un lado las herramientas tradicionales para el cumplimiento de estas tareas, como textos impresos, charlas, capacitaciones, entre otros, y se procedió con tecnología de fácil uso y acceso, en este caso la utilización de aplicativos móviles y los servicios de internet como el LMS y el OVA.

Por otro lado, la realización de este proyecto inició una relación directa entre la Universidad de Cartagena y BIOFILM S.A., para la realización de trabajos e investigaciones conjuntas entre ambas instituciones, que ayuden a potencializar el conocimiento de los investigadores de los proyectos, además del intercambio de conocimientos que permiten aumentar el nivel académico de la Universidad. De igual modo, las documentaciones y los resultados formales del trabajo realizado, contribuyen a la parte científica de la Universidad y la impulsan como academia. Dentro de la Universidad de Cartagena, este proyecto por corresponder a la línea de investigación de Tecnologías de la Información y las Telecomunicaciones del grupo GIMATICA del programa de Ingeniería de Sistemas, ayuda a enriquecer las bases científicas del mismo y a seguir impulsándolo como grupo investigativo.

Otro aspecto relevante que permite este proyecto, es la disminución del uso del papel para la divulgación de las políticas de seguridad y la evaluación de las mismas; debido a la utilización de herramientas tecnológicas, el papel queda relegado a un segundo plano, lo que permite ver la contribución ambiental que tienen los controles como solución a los problemas planteados por la empresa, y a su vez la ayuda en la parte económica por el ahorro de dinero y recursos invertidos en la impresión de hojas y folletos que contengan información sobre las políticas de SdI.

De igual modo, como factores de viabilidad económica del proyecto, se destaca lo siguiente: 1) No hubo necesidad de contratar a terceros para la implementación de los controles; 2) La Universidad de Cartagena suministró en especie el tiempo de la directora del proyecto; 3) La empresa BIOFILM S.A., delegó parte de su personal para brindar las tutorías necesarias a este proyecto, lo cual fue aportado en especie por parte de la misma empresa; 4) La herramienta SIEM implantada es de código abierto (Open Source); 5) No se necesitó personal extra en las charlas y capacitaciones, para divulgar y concientizar sobre el uso de las políticas de seguridad; 6) La herramienta SIEM, indirectamente, relegó el uso de hardware y software costosos en el control y monitoreo de los sistemas de información que tienen relación directa con la

infraestructura de red y la SdI; 7) La licencia de la herramienta utilizada para crear el OVA, es de bajo costo.

6. MARCO DE REFERENCIA

6.1. ESTADO DEL ARTE

Es tedioso hablar de los diferentes esfuerzos que han hecho los especialistas en el campo de la seguridad de la información a lo largo de la historia, para contrarrestar los efectos negativos que plantea el reto de la seguridad. Es por ello, que en esta sección se enfatizó solo en las eventualidades presentes a lo largo de esta última década. Así mismo, se estructuró el estado del arte en cuatro apartados, el primero dedicado al ámbito internacional, seguido por un referido al desarrollo a nivel nacional, luego se presentó uno para el nivel local, y el último corresponde al análisis de la información encontrada para cada panorama.

6.1.1. PANORAMA INTERNACIONAL

En el año 2015 se planteó en la Universidad Politécnica Salesiana con sede en Quito, Ecuador, una propuesta de mejoramiento de la herramienta OSSIM SIEM para obtener los niveles óptimos de la gestión en la administración de la seguridad, en una red implementada en el cloud computing. La cual consiste en mejorar la función de la herramienta con el fin de aprovechar al máximo sus funcionalidades y prestaciones. La optimización de la herramienta permite generar un sistema robusto basado en la identificación de amenazas en tiempo real y su mitigación. (Balarezo Chávez & Poveda Pilatasig, 2015).

También en el 2015, en la Escuela Superior Politécnica del Litoral (Quito, Ecuador), se implanto una herramienta OSSIM para el monitoreo y gestión de la seguridad de la red y plataformas Windows y Linux aplicado a empresas medianas. Cuyo fin es la implantación de OSSIM en una empresa con servidores en producción, para poder integrar todos los registros, basándose en la identificación de los logs generados a partir de las peticiones hechas a los servidores, por parte de cada uno de los equipos conectados a la red. (Villafuerte Quiroz & Bravo Bravo, 2015a).

De igual modo, en el año 2015 en la Universidad Carlos III de Madrid (España), se desarrolló un escrito que proporcionó un método para hacer que la herramienta SIEM fuese capaz de auto adaptarse a ataques nuevos y de ese modo optimizar y reducir significativamente la intervención de los operadores. Implementando la programación genética, se logra hacer que la herramienta

automáticamente aprenda y produzca reglas de correlación basadas en el contexto para diferentes tipos de ataques multipaso. Esto permite que se puede tener un control más actualizado sobre las nuevas amenazas que se plantean en el exterior. (Suarez-Tangil, Palomar, Ribagorda, & Sanz, 2015).

En el año 2016 en la Universidad Regional Autónoma de los Andes de Ecuador, se estableció una propuesta de investigación para la seguridad operacional en las PYMES de la ciudad de Pepileo, Ecuador, que busca mediante la implementación de una herramienta SIEM, establecer un control adecuado de las actividades operacionales de las PYMES, aportando al mejoramiento de la seguridad institucional. Lo que implica que el uso de las SIEM permite el mejoramiento de las estructuras operacionales basadas en las redes y los sistemas de información, nutriéndolos de mejoras en el control y la gestión de eventos, logrando mantener la integridad de las actividades institucionales. (Pico Barrera, 2016).

También en el año 2016, en la Universidad Pace de Nueva York, Estados Unidos, se propuso mediante un escrito detallado, las ventajas de la implementación de herramientas SIEM para el monitoreo de redes sobre las técnicas tradicionales. Se describe las características principales que otorgan la utilización de dichas herramientas y la insuficiencia de los métodos tradicionales para soportar los ataques cibernéticos. Este estudio demuestra una vez más, la importancia que tiene la implementación de las SIEM en el monitoreo de las redes de datos y los sistemas de información. (Thakur et al., 2016).

Un año después, es decir, año 2017, se desarrolló un artículo de nombre "Towards a system for complex analysis of security events in large-scale networks", en el cual presentan un nuevo prototipo de SIEM para corregir las fallas que pueden contener lo actuales, con respecto a la normalización de fuentes de datos heterogéneas, un alto número de alertas falsas positivas y largos tiempos de análisis, en redes de gran volumen de eventos de seguridad. Para lograr solucionar esos inconvenientes, en el prototipo propuesto analizan datos normalizados utilizando una combinación de tres enfoques diferentes para el análisis de seguridad: detección de uso indebido, análisis basados en consultas y detección de anomalías. Pero, sobre todo, basándose en un novedoso algoritmo híbrido de detección de valores atípicos que devuelve grupos de anomalías clasificadas, el cual permite que el administrador de la red se concentre en las varias

anomalías mejor clasificadas, en lugar de buscar en un grupo de eventos sospechosos sin clasificar. (Sapegin, Jaeger, Cheng, & Meinel, 2017).

Pero no sólo la herramienta OSSIM ha sido utilizada para estudios e implementaciones a nivel empresarial o educativo. En el año 2015, en el Instituto Politécnico do Porto, Portugal, se realizó un estudio comparativo entre distintas herramientas SIEM para la gestión de eventos de seguridad. Para ello se basaron en la investigación y utilización de las herramientas OSSEC, GRAYLOG, PRELUDE-SIEM, y OSSIM en un entorno real, y por medio de los resultados obtenidos y las conclusiones, hicieron la comparación de las mismas. En dicho cotejo, no exaltan ni destacan a una con referencia a las demás, debido a que todas tienen potencial para rendir en la industria. La utilización de una o alguna de ellas, estará ligada directamente a las necesidades y el entorno de la empresa. (João Pedro G. Alves, 2015).

Del mismo modo, en el 2015 se realizó un artículo en el cual se muestran todas las bondades y características de la herramienta Graylog SIEM para soportar, analizar y gestionar grandes cantidades de datos. Definen a la herramienta como un sistema integrado para recopilar, indexar y analizar datos estructurados y no estructurados de casi cualquier fuente. En este artículo, le otorgan toda la facultad a Graylog de ser una herramienta de análisis de registro empresarial al alcance de las organizaciones que no cuentan con los recursos para soluciones comerciales costosas o alternativas de código abierto. (Graylog Inc., 2015).

En el año 2016, en la Universidad de Kansas, Estados unidos, se realizó un trabajo de grado en el que implementan un marco del modelo de cadena de muerte en una herramienta SIEM, el cual consiste en representar actividades de amenazas modernas basadas en patrones de acción, indicadores conocidos y fases metódicas de intrusión, es decir, formar una herramienta capaz de normalizar los datos del sensor de seguridad de acuerdo con la investigación moderna de amenazas, y de este modo brindarle a los analistas de seguridad, más claridad sobre los ataques modernos y actualizados que se desarrollan, y de ese modo tener soluciones más eficaces. La herramienta utilizada fue LogRhythm SIEM. (Blake Dougals Bryant, 2016).

En ese mismo año, Ross Brewer, un trabajador de la empresa LoghRhythm, realizó un artículo de seguridad de redes, en el cuál hablan principalmente de un software malicioso llamado ‘Ransomware’ que consiste en un troyano que genera una estafa hacia las empresas. Durante el año 2016, según cifras del FBI, los hackers habían logrado obtener de las cuentas de las

empresas atacadas, $1000 millones de dólares, lo que convertía este ataque en un arma peligrosa para la economía nacional, y en específico para las empresas afectadas. Para prevenir, enfrentar y solucionar los problemas de este ataque, la empresa LoghRhythm a través de su SIEM ofrece detección e indicadores de ataques y gestión contra los mismos. (Brewer, 2016).

En el 2016 e inicios del 2017, se realizó un trabajo de grado, el cual lleva por título "Sistema de autenticidad para aplicaciones de análisis de eventos de seguridad", en el cual se pretende afrontar la creación de un sistema distribuido, capaz de garantizar la autenticidad de los datos transmitidos entre el host cliente y servidor con el fin de asegurar la integridad de los mismos. Para el desarrollo de este proyecto de grado se optó por emplear la herramienta OSSEC SIEM, teniendo en cuenta sus características, que permiten satisfacer en gran medida las propiedades requeridas por el sistema de autenticidad. (Escamilla Pardo, 2017).

En el año 2017, se realizó un artículo de nombre "A novel kill-chain framework for remote security log analysis with SIEM software", el cual consiste en el desarrollo de un marco de seguridad para identificar la relación de las alarmas de seguridad a lo largo de un continuo de comportamientos esperados. El estudio para la realización de este artículo, se basó en investigaciones previas relacionadas con el modelado de amenazas cibernéticas con cadenas de muerte, así como la aplicación práctica de modelos de amenazas para operaciones forenses. En el artículo se realizaron modificaciones en los modelos convencionales de cadena de muerte para facilitar la agregación de datos lógicos dentro de una base de datos relacional que recopila datos a través de sensores remotos dispares, lo que resulta en alarmas más detalladas para los analistas de seguridad. LoghRhythm fue seleccionada como el sistema SIEM preferido para evaluar la inclusión de un modelo de cadena de muerte y poner en marcha el marco de seguridad desarrollado. (Blake D. Bryant & Saiedian, 2017).

También en ese año, Casola, De Benedictis, Rak, & Villano, crearon un artículo sobre la seguridad de los datos resguardados en la nube. Bajo el incremento del uso de los servicios de almacenamiento en la nube, el paradigma de computación en la nube ha ido en aumento, pero de igual modo lo hacen los ataques y amenazas sobre la integridad, disponibilidad y confiabilidad de los datos almacenados, y sobre los cuales los acreedores del servicio en la nube (CSC) no tienen un completo control. Para mitigar la incertidumbre que genera este problema, se crean los acuerdos de nivel de servicio de seguridad (SLA) entre el cliente y el proveedor del servicio,

para regular las condiciones bajo las cuales los servicios objetivo deben entregarse a los clientes, e incluyen términos y garantías relacionados con la seguridad que especifican el nivel de seguridad que los servicios deben garantizar. De acuerdo con dichos acuerdos, los requisitos de seguridad, como los relacionados con la protección contra intrusiones y la correcta evaluación de vulnerabilidad, pueden ser otorgados por un proveedor de servicios en la nube (CSP) y regulados a través de objetivos de nivel de servicio (SLO) dedicados que tienen métricas de seguridad que se utilizarán con fines de monitoreo. Estas métricas pueden estar soportadas por una herramienta SIEM como mecanismo de seguridad y monitoreo. En este artículo la herramienta utilizada fue OSSEC SIEM. (Casola et al., 2017).

Por otro lado, múltiples empresas, organizaciones y universidades han hecho estudios e implantado métodos y estrategias para el aprendizaje y concientización de las políticas de seguridad en un lugar específico. Como es el caso de la Universidad Politécnica de Valencia (España), quien en el año 2014 realizó una investigación y estudio sobre el aprendizaje de políticas de seguridad para los profesionales en seguridad, por medio de una formación on-line y en el que, de igual forma, utilizan el aprendizaje basado en el trabajo o la práctica como medio útil y rápido para la concientización y adquisición de conocimientos de las políticas de seguridad. Como resultado se pudo apreciar que el personal que fue sometido al proceso de nombre RISKY, logró desarrollar competencias con respecto al manejo de las políticas de seguridad. (Morán, García, Martínez, Baraza, & Gil, 2014).

Del mismo modo, la utilización de los objetos virtuales para el aprendizaje y adquisición de conocimiento, es utilizado en múltiples áreas. Aunque a nivel internacional no se le ha dado la misma aplicación de la idea central de este proyecto, la cual radica en la divulgación, aprendizaje y concientización de las políticas de seguridad. En el año 2011 se realizó una investigación con el objetivo de evaluar el objeto virtual de aprendizaje “Raciocinio Diagnóstico en Enfermería Aplicado al Prematuro” en una unidad de cuidado intermedio neonatal. Se trata de un estudio descriptivo que se hizo sobre la evaluación de la apariencia y contenido del objeto virtual en los aspectos relacionados a la presentación, organización, usabilidad e impresión general. Cada una de las características que poseía el OVA fue analizado y evaluado por peritos del área de informática y enfermería, debido a que los conocimientos que imparte el OVA son concernientes y sirven como apoyo para la enfermería y sus procesos, por lo que conocimientos erróneos

pueden generar grandes problemas. (Nogueira de Góes, Monti Fonseca, Carvalho Furtado, Moraes Leite, & Silvan Scochi, 2011).

6.1.2. PANORAMA NACIONAL

Dentro de los diferentes trabajos e investigaciones a nivel nacional se pudo encontrar que en el año 2012 se desarrolló un proyecto el cual buscaba la integración y evaluación del piloto de la herramienta ALIENVAULT OSSIM en la plataforma tecnológica de Telefónica Telecom. Dentro de las finalidades de este trabajo se encuentra el hecho de determinar la efectividad en las garantías de seguridad de la herramienta ALIENTVAULT, en el datacenter de Telefónica Telecom, por medio de pruebas y comparaciones de desempeño técnico y económico, con lo que se pretende llegar luego a un análisis de profundidad, y recomendaciones sobre qué es lo más conveniente al momento de ofrecer el servicio de seguridad gestionada a sus clientes (Amaya Guzmán & Quiroga Martínez, 2012).

En el año 2015 se presentó en la Universidad Católica de Colombia un trabajo con relación a las tecnologías tipo SIEM, el cual básicamente busca establecer una guía metodológica para la gestión centralizada de registros de seguridad a través de SIEM , el enfoque desarrollado en este trabajo de investigación da a conocer una ayuda a empresas que no poseen recursos y conocimiento para el análisis centralizado de los registros de seguridad generados, sin duda esta temática se inscribe en la línea de "Software inteligente y convergencia tecnológica", teniendo en cuenta que en dicho estudio se pueden identificar variables que colaboran en la toma de acciones y decisiones preventivas y correctivas de ámbito técnico, tecnológico y seguridad de la información, que buscan reducir las vulnerabilidades de las tecnologías de la información de las compañías. (Avella Coronado, Calderón Barrios, & Mateus Díaz, 2015).

En ese mismo año en la Universidad Nacional Abierta y A Distancia de Colombia se llevó a cabo un proyecto el cual básicamente planteaba el hecho de buscar una metodología de gestión de incidentes de seguridad de la información y gestión de riesgos para la plataforma SIEM de una entidad financiera basada en la norma ISO/IEC 27035 E ISO/IEC 27005, dentro de las conclusiones obtenidas luego de realizar este trabajo investigativo se destaca el hecho de lograr construir un modelo integro que abarca la gestión de incidentes y gestión de riesgos asociada a estos incidentes, el cual permitió inicialmente la identificación y análisis de los componentes que

hacen parte del contexto bajo el cual se implementaron las normas. Otro de los puntos a resaltar con relación a la implementación de las herramientas SIEM en este proyecto son los beneficios de implantar un modelo basado en un estándar, pues podemos encontrar mejor estructuración de un proceso, control sobre cada una de las actividades definidas dentro del proceso, la eficiencia de los resultados, responsabilidades claramente definidas y validación misma del proceso para identificar mejoras en el mismo. Lo anterior deja entrever que los criterios para la evaluación de los incidentes, como aquellos necesarios para la valoración de los riesgos heredados de los incidentes, están alineados con el SIEM (Tibaquira Cortes, 2015).

También en el 2015 fue llevado a cabo en la Universidad Abierta y a Distancia con sede en Bogotá, un trabajo de especialización en seguridad informática en el que se realiza un estudio sobre el análisis y la gestión del riesgo de la información en una entidad del gobierno, en el cual se estableció que las entidades del gobierno, para protegerse de ataques, intrusos y daños, utilizan herramientas SIEM cómo método efectivo en la reducción de ataques y daños informático al sistema, las redes y la infraestructura sobre la que se soportan los servicios (Garavito Robles, 2015). Lo que proporciona unas bases que impulsan a la confianza sobre las herramientas SIEM. Debido a que, si los sistemas del gobierno que contienen tanta información y peticiones hacia las mismas, están soportados por dichas herramientas, deja visto la potencia y efectividad que éstas tienen para con el monitoreo de las redes y de sistemas grandes y en general para todos.

En cuanto a la utilización de los objetos virtuales de aprendizaje (OVA), a nivel nacional se han desarrollado múltiples escritos para la implementación de los mismos en la adquisición de conocimiento competentes con distintas áreas del conocimiento. En el año 2010 se realizó para la universidad de Córdoba, Colombia, un proyecto de desarrollo para la creación de un OVA que permita comprender de una mejor forma la utilización de diferentes algoritmos de búsquedas en metaheurística. Éste OVA deberá permitir que el usuario cree un problema sencillo para cada metaheurística que desee ver y posteriormente vea paso a paso, como se soluciona un problema o que perciba como se llega a una solución por medio de la metaheurística elegida, permitiendo que obtenga conocimientos básicos del tema. Esta herramienta resultó ser de gran utilidad, conclusión que se toma luego de haber sido realizada una pos-evaluación sobre los usuarios que utilizaron el OVA. (Vega & Chica, 2010).

En el año 2013 se realizó un artículo de investigación para explicar de forma descriptiva, la importancia en la utilización de un OVA para obtener conocimiento básico sobre redes inalámbricas. Cómo método de evaluación de la herramienta OVA, se utilizó un cuestionario otorgado antes y después de los estudiantes hayan utilizado dicha herramienta, arrojando como resultado que este método de aprendizaje ayuda e impacta de manera positiva en la adquisición de conocimientos. (Mario, Plata, Georgina, & Zermeño, 2013).

En el año 2016, se realizó un estudio de investigación científica para el diseño y desarrollo de un Objeto Virtual de Aprendizaje para un Curso de Electrónica de la Universidad Cooperativa de Colombia, donde el objetivo principal radica en lograr una herramienta computacional para facilitar la comprensión de los temas y permitir el acompañamiento durante el tiempo de trabajo independiente de los estudiantes del curso de Electrónica Básica del programa de Ingeniería de Sistemas, por medio de implantación de componentes pedagógicos. (Silva Quinceno & Sosa Chica, 2016).

6.1.3. PANORAMA LOCAL

Actualmente, no se encuentra literatura sobre investigaciones y trabajos realizados por universidades, empresas u organizaciones a nivel de Cartagena con respecto a la utilización de herramientas SIEM. Lo cual indica que éste escrito podría ser el primero dentro del ámbito local. Quizás esto se deba a lo relativamente nueva que es la implementación de las herramientas SIEM para el control y monitoreo de eventos de registros de seguridad en redes informáticas y sistemas de información. Lo verdaderamente importante, es el hecho de abrir paso a la temática en la ciudad.

Por el contrario, con respecto a la utilización e implementación de estrategias para la divulgación de políticas de seguridad, en la Universidad de Cartagena en el año 2012 se desarrolló un proyecto de grado en el cual se creó un software de apoyo para el proceso de creación, redacción, clasificación y registro de políticas de seguridad informática en organizaciones basado en el estudio de diferentes normas y estándares existentes para el establecimiento de Políticas de Seguridad Informática. Este software brindaría la oportunidad de tener, en una plataforma, todas las políticas de seguridad que se desarrollan en la empresa u organización. De este modo,

cualquier empleado que lo amerite, tiene acceso a dicha plataforma. Esto ayuda como soporte masivo, a la divulgación de las políticas de seguridad, aunque no en la magnitud deseable (Marrugo Marrugo, Nuñez Barcos, & Martelo Gómez, 2012).

Por otro lado en lo que concierne al desarrollo de un OVA, se puede decir que en la universidad de Cartagena se han llevado a cabo diferentes trabajos en materia de objetos virtuales de aprendizaje, por ejemplo en el año 2013 se realizó un trabajo el cual consistía en el desarrollo de objetos virtuales de aprendizaje para la anatomía de las estructuras de soporte de los órganos dentarios en la facultad de odontología de la universidad de Cartagena, dicho proyecto se desarrolló con el fin de hacer más ameno el proceso de aprendizaje, utilizando la realidad aumentada en dispositivos móviles para tal fin. (Pomares Agamez, Betín Díaz, Puello Marrugo, & Insignares Órdoñez, 2013).

Posterior a ello se elaboró un trabajo de grado que guarda cierta relación con el referido anteriormente, el proyecto de grado consistía en el desarrollo de una plataforma para la gestión de objetos virtuales de aprendizaje para la facultad de odontología en la universidad de Cartagena, la idea era proporcionar a los estudiantes del programa de odontología una plataforma web donde pudieran estudiar por medio de la manipulación de objetos virtuales las temáticas planteadas a lo largo del programa, convirtiendo esto en una ventaja para los estudiantes a la hora de adquirir nuevos conocimientos. (Lorduy Salas, Peña Esquivel, & Puello Marrugo, 2014).

En ese mismo año se realizó un estudio el cual consistía en la construcción de un objeto virtual de aprendizaje para la capacitación en análisis forense de teléfonos móviles, una de las cosas que se buscaba a través de este trabajo era apoyar directamente el proceso de enseñanza de la asignatura de computación forense en la línea de seguridad informática, y convertir de esta forma la herramienta en un instrumento para el desarrollo profesional del estudiante de ingeniería de sistemas de la universidad de Cartagena. (Nobles Perez & Ruiz Garcia, 2014).

En el año 2016 se realizó un proyecto de investigación que tenía como principal objetivo desarrollar objetos virtuales de aprendizaje como apoyo al estudio de la endodoncia en la facultad de odontología de la universidad de Cartagena , utilizando la digitalización de modelos de piezas dentales en 3d y realidad aumentada en dispositivos móviles, el proyecto surgió con el fin de recrear la anatomía de los órganos dentales para apoyar el estudio de la morfología y fisiología de la pulpa dental en el tratamiento del conducto radicular (Endodoncia), apoyándose

para esto en tecnologías de primera mano. (Barrios Valencia, Ferrer Garcia, Tovar Garrido, & Pupo Marrugo, 2016).

6.1.4. ANÁLISIS DEL ESTADO DEL ARTE

En el panorama internacional se evidenció que cada una de las implementaciones que se les ha otorgado a las herramientas SIEM, han estado orientadas a la utilización y aprovechamiento de todas las características y funcionalidades que ésta brinda. Su manejo es tan flexible que permite la integración con múltiples plataformas y temáticas, lo que indica que estamos bajo un tipo de herramienta ostentosa y poderosa para el control y monitoreo de riesgos dentro de las redes y la infraestructura informática.

Esta temática en Colombia aún presenta falencias en cuanto a su uso, pese a los grandes beneficios que ofrecen las herramientas SIEM en el área de las redes y sistemas de información, su uso no se ha masificado y no todos los que han trabajado e implementado estas herramientas lo han divulgado o han realizado escritos formales en los que exista constancia de tal trabajo. Por este motivo, la industria está inmersa en un bajo desarrollo de la implementación de las SIEM en las empresas y centros de educación en todo el territorio nacional, quizás esto se deba a la poca innovación que tiene Colombia con respecto al área de las TIC y en el manejo de sistemas de información (Perdomo, 2009). Con este trabajo los autores se permiten incursionar y apoyar a los pocos grupos investigativos que anteriormente realizaron trabajos sobre las herramientas SIEM, y dan un paso e invitan a la incursión por parte del personal que está por fuera del área de la temática, a la realización de proyectos e investigaciones sobre las SIEM.

La idea central de este proyecto con respecto a la implantación de la herramienta SIEM, que la diferencia de las demás realizadas, radica en obtener de dicha herramienta los niveles óptimos para el control y monitoreo de redes, y la habilidad para autoadaptarse a los nuevos ataques que se creen en el exterior. Esto permite contar con una herramienta robusta, ostentosa y autoadaptable que proporcionará una capa más de seguridad a la infraestructura de red y al sistema de información de BIOFILM S.A.

En cuanto a la creación de una estrategia para la divulgación de las políticas de seguridad, sólo se encontró un escrito, el cual está alejado de las intenciones principales de este proyecto, en

relación con la divulgación, aprendizaje y evaluación de las políticas de seguridad de BIOFILM S.A. por medio de un aplicativo móvil, lo que indica que este trabajo sería el primero formalmente definido en el que se implemente dichas características como metodología de aprendizaje de las políticas de SdI de la empresa.

Por otro lado, las utilizaciones que se le han otorgado a la herramienta OVA, están involucradas con la adquisición de conocimientos de múltiples áreas del conocimiento, pero dentro de las publicaciones no se destaca un escrito que tenga relación con la divulgación, conocimiento, concientización y evaluación de políticas de seguridad.

De igual modo, la unión de estas tres ideas en dos controles para el fortalecimiento de la seguridad de la información, es decir, la implantación de una herramienta SIEM, la creación de un aplicativo móvil, y la creación de un OVA, dan forma al primer trabajo debidamente publicado que utilice estas herramientas como controles para tal fin.

6.2. MARCO TEORICO

6.2.1. NORMA ISO 27000

La ISO 27000 es una serie bien establecida de normas de seguridad de la información. El alcance de la aplicación de estas normas puede ser una organización en su conjunto, procesos de negocio individuales o incluso una aplicación de TI o infraestructura de TI. El establecimiento del contexto y la identificación de los activos se encuentran entre los primeros pasos a realizar. La calidad de los resultados producidos al realizar estos pasos tiene una influencia crucial en los siguientes pasos, como la identificación de pérdidas, vulnerabilidades, posibles ataques y la definición de contramedidas (Ladino A., Villa S., & María, 2011).

Las empresas y organizaciones con el pasar del tiempo obtienen exigencia por parte del mercado, que la impulsan a crear planes y metodologías para solventar dichas exigencias y problemáticas. Para ello, deben generar un plan de acción frente a éstas. Este plan de acción es conocido como Sistema de Gestión de Seguridad de la Información (SGSI) (Ladino A. et al., 2011).

6.2.2. SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

En un SGSI (Sistema de Gestión de Seguridad de la Información) la implementación de políticas y controles no garantizan una total protección de la información y de los sistemas que la procesan. Posterior a su despliegue se encuentra un riesgo residual, el cual se puede materializar por la existencia de alguna vulnerabilidad por pequeña que sea y donde los controles implementados son inefectivos. Para estos tipos de casos, es necesario implementar un sistema de administración de aquellos incidentes de seguridad que puedan hacer realidad este riesgo residual (Tibaquira Cortes, 2015).

La gestión se encuentra organizada en 5 fases (Tibaquira Cortes, 2015):

1. Planear y Preparar: En esta fase de planea y se define la política de gestión de incidentes de seguridad, alineada a la política de seguridad de la información y de análisis de riesgos, además de concientizar a la gerencia. Se debe definir un equipo de respuesta a incidentes de seguridad de la información.
2. Detección y Reporte: Es la detección y el registro o reporte del incidente, donde se realiza la recolección asociada al incidente. Es la primera fase del proceso operacional de la gestión.
3. Evaluación y Decisión: Es la evaluación de la información recolectada y un análisis para validar si el evento reportado es un incidente de seguridad.
4. Respuesta: Respuesta al incidente de seguridad, con el análisis forense si fue necesario realizarlo, dependiendo de la decisión tomada en la fase de Evaluación y Decisión, y la respectiva entrega del reporte a las personas involucradas.
5. Lecciones Aprendidas: Se identifican las lecciones aprendidas del incidente de seguridad y la mejora del proceso o del SGSI. De ser necesario validar el proceso de gestión de incidentes para implementar mejoras, debido a la lección aprendida del resultado del incidente de seguridad.

6.2.3. SEGURIDAD DE LA INFORMACIÓN

El ministerio de las TIC en Colombia, define la seguridad de la información como un conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones

resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma (Mintic, 2016).

En la actualidad se considera que las empresas dependen cada día más de los sistemas de información, junto con la información guardada en ellos. Por tanto, la seguridad sobre los sistemas de información se ha vuelto importante para preservar la información contenida en los mismos.

Normalmente, La seguridad ha pasado de utilizarse para preservar los datos clasificados del gobierno en cuestiones militares o diplomáticas, a tener una aplicación de dimensiones inimaginables y crecientes que incluye transacciones financieras, acuerdos contractuales, información personal, archivos médicos, comercio y negocios por internet, domótica, inteligencia ambiental y computación ubicua. Por ello se hace imprescindible que las necesidades de seguridad potenciales sean tenidas en cuenta y se determinen para todo tipo de aplicaciones (Pico Barrera, 2016).

La información es el instrumento fundamental para el funcionamiento de las empresas y la operación de los negocios, esto hace que la información deba protegerse como el activo más importante de la organización (Ladino A. et al., 2011).

6.2.3.1. AMENAZAS A LA SEGURIDAD DE LA INFORMACIÓN

Para Balarezo Chávez & Poveda Pilatasig, 2015, Las amenazas se clasifican en cuatro grandes grupos dependiendo del nivel y propósito de afectación, tal cual lo muestra la siguiente tabla:

PROPÓSITO	DESCRIPCIÓN
INTERRUPCIÓN	Produce que un objeto se pierda y que sea inutilizable.
INTERCEPCIÓN	Interceptar información la cual está siendo transmitida.
MODIFICACIÓN	Acceso no autorizado el cual permite modificar un objeto del sistema.
FABRICACIÓN	Objeto que sea difícil de distinguir entre el original.

Tabla 1. Amenazas según el tipo de afectación. (Tomada de Balarezo Chávez & Poveda Pilatasig, 2015*).*

6.2.3.1.1. Elementos considerados amenazas.

Dentro de la seguridad de la red, existen varios factores que son denominados como amenazas, esto debido a la incidencia que tienen hacia el error y el uso no adecuado de los dispositivos asociados a la red. Para Balarezo Chávez & Poveda Pilatasig, 2015, los siguientes elementos son considerados amenazas:

- Personas.

La mayoría de ataques son producidos por personas que voluntaria o involuntariamente causan grandes pérdidas y producen grandes fallos en el sistema.

- Amenazas lógicas.

Se considera a todo software que pueda hacer daño al sistema. Los conocidos como Malware.

- Software incorrecto.

Las amenazas más frecuentes y conocidas son las generadas por fallas involuntarias de los programadores al desarrollar el sistema.

6.2.4. NAGIOS

NAGIOS es un sistema de monitorización de equipos y de servicios de red, creado para ayudar a los administradores a tener siempre el control de qué está pasando en la red y conocer los problemas que ocurren antes de que los usuarios de la misma los perciban. (Zuleta Londoño, 2013).

La herramienta NAGIOS monitorea la red para problemas causados por enlaces de datos sobrecargados o conexiones de red, así como routers de monitoreo, conmutadores y más. Fácilmente capaz de monitorear la disponibilidad, el tiempo de actividad y el tiempo de respuesta de cada nodo en la red, Nagios puede entregar los resultados en una variedad de representaciones visuales e informes. (Nagios Enterprises, 2017).

Para Zuleta Londoño, 2013, NAGIOS cuenta con las siguientes características:

- Monitorear servicios de red (SMTP, POP3, HTTP, PING, etc.)

- Monitorear recursos de los hosts (carga de procesador, uso de disco, etc.)
- Diseño simple de plugins para que podamos crear los nuestros a nuestras necesidades específicas.
- Notificaciones a contactos cuando un servicio o host tenga problemas y puedan resolverlo (email, definido por el usuario).
- Interfaz Web para observar la funcionalidad de los equipos monitoreados.
- Entre otros servicios que presta esta herramienta de monitoreo.

Mientras que para Pereira Diéguez, 2015, una característica muy importante de Nagios es el sistema de dependencia. Este se basa en los niveles de dependencia entre los equipos de la red, es decir, qué equipo está conectado a qué otro u otros. Esto permite posteriormente reflejar la topología real de la red. Y de tal forma, NAGIOS no realizará una petición a un dispositivo dependiente de otro que se encuentre apagado, debido a que no podrá ser fructífera si no existe otro camino. Como lo indica la *figura 1*.

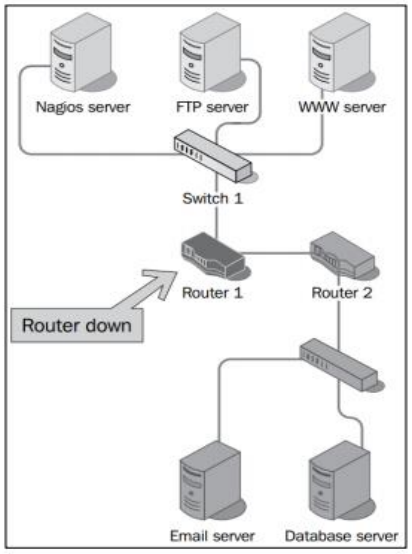


Figura 1. Dependencia entre equipos. (Tomado de Pereira Diéguez, 2015).

6.2.5. SIEM

El término SIEM (Security Information and Event Management o Información de Seguridad y Gestión de Eventos) es utilizado para señalar a las herramientas relacionadas con la información de seguridad y administración de eventos dentro de un contexto informático a nivel de networking. Una herramienta SIEM es el resultado de la combinación de dos herramientas

antecesoras: Security Information Management (SIM o gestión de la información de seguridad) y Security Event Management (SEM o gestión de eventos de seguridad). Estos tres términos deben ser distinguidos uno del otro, puesto no hacen referencia a las mismas funciones (Tibaquira Cortes, 2015).

Básicamente consiste en brindar la oportunidad de monitorear en tiempo real, todos los sistemas, componentes de redes, bases de datos y aplicaciones a las cuales esté asociada dicha herramienta. De igual modo, ofrece toda la información pertinente con la gestión de las amenazas y las vulnerabilidades encontradas en cada monitoreo, para que de ese modo se puedan realizar las correcciones y los planes de contingencia pertinentes (Pico Barrera, 2016).

Para Suarez-Tangil et al., 2015, las herramientas SIEM están diseñadas principalmente para centralizar toda la información de seguridad generada por fuentes de datos distribuidos (denominados sensores) situados junto a una red informática, los sistemas SIEM se centran en normalizar los datos sensoriales en un formato común, proporcionar un acceso rápido a los eventos reportados, realizar un análisis eficiente de los eventos dispersos, y también generar alarmas de correlación.

A nivel global, las industrias han implementado múltiples mecanismos y herramientas para controlar el flujo de información que entra y sale de sus sistemas de información e infraestructura, aunque solamente se basaban en herramientas de tipo SEM (Security Event Management) que monitoreaban y analizaban los eventos de seguridad. Pero esto no era suficiente para el control y prevención de riesgos dentro de la red, es por eso que se utilizaban las herramientas SIM (Security Information Management), que junto con SEM proporcionaban un marco de seguridad más amplio. Para hacer más ágil el proceso, se integraron estas dos herramientas para permitir una mayor robustez y rigurosidad en el tratado de amenazas, soportándose en correlaciones (Tibaquira Cortes, 2015).

6.2.5.1. CARACTERISTICAS DE LOS SISTEMAS SIEM

Para Pico Barrera, 2016, la forma cómo evoluciona la industria y sus necesidades, impulsan a que las herramientas que soportan los sistemas de las empresas estén a las alturas de las exigencias. En la actualidad los sistemas SIEM han evolucionado de manera rápida, adaptándose

a las exigencias que plantea el mercado, básicamente en identificación de eventos reales y en aspectos de interfaz, logrando observar que la mayor cantidad de estos tipos de sistemas SIEM, muestran interfaces gráficas o interfaces web en donde consolidan todos sus servicios, así como sus principales herramientas. Entre las características más comunes y básicas que cita el autor anterior, están:

- Control de direccionamiento IP
- Acceso centralizado y administración de logs.
- Cumplimiento normativo de TI.
- Correlación de eventos.
- Respuesta activa del servidor (seguridad y monitoreo local)
- Seguridad de endpoint y escaneo de equipos.
- Entre otros.

6.2.5.2. CORRELACIÓN DE EVENTOS

La correlación de eventos, trata de establecer la relación o dependencia que existe entre múltiples variables o eventos anómalos dentro de una red, permitiendo agruparlos en una amenaza en concreto para luego tomar las medidas correspondientes. Las SIEM como sistemas de correlación de eventos, son capaces de generar respuestas y soluciones ante eventos anómalos. (Delgado Mendieta & Suárez Asencio, 2015).

6.2.6. GESTIÓN DE LA INFORMACIÓN DE SEGURIDAD (SIM)

Dentro del ámbito de la TI, los SIM hacen referencia al almacenamiento de los datos productos del monitoreo de las redes y los sistemas de información, (logs, eventos, vulnerabilidades). De igual modo, se encargan del análisis y reportes de los datos registrados (Iturralde & Moreano Jurado, 2015).

Para Matteis & Ardenghi, 2011, los sistemas SIM se caracterizan principalmente por permitir mayor análisis histórico de los datos y eventos almacenados en los mismos. Así como también incluyen la posibilidad de generar diversos tipos de reportes. Estos sistemas posibilitan también

el aplicar técnicas de correlación sobre los datos y eventos, pero no en tiempo real. Se cuenta en ellos con un repositorio para los sucesos (logs) y, por lo general, algún mecanismo flexible de consulta que permite obtener reportes diversos.

6.2.7. GESTIÓN DE EVENTOS DE SEGURIDAD (SEM)

A diferencia de los SIM, SEM utiliza el monitoreo en tiempo real para correlacionar diversos eventos, lo que posibilita la generación de notificaciones y la obtención de reportes de manera precisa y oportuna (Matteis & Ardenghi, 2011).

Para Nicolett & Kavanagh, 2011, SEM procesa los datos de registro y eventos de dispositivos de seguridad, dispositivos de red, sistemas y aplicaciones en tiempo real para proporcionar monitoreo de seguridad, correlación de eventos y respuestas a incidentes. SEM soporta las actividades de supervisión de amenazas externas e internas de la organización de seguridad de TI y mejora las capacidades de administración de incidentes.

6.2.8. COMPARATIVO ENTRE NAGIOS Y SIEM

Mediante el estudio de los dos tipos de herramientas que se manejan en esta investigación, se destacan características con las cuales se puede hacer una comparación:

VARIABLES	SIEM	NAGIOS
SOFTWARE	X	X
HARDWARE	X	
MONITOREO DE LA DISPONIBILIDAD Y DESEMPEÑO DE REDES.	X	X
MONITOREO DEL TRÁFICO DE REDES.	X	X
GESTIÓN DE ENRUTADORES.	X	

MONITOREO DE SERVIDORES.	X	X
MONITOREO DE LA INFRAESTRUCTURA TI.	X	X
MONITOREO DE LA INFRAESTRUCTURA DE OTROS DISPOSITIVOS.	X	
ALERTAS	X	X
EVITA ALERTAS FALSAS.	X	
REPRESENTACIÓN GRÁFICA A TIEMPO REAL DE REDES.	X	X
GENERA REPORTES INTEGRALES DE REDES.	X	X
ADMINISTRACIÓN DE SERVICIOS.	X	X
MONITOREO DE LA WEB.	X	
CORRELACIÓN DE EVENTOS.	X	
IDENTIFICA PATRONES DE ATAQUE.	X	X
EXTIENDE EL PODER DE LA HERRAMIENTA.	X	X

Tabla 2. Comparativo NAGIOS vs SIEM (Tomado y modificado de Amaya Guzmán & Quiroga Martínez, 2012*).*

En un entorno real, la utilización de una herramienta SIEM brinda muchas más posibilidades para generar seguridad en la infraestructura de red, puesto cumple con más características con respecto a las NAGIOS.

6.2.9. OSSEC SIEM

Es una herramienta de uso libre (open source, en inglés) potente, que realiza detección de intrusos basados en host, análisis de logs, validación de integridad de archivos, monitoreo de

políticas, detección de rootkit, alertas y respuesta activa en tiempo real. Permite detectar cambios o amenazas que puedan sugerir el incumplimiento en temas de seguridad de la regulación o normas a las que se encuentra sujeta la organización (Avella Coronado et al., 2015).

Para Balarezo Chávez & Poveda Pilatasig, 2015, OSSEC es un sistema de monitoreo y detección de intrusos, que gestiona la información generada de los eventos para la obtención y verificación de la información.

OSSEC Funciona como host basado en el sistema de detección de intrusos (host-based intrusion detection system - IDS) que permite controlar procesos locales, integridad de ficheros, detectar Troyanos y Rootkits. Ossec funciona a nivel local y requiere instalar un agente local en las maquinas que se están analizando (Amaya Guzmán & Quiroga Martínez, 2012).

6.2.9.1. CARACTERÍSTICAS DE OSSEC

Dentro de las características más relevantes, se encuentran las que proponen Balarezo Chávez & Poveda Pilatasig, 2015.

- Comprobación de la integridad de los sistemas.
- Verificación y supervisión de los registros de los sistemas operativos Windows.
- Envío de la información obtenido de los sucesos en tiempo real para una respuesta activa.

Mientras que para Avella Coronado, Calderón Barrios, & Mateus Díaz, 2015, OSSEC posee las siguientes características:

- Verificación integridad de archivos.
- Monitoreo de logs en tiempo real.
- Respuesta activa a incidentes.

6.2.10. LOGRHYTHM SIEM

Es una herramienta de detección de amenazas a nivel de redes dentro del entorno empresarial. Utiliza para dicha tarea, la gestión de logs, análisis forense de redes y puertos finales, y analítica de seguridad avanzada. Además de proteger a los usuarios de ataques cibernéticos. Esta

herramienta se ajusta a cualquier tamaño de empresa, adaptándose a cambios que tenga la red ante anexo o eliminación de dispositivos, según sean las necesidades de dicha empresa. (LOGRHYTHM, 2016)

Logrhythm maneja una jerarquía para el análisis de amenazas que permitirá al analista de redes, tener una visión más acertada de la actualidad de la red al momento de detectar amenazas. Esta jerarquía está ilustrada a continuación:

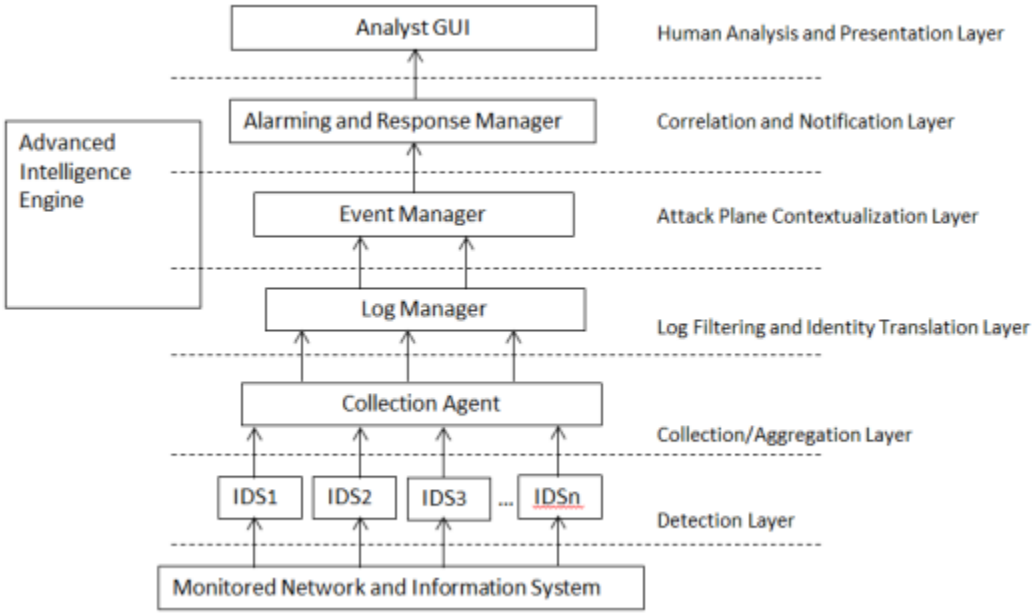


Figura 2. Jerarquía de análisis de LogRhythm SIEM. (Tomada de Bryant, 2016*).*

6.2.10.1. CARACTERÍSTICAS DE LOGRHYTHM SIEM

Logrhythm SIEM posee las siguientes características que le permiten al administrador de red, tener más control sobre la red y prevenirla de cualquier eventualidad. (LOGRHYTHM, 2016):

- Análisis forense: permite descubrir e identificar comportamientos sospechosos en la red, analizar y preservar los datos valiosos, y explorar vulnerabilidades en las redes antes de que los piratas informáticos lo hagan.
- Monitoreo en tiempo real: verifica, administra y explota las amenazas al momento cuando ocurren. Mantiene informado al analista de red de todos los acontecimientos ocurridos en la red.

- Resultados y análisis eficaces: emplea análisis contextuales o desestructurados para detectar amenazas y analizar eventos en las redes. Las herramientas de análisis de LogRhythm otorga criterios y respuestas precisas para atender y explotar las vulnerabilidades de sus redes.
- Ahorro de tiempo y perfilación de búsquedas: posee algoritmos de prioridad que permiten la identificación automática de amenazas reales, riesgos y vulnerabilidades, lo que libera a los equipos de efectuar análisis complicados que pueden prolongarse por demasiado tiempo.

6.2.11. OSSIM SIEM

La sigla OSSIM se deriva para Open Source Security Information Management (Herramienta de Código Abierto para la Gestión de Seguridad de la información), OSSIM no es una herramienta única, al decir OSSIM se entiende que es un conjunto de herramientas unidas en un solo programa que facilita el análisis, visualización y la gestión de manera centralizada de los eventos que ocurren en los diferentes componentes de la infraestructura IT de la empresa, obteniendo de esta forma mayor efectividad a la hora del monitoreo y de encontrar errores u vulnerabilidades en la seguridad de la red (Villafuerte Quiroz & Bravo Bravo, 2015a).

En la actualidad, OSSIM se identifica por ser una herramienta que ayuda a solventar y responder a los ataques que puedan pasar desapercibidos por los IDS convencionales, permitiendo administrar los diferentes logs que obtiene la red de una manera sencilla para así lograr importantes informes (Balarezo Chávez & Poveda Pilatasig, 2015).

OSSIM posee una estructura peculiar con la cual logra centralizar todo el control sobre los dispositivos conectados a la red y en general sobre ella misma. La siguiente imagen representa lo dicho:

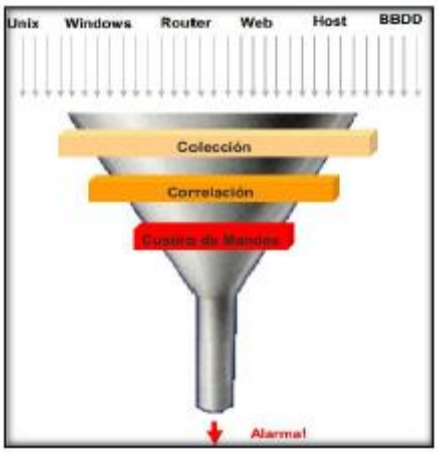


Figura 3. Estructura de OSSIM. (Tomada de Balarezo & Poveda, 2010).

6.2.11.1. CARACTERÍSTICAS DE OSSIM

OSSIM trae un conjunto de características que permite al administrador de red gestionar de forma más eficiente la seguridad interna de los servidores, de la red de datos y voz. Para Villafuerte Quiroz & Bravo Bravo, 2015, se pueden mencionar las siguientes:

1. Gratuita.
2. Monitoreo centralizado.
3. Analiza el comportamiento de nuestra Red.
4. Presenta informes técnicos.
5. Realiza un análisis de los posibles riesgos y anomalías en la red.
6. Controla los posibles ataques/intruso en la red.
7. Monitorea el excesivo tráfico que se pueda generar.
8. Presenta una interfaz gráfica web amigable hacia al Administrador.
9. Permite recolectar logs de los servidores sin importar que distribución de Linux tenga instalado.
10. El cliente recolector de logs que se instala en Windows es muy sencillo de configurar.
11. Realiza test de vulnerabilidad.
12. Realiza notificaciones automáticas mediante alertas.
13. Cuenta con gran cantidad de plugin gratuitos.
14. Las notificaciones que se envían pueden ser:

- Falso supuesto.
- Alerta de duplicidad de mac.
- Clave incorrecta.
- Alerta de intruso.
- Posible ataque.
- Trafico excesivo.

6.2.12. GRAYLOG SIEM

Graylog es un SIEM de código abierto totalmente integrado para la recolección, indexación y el análisis de datos estructurados y no estructurados de cualquier fuente. Proporciona un sistema unificado y centralizado de mensajes procedentes de diferentes fuentes: sistema operativo, servidores de aplicación, sistemas de información, etc. Dispone de un sistema de alertas y de búsqueda de histórico de logs. Es ideal para escenarios complejos (Avella Coronado et al., 2015).

6.2.12.1. CARACTERÍSTICAS DE GRAYLOG

Para Avella Coronado, Calderón Barrios, & Mateus Díaz, 2015, Graylog cuenta con las siguientes características:

- No requiere una inversión económica en software, debido a que es de uso libre.
- Plataforma que permite mejorar tiempos de respuesta para gestionar los registros de datos.
- Plataforma centralizada para la gestión de logs.
- La arquitectura permite mejoras de procesamiento y almacenamiento de la herramienta, cambiando o incrementando los recursos de la misma.
- Formato de mensaje de registro optimizado (GELF, en inglés) mejora la eficiencia de procesamiento de los mensajes.
- La arquitectura de la herramienta, permite el procesamiento en tiempo real de logs antes de su almacenamiento.

- Utiliza API REST, son sistemas para que desarrolladores puedan integrar otro software de gestión.

Estas características le permiten a la herramienta Graylog, contribuir al fortalecimiento de la seguridad de la información de la empresa en la cual se implemente.

6.2.13. COMPARATIVO ENTRE HERRAMIENTAS SIEM

De acuerdo a la comparación realizada por Avella Coronado et al., 2015, se contrastaron las distintas herramientas SIEM, teniendo en cuenta las características y funcionalidades enfocadas a la gestión de logs que cada una ofrece. A continuación, se muestra la tabla con el comparativo realizado.

		HERRAMIENTAS			
		OSSEC	**OSSIM**	**GRAYLOG**	**LOGRHYTHM**
CARACTERISTICAS	Descubrimiento de activos		X		
	Gestión centralizada	X	X	X	X
	Recolección de Logs y eventos de seguridad	X	X	X	X
	Correlación de Eventos	X	X		X
	Análisis de Logs	X	X	X	X
	Clasificación y Prioridad de eventos	X	X		X

	Monitoreo en tiempo Real	X	X	X	X
	Normalización	X	X	X	X
	Reportes	X	X	X	X
	Interfaz Gráfica de administración	X	X	X	X
	Modo de recolección de eventos	**Agente/ Sin Agente**	**Agente/ Sin Agente**	**Agente/Sin Agente**	**Agente/Sin Agente**
S.O SOPORTADO	LINUX/UNIX	X	X	X	X
	MAC	X	X		
	BSD	X	X		
	WINDOWS	X	X		X

Tabla 3. Comparativos entre herramientas SIEM. (Tomada y modificada de Avella Coronado et al., 2015).

6.2.14. APLICACIÓN MÓVIL

En los últimos años los computadores de escritorio han perdido espacio en el mercado informático, debido exclusivamente al aspecto de movilidad y transporte, características que aparecieron en otros equipos informáticos, tales como laptops, netbooks, tablets o smartphones. Estas categorías de equipos son más apreciadas debido a la facilidad de transportarlos ya sea dentro de las organizaciones o dentro de los hogares, pero la mayor utilidad de los equipos es la de conectarse a redes de computadoras de manera inalámbrica, lógicamente con equipos de red apropiados para el tipo de conexión (Pico Barrera, 2016).

Todo ello ha provocado que los dispositivos móviles se hayan convertido en uno de los principales medios de conexión a la red, siendo ya una verdadera alternativa a las formas tradicionales. Desde hace tiempo para cualquier empresa es imprescindible tener presencia en la red, sin embargo, hoy en día esto no es suficiente, porque estas nuevas reglas de juego hacen necesario que los contenidos sean además accesibles a través de cualquier dispositivo móvil. En este sentido, no solo es fundamental disponer de una web adaptada para su visualización en los

teléfonos móviles, sino que al contar con una aplicación personalizada supondrá sin duda un elemento diferenciador.

Las APPs móviles son, hoy en día, unas herramientas de comunicación muy importantes que muchas empresas no pueden obviar en sus estrategias corporativas y acciones que busquen resultados tanto tangibles como intangibles; tanto a corto como a medio y largo plazo.

6.2.15. OBJETO VIRTUAL DE APRÉNDIZAJE (OVA)

Según el Ministerio de Educación Nacional (MEN), un objeto de aprendizaje es un conjunto de recursos digitales, auto contenible y reutilizable, con un propósito educativo y constituido por al menos tres componentes internos: Contenidos, actividades de aprendizaje y elementos de contextualización. El objeto de aprendizaje debe tener una estructura de información externa (metadatos) que facilite su almacenamiento, identificación y recuperación. (Mineducación, 2017).

Algunos de los beneficios relevantes que se pueden obtener la construcción de objetos virtuales de aprendizaje, son: dinamizar los procesos de investigación, desarrollo de competencias, facilitar el aprendizaje a la medida, adaptabilidad dinámica y permanente para la demanda de información y comunicación, ahorro en tiempo para docentes y estudiantes e investigadores, acceso simultáneo, permite la utilidad en más de una secuencia para los procesos formativos en diversas áreas del conocimiento, promueven el trabajo colaborativo y el aprendizaje autónomo, hipertextos y acceso remoto a contenidos actualizados de aprendizaje. (Pascuas, Y., Jaramillo, C. & Verástegui, 2015).

Actualmente estos recursos digitales además de facilitar los ambientes virtuales de aprendizaje se convierten en instrumentos de mediación, posibilitando interacciones entre el individuo y el conocimiento; además, facilitan la comunicación y el procesamiento de la información tecnológica. Por lo tanto, cada vez más existe un interés progresivo en la necesidad de la sociedad actual en relación con el uso de las tecnologías, materia digital, virtual y educación en línea.

Por otro lado, Pascuas, Y., Jaramillo, C. & Verástegui, 2015, mencionan que es importante destacar que la conceptualización, estructuración, circulación y en general el análisis de los OVA se ha hecho fundamental en el exterior, pero los diferentes procesos locales exigen el desarrollo de estos, y Colombia no ha sido la excepción, pues desde hace ya varios años se viene explorando la forma de aprovechar estas herramientas en el proceso educativo ya sea en las escuelas o entornos empresariales. Sumado a lo anterior la implementación de este tipo de recursos digitales permite proyectar y concretar posibilidades claras a futuro dentro del sector industrial, más específicamente para este caso BIOFILM S.A.

6.2.16. SISTEMA DE GESTIÓN DE APRÉNDIZAJE (LMS)

LMS significa "Learning Management System" o lo que es lo mismo Sistema de gestión de aprendizaje. El LMS es una herramienta informática dirigida a la comunidad estudiantil para la gestión y presentación de materiales educativos. El objetivo de estas herramientas es permitir el aprendizaje en cualquier parte y en cualquier momento y la mayoría de estas son herramientas Web. (Pascuas, Y., Jaramillo, C. & Verástegui, 2015).

Por lo anterior, el LMS se trata de un programa que permite organizar materiales y actividades de formación en cursos, hacer seguimiento de su proceso de aprendizaje, evaluarlos, comunicarse con los aprendices mediante foros de discusión, Chat o correo electrónico, etc., es decir, permite hacer todas aquellas funciones necesarias para gestionar cursos de formación a distancia (aunque pueden usarse como complemento en la enseñanza presencial).

Por otra parte, la implementación de plataformas LMS en Colombia impulsa a la industria a buscar nuevas alternativas e integraciones para los sistemas de gestión de aprendizaje, el desarrollo de nuevas tendencias de educación virtual, la adaptación dentro de los procesos educativos clásicos de las plataformas LMS constituyen básicamente la necesidad de ampliar las experiencias y el recurso de formación dentro de los sistemas educativos convencionales (Robledo, Osorio, & López, 2014).

Para Robledo, Osorio, & López, 2014, los nuevos sistemas de gestión de aprendizaje o LMS en Colombia han llevado a proporcionar nuevas experiencias a los usuarios de las plataformas, la implementación de estrategias pedagógicas electrónicas, el fácil uso de las herramientas del

sistema, y el fácil acceso al mismo hacen de los sistemas virtuales de educación una opción perfecta para complementar la experiencia educativa que instituciones y organización empresariales puedan aportar a sus sistemas educativos o de capacitación empresarial interna.

6.2.17. MOBILE-D

Es una metodología exclusiva para el desarrollo móvil, basada en otras metodologías ágiles como Extreme Programming y Crystal. Fue creada por Pekka Abrahamsson y su equipo Technical Research Centre of Finland, quienes son ponentes del desarrollo móvil en Finlandia. Las prácticas asociadas a Mobile-D incluyen desarrollo basado en pruebas, la programación en parejas, integración continua y refactorización, así como las tareas de mejora de procesos de software, y para muchos autores, debe ser utilizada por un equipo de no más de diez desarrolladores, trabajando en conjunto para suministrar un producto listo en un plazo máximo de diez semanas. (Amaya Balaguera, 2013).

Como toda metodología para desarrollo software, Mobile-D propone un ciclo de vida basado en cinco fases:

- Exploración.
- Iniciación.
- Producción.
- Estabilización.
- Prueba del sistema.

Algunos autores agregan una etapa inicial llamada “Levantamiento de información”, en la cual se realiza una investigación sobre documentos existentes que sirvan para el desarrollo del proyecto, como lo señala Ayala Guanina & Segovia Bedón.

Figura 4. Ciclo de desarrollo de Mobile-D. (Tomado de Ayala Guanina & Segovia Bedón, 2016).

Existen múltiples autores que definen este ciclo de desarrollo. Los investigadores de este proyecto citan a dos de ellos.

Ciclo de vida definido por Ayala Guanina & Segovia Bedón, 2016.

- **Exploración:** esta etapa se centra la atención en la planificación y en los conceptos básicos del proyecto. Aquí es donde se hace una definición del alcance del proyecto y su establecimiento con las funcionalidades donde se quiere llegar.
- **Inicialización:** Se configura el proyecto identificando y preparando todos los recursos necesarios, en esta fase se le dedica un día a la planificación y el resto al trabajo y publicación.
- **Producción:** Aquí se repiten interactivamente las etapas. Se usa el desarrollo dirigido por pruebas (TDD), antes de iniciar el desarrollo de una funcionalidad debe existir una prueba que verifique su funcionamiento. En esta fase se lleva a cabo toda la implementación.
- **Estabilización:** Aquí se realizan las acciones de integración para enganchar los posibles módulos separados en una única aplicación.
- **Pruebas:** Cuando se finalice totalmente con el desarrollo, se pasa una fase de testeo hasta llegar a una versión estable según lo establecido en las primeras fases por el cliente. Si es

necesario se reparan los errores, pero no se desarrolla nada nuevo. Una vez acabada todas las fases se debe tener una aplicación estable para entregar.

Amaya Balaguera, 2013, define el ciclo de desarrollo de la siguiente forma:

- **Exploración:** En esta fase, el equipo de desarrollo debe generar un plan y establecer las características del proyecto. Esto se realiza en tres etapas: establecimiento de actores, definición del alcance y el establecimiento de proyectos. Las tareas asociadas a esta fase incluyen el establecimiento del cliente (los clientes que toman parte activa en el proceso de desarrollo), la planificación inicial del proyecto y los requisitos de recogida, y el establecimiento de procesos.
- **Inicialización:** Los desarrolladores preparan e identifican todos los recursos necesarios. Se preparan los planes para las siguientes fases y se establece el entorno técnico como los recursos físicos, tecnológicos y de comunicaciones. Esta fase se divide en cuatro etapas: la puesta en marcha del proyecto, la planificación inicial, el día de prueba y día de salida.
- **Producción:** Se repiten las tareas de planificación, trabajo y liberación, estas se iteran hasta implementar todas las funcionalidades. Primero se planifica la iteración de trabajo en términos de requisitos y tareas a realizar, luego se preparan las pruebas de la iteración de antemano y, por último, las tareas se llevarán a cabo durante el día de trabajo, desarrollando e integrando el código con los repositorios existentes. Durante el último día se lleva a cabo la integración del sistema (si el trabajo estuvo dividido por equipos), seguida de las pruebas de aceptación.
- **Estabilización:** Se llevan a cabo las últimas acciones de integración para asegurar que el sistema completo funciona correctamente. Esta será la fase más importante en los proyectos multiequipos con diferentes subsistemas desarrollados por equipos distintos. En esta fase, los desarrolladores realizarán tareas similares a las que debían desplegar en la fase de “producción”, aunque en este caso todo el esfuerzo se dirige a la integración del sistema. Adicionalmente se puede considerar en esta fase la producción de documentación.
- **Pruebas:** El producto terminado e integrado se prueba con los requisitos de cliente y se eliminan todos los defectos encontrados.

6.2.18. METODOLOGÍA AODDEI

Es una metodología para desarrollar OVA´S e integrarlos a un sistema de gestión de aprendizaje, apoyándose en sus diferentes fases, las cuales permiten que por medio de cada una de estas se vaya estructurando el OVA. Esta metodología tuvo su primera aplicación en un curso intensivo de la unidad de formación de profesores en la universidad autónoma de Aguascalientes, con un desempeño sobresaliente en su aplicación. (Tovar, Bohórquez, & Puello, 2014)

AODDEI como toda metodología para el desarrollo de objetos virtuales, cuenta con diversas fases que permiten a través de cada una de estas, ir ensamblando la estructura general del OVA. A continuación, se presentan las cinco fases en las cuales se divide esta metodología:

1. Análisis y Obtención: En esta fase se identifica una necesidad de aprendizaje (resolver un problema, mejorar, innovar), con base en esto se tiene claro que es los que se va a enseñar, se identifican los datos generales del OVA, y se obtiene el material didáctico necesario para realizarlo.

   Dentro del Análisis y Obtención se encuentran 3 subetapas fundamentales como lo son análisis, obtención y digitalización. Todos estos 3 pasos se vendrían a complementar entre sí para proporcionar un análisis más claro con relación a lo se hará partiendo del objeto virtual de aprendizaje.
2. Diseño: Aquí será importante dejar claro, como se va a enseñar, para esto se realiza un esquema general del OVA, el cual indicara como están interrelacionados el objetivo, contenidos informativos, actividades de aprendizaje y la evaluación.
3. Desarrollo: En esta fase de desarrollo mediante diversas herramientas computacionales, se arma la estructura del esquema general del OVA elaborado en la fase de diseño. Para esta fase se ve en la necesidad de que intervenga en lo posible un técnico de diseño, para proveer al OVA, de una interfaz adecuada que motive a los empleados a aprender.

   Es de resaltar que en el desarrollo aparecen 3 pasos fundamentales, como lo son programación, armado y empaquetado. Todos estos pasos permitirán concretar las ideas prestablecidas sobre el OVA.

4. Evaluación: Aquí es importante aclarar que no se realiza una evaluación del objetivo de aprendizaje del OVA, sino más bien se evalúa al mismo como un todo, tomando como referencia algunos criterios.

   Para esta fase aparecen 2 subetapas como lo son evaluar el OVA y almacenar el OVA en un repositorio de OVA's evaluados. Estos pasos serán fundamentales, debido a que es donde se hace una examinación del objeto virtual de aprendizaje por un grupo de expertos, tomando como referencia una serie de indicadores.
5. Implementación: En esta fase final, el OVA será integrado en un sistema de gestión de aprendizaje, el cual puede ser propio o comercial, esto es con la finalidad de interactuar con el mismo en un determinado contexto, para hacer uso y reuso de este. En esta fase también será la pauta para que el OVA sea evaluado por los empleados, los cuales pueden proveer una retroalimentación valiosa. Con base en esta retroalimentación la persona a cargo del objeto virtual de aprendizaje, podrá detectar si le falto agregar elementos interactivos, o de otro tipo que fomenten el aprendizaje de los empleados.

6.2.19. IONIC

Framework de JavaScript creado por Google bajo el Modelo Vista Controlador (MVC) útil para el desarrollo del front-end de forma dinámica y rápida. El framework permite extender el vocabulario de HTML con atributos y directivas para crear componentes dinámicos. Los dos puntos estructurales de Angular son la inyección de dependencias y el Data Binding. (Carvaca Morán & Ramos Tamayo, 2017)

Ionic integra tecnologías ya conocidas, como: 1) Angular; 2) JavaScript; 3) TypeScript; 4) HTML. Esta combinación permite la creación dinámica de aplicativos móviles. El desarrollo en este framework, permite la creación de aplicativos completamente multiplataformas y posee documentación oficial para el desarrollo íntegro de las mismas aplicaciones.

6.2.19.1. INYECCIÓN DE DEPENDENCIAS

Una aplicación en Angular la conforman un grupo de módulos/componentes diferentes que se integran para construir un aplicativo. La aplicación podría tener un modelo para interactuar con

un objeto específico de una Interface de Programación de Aplicaciones (Aplication Programing Interface, API), también conocido como controlador que manda datos a las vistas, o un módulo que maneja el enrutamiento de la aplicación Angular.

La inyección de dependencias es el método por el cual a un objeto se les da las dependencias que requiere para su funcionamiento es decir un objeto depende de otro. Hay diferentes grados de dependencia, pero el mayor uso de ella hace que testear el código sea complicado o que algunos procesos se ejecuten más tiempo de la cuenta.

6.2.19.2. DATA BINDING

Con Angular se ha eliminado la manipulación del Modelo de Objeto del Documento (Document Object Model, DOM) y al ser modelo MVC los datos se almacenan en un solo lugar. Mediante el Data Binding, la vista (archivos HTML) se actualizará de forma automática cada vez que el modelo cambie y viceversa.

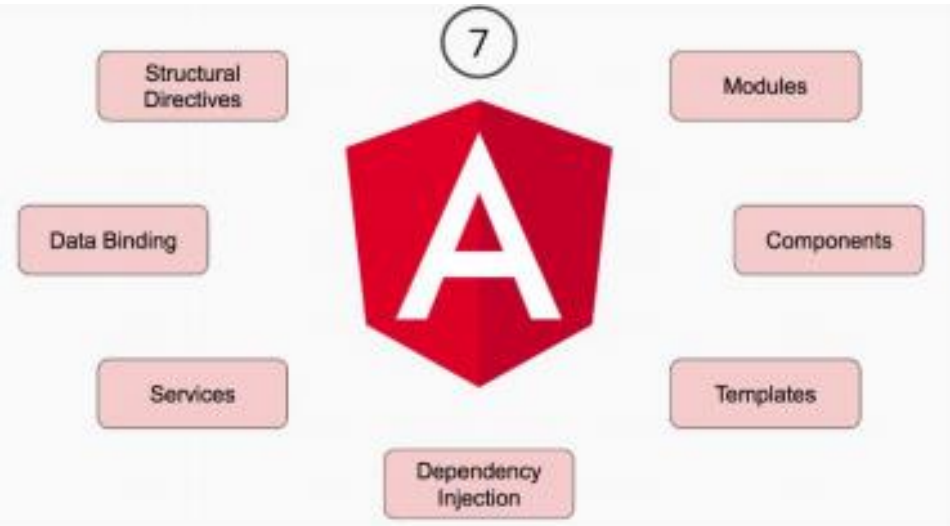


Figura 5. Simplificación del Data Binding. (Tomada de Andrés & Genesis, 2017)

7. OBJETIVOS

7.1. OBJETIVO GENERAL.

Implementar controles en los dominios de Recursos humanos y Telecomunicaciones para la gestión de la seguridad de la información en BIOFILM S.A. mediante el uso de tecnologías de gestión de redes, plataformas de aprendizaje y sistema operativo Android para móviles.

7.2. OBJETIVOS ESPECIFICOS.

1. Identificar las políticas de seguridad de la empresa sobre las cuales estarán soportados los controles a desarrollar.

2. Seleccionar una herramienta SIEM de acuerdo a sus características y las necesidades de BIOFILM S. A., para implantar en la empresa.

3. Implantar una herramienta SIEM en el dominio de Telecomunicaciones para la gestión de la infraestructura de red en la empresa BIOFILM S.A.

4. Crear un aplicativo móvil para el dominio de Recursos Humanos que permita potencializar la divulgación, aprendizaje y concientización de las políticas de seguridad de la empresa.

5. Construir y anexar un OVA al LMS empresarial para la divulgación y evaluación de los conocimientos sobre las políticas de la empresa.

8. ALCANCE

En este proyecto se estipularon dos controles para ayudar en los procesos desarrollados por los dominios de Telecomunicaciones y Recursos Humanos, concernientes con la seguridad de la información (SdI) al interior de BIOFILM S.A. En aras de conseguir lo planteado, se detallaron los ámbitos sobre los cuales se aplicaron los controles desarrollados, así:

1. El desarrollo del trabajo fue estipulado a 1 año, contados a partir de la aprobación del anteproyecto, contemplando dos periodos académicos, dentro de los cuales se realizaron en el primer periodo, las investigaciones pertinentes a la problemática sobre el fortalecimiento de la SdI y en el segundo se materializó lo investigado en dos controles: 1) La implantación de una herramienta SIEM para el monitoreo de la infraestructura de red; 2) Creación de una estrategia para la divulgación, aprendizaje y concientización de las políticas de seguridad que la empresa implementa para sus trabajadores. A su vez, éste último se conformó por la creación de un OVA desplegado en el Servidor de Archivos empresarial, por solicitud de la empresa BIOFILM S.A, como medio de enseñanza/aprendizaje de las políticas de SdI, y la creación de un aplicativo móvil (APP) a modo de juego de preguntas para celulares móviles con plataformas Android, como medio de evaluación de los conocimientos adquiridos mediante la utilización del OVA, con el fin de maximizar el conocimiento de las políticas de SdI, su uso y su importancia.

   En la etapa del anteproyecto, se planteó desplegar el OVA en el LMS empresarial; sin embargo, en la etapa del desarrollo del proyecto, la empresa solicitó cambiar la estrategia de despliegue, y realizarlo en el Servidor de Archivos. Del mismo modo, en esa etapa se había estipulado la realización de un aplicativo móvil informativo, el cual también fue modificado por petición de la empresa, pasando a ser un aplicativo móvil contenedor del componente evaluativo del OVA, en formato de juego de preguntas. Por lo anterior, el OVA contempla dos componentes, el contenido y la taxonomía, es decir, es utilizado solamente para la adquisición de los conocimientos sobre las políticas.

2. Debido a que existen políticas que regulan el uso de los dispositivos móviles dentro de la planta, se desarrollaron dos opciones como estrategia para la divulgación, el aprendizaje y la concientización de las políticas de seguridad que dispone la empresa para sus trabajadores, al igual que la evaluación de los conocimientos adquiridos sobre las

mismas. Estas opciones permiten que, tanto dentro como fuera de la empresa, se pueda obtener conocimientos sobre las políticas de seguridad. La divulgación de las políticas en el Servidor de Archivos empresarial, a través del OVA anexado al mismo, es el modo de adquisición de conocimientos que tiene el trabajador cuando se encuentre dentro de la empresa. Mientras que, si se encuentra por fuera de la misma, cuenta con la opción de poseer un aplicativo móvil en el que se evalúan y se retroalimentan los conocimientos de las políticas de SdI que la empresa coloca a disposición de los empleados.

3. Los controles desarrollados están orientados hacia la planta de producción central de BIOFILM S.A. ubicada en la zona industrial de Cartagena de Indias D.T y C. y sus trabajadores, por lo que una ampliación e implementación de estos controles en la segunda planta de la empresa ubicada en Altamira, México, queda como posibilidad para trabajos futuros. La creación de los controles y su puesta en marcha, está regida por las políticas de seguridad que la planta central tiene para tal fin, es decir, la implantación de la herramienta SIEM, junto con la creación del aplicativo móvil y la creación del OVA, están ligadas a las políticas de seguridad de la empresa.

El desarrollo de los controles para la gestión de la SdI permite que el dominio de Telecomunicaciones tenga una herramienta para monitorear los procesos y actividades realizadas por medio de la red, así como disminuir las posibilidades de encontrar ataques, virus y otros obstáculos que interrumpan el normal funcionamiento de los movimientos que se realicen con la información y los servicios alojados en los servidores. Esto debido a las funcionalidades que la herramienta SIEM posee y coloca a disposición para su uso. De igual manera, con el desarrollo del aplicativo móvil y la creación del OVA, la empresa espera, en un futuro cercano, la disminución en el índice de incidentes de seguridad con respecto al manejo de la información, la privacidad de datos y los procesos operacionales llevados a cabo en el marco de la SdI, para de ese modo lograr una mejor operatividad.

4. Luego de hacer un estudio de las diferentes herramientas SIEM existentes en el mercado, se eligió, junto con BIOFILM S.A., las que mejores condiciones ofrecen de acuerdo a sus funcionalidades y las soluciones que brindan con respecto a los problemas que se presentaban con la herramienta NAGIOS que usaban, y de ese modo se seleccionó la más adecuada, que posteriormente fue implantada en la empresa.

5. La APP fue desarrollada para su uso en el idioma español. Por consiguiente, la aplicación está orientada a los trabajadores de habla hispana y aquellos que tienen conocimientos sobre el mismo. La implementación de la APP para un segundo lenguaje, quedó a disposición de trabajos futuros.

6. La aplicación móvil fue entregada con un manual de usuario, en el cual están estipuladas las utilidades y la forma de uso de la misma. De igual forma, el OVA fue entregado con un documento de preguntas frecuentes que servirá de fundamento para aprender sobre la forma de uso del mismo.

7. La creación del aplicativo móvil tiene como fin único el acompañamiento en la evaluación no remunerada del conocimiento adquirido por parte de los empleados sobre las políticas de seguridad de la empresa. Por tanto, al ser usado con otra finalidad es responsabilidad única de BIOFILM S.A.

9. METODOLOGÍA

9.1. TIPO DE INVESTIGACIÓN

Este proyecto por sus características se clasifica como una **Investigación Aplicada,** debido a que inició de una situación problema dada por los diversos inconvenientes que se presentaban a nivel de la gestión de la infraestructura de red, y a nivel del conocimiento y práctica de las políticas con respecto a la SdI manejadas dentro de BIOFILM S.A. Frente a dicha situación, existió la necesidad de intervenir y potencializar los procesos relacionados con la SdI, llevados a cabo por los dominios de Telecomunicaciones y RRHH dentro de la empresa.

Por otro lado, el desarrollo del proyecto se realizó bajo un enfoque mixto, debido a que dentro del proceso de investigación se recolectaron, analizaron y vincularon datos cuantitativos y cualitativos en un mismo estudio para responder al planteamiento del problema. Del mismo modo, se optaron por incluir metodologías puntuales para el desarrollo del aplicativo móvil y del OVA, lo que permitió la realización del cuarto y quinto objetivo, respectivamente planteados en el proyecto.

9.2. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Teniendo en cuenta objetivos y características del proyecto, la investigación se identificó de acuerdo a diferentes criterios, los cuales estuvieron orientados a la realización de los objetivos previamente establecidos. Con el fin de acercarse a ellos, se realizó lo siguiente: 1) Búsqueda de información pertinente o estudio del estado del arte, apoyándose en materiales bibliográficos debidamente publicados; 2) Implementación de un entorno controlado de pruebas para la búsqueda y obtención de información directamente en los escenarios de trabajo. Lo anterior considerando que el proyecto es de carácter investigativo y experimental.

Dentro del desarrollo y ejecución de este proyecto, se desarrollaron diferentes reuniones y entrevistas en las cuales se aclararon las necesidades que el proyecto debió resolver. También, se hizo necesario contar con la constante comunicación y con el apoyo del personal competente de BIOFILM S.A., así como del uso de sus recursos y de las instalaciones de la misma empresa, a quien van dirigidos los controles desarrollados en este proyecto. Del mismo modo, se utilizó la oficina de la directora del proyecto, ubicada en las instalaciones de la sede Piedra de Bolívar de

la Universidad de Cartagena, para realizar reuniones con el fin de debatir ideas y llevar un seguimiento a las tareas realizadas por los investigadores. Estos dos lugares, fueron principalmente en los que se realizó el proyecto a lo largo del tiempo de desarrollo estipulado en el alcance.

9.3. DISEÑO Y DESARROLLO POR OBJETIVOS

El desarrollo de este proyecto se llevó a cabo por medio de una metodología mixta, a través de la cual se buscó abarcar dos puntos claves, que fueron: 1) La implantación de una herramienta SIEM para el monitoreo de la infraestructura de red; 2) Creación de una estrategia para la divulgación, aprendizaje, concientización y evaluación de las políticas de seguridad. Todo lo anterior se realizó en la medida que se cumplieron en su totalidad los objetivos específicos propuestos. Cada uno de los objetivos desarrollados, necesitaron de documentación, pruebas, investigaciones y/o reuniones para su realización. A continuación, se detalla la forma en que se hizo su desarrollo:

1. **Identificar las políticas de seguridad de la empresa sobre las cuales estarán soportados los controles a desarrollar.**

Las soluciones a implementar o implantar en una empresa, no se pueden realizar de manera arbitraria, sino más bien respetando las políticas que la misma dispone para tal fin. Para esto, mediante una reunión con la jefa de TI de la empresa BIOFILM S.A. *(ver anexo 2),* se establecieron las políticas que debieron cumplir los controles al momento de su desarrollo y su posterior puesta en marcha, para no violar o estar en contra de las normatividades que la empresa maneja. Esto se hizo para garantizar que la solución desarrollada cumpliera con los estatutos y leyes de la empresa.

La determinación de las políticas de seguridad creó un marco legal que reguló la realización del proyecto, dentro del cual los investigadores supieron las normatividades y los pasos que se debían realizar para, en el desarrollo y ejecución de los controles, consumir los recursos necesarios de la empresa en la realización de las tareas pertinentes con el fin de cumplir con los objetivos planteados y, en general, crear los controles como herramienta para fortalecer los

procesos llevados a cabo por los dominios de RRHH y Telecomunicaciones concernientes con la SdI.

2. Seleccionar una herramienta SIEM de acuerdo a sus características y las necesidades de BIOFILM S. A., para implantar en la empresa.

Antes de seleccionar la herramienta para la implantación en la infraestructura de red, se hizo un estudio investigativo representado en un cuadro comparativo, en el cual se colocaron en evidencia las competencias y facultades que posee el tipo de herramienta SIEM con respecto a otros tipos de herramientas que, a razón de los investigadores del proyecto y de los empleados de TI de la empresa BIOFILM S.A., son las de mayor uso y de mayores capacidades para la gestión de redes. En este estudio se determinaron aspectos o parámetros comparadores para la diferenciación de los distintos tipos de herramientas analizadas.

Dentro de los parámetros comparadores, se utilizaron aquellos que permitieron determinar que el tipo de herramienta no solo sirva para monitorizar redes, sino también para gestionarlas, por lo cual, las características de correlación de eventos, identificación de patrones de ataque y la creación de bases de conocimiento, se utilizaron en la comparación para la determinación del tipo de herramienta, por ser características realizadas netamente por herramientas de gestión de redes. Del mismo modo, se utilizó como comparación el monitoreo de activos asociados a la red, debido a que es una tarea que se debe realizar en la infraestructura de red de BIOFILM S.A., para mantener control y conocimiento de todos los dispositivos asociados a la red. Como resultado de esta comparación, se obtuvo que el tipo SIEM es la mejor solución a las exigencias que presentaba la empresa en cuestiones de redes.

Luego de lo anterior, también mediante un estudio investigativo sobre las herramientas SIEM más utilizadas actualmente en el mercado, se hizo la selección de la que mejor cumple con los requisitos que plantearon las necesidades que presentaba BIOFILM S.A. a nivel de TI. Para dicha escogencia, entre los investigadores de este proyecto y el personal de la división de TI que la empresa puso a disposición, se definieron las herramientas SIEM más utilizadas, y se estipularon nuevos aspectos comparadores y diferenciadores entre las mismas, los cuales permitieron identificar y escoger la herramienta adecuada para implantar en la planta principal de la empresa que se encuentra en la zona industrial de Cartagena de Indias D.T y C.

3. Implantar una herramienta SIEM en el dominio de Telecomunicaciones para la gestión de la infraestructura de red en la empresa BIOFILM S.A.

Después de haber escogido la herramienta SIEM a implantar, se procedió a crear un espacio controlado en la sección de TI de la planta, dotado con todo lo necesario para el desarrollo de simulaciones y pruebas que sirvieron como ajustes de detalles y recopilación de información, antes de la entrega final de la herramienta, *(ver anexo 3)*. Este proceso se llevó siempre a cabo en compañía del personal competente que la empresa designó para este proyecto. Estos empleados se encargaron de verificar que los procesos que se realizaron en el marco de este objetivo, se desarrollaran de la mejor manera sin presentar fallos o interrupciones en la funcionalidad de la red y la prestación de sus servicios.

Los resultados y comportamientos observados en la realización de las pruebas, permitieron el ajuste de características relacionadas con la funcionalidad de la herramienta, con el fin de implantar una herramienta estable que permitiera potencializar la gestión sobre los procesos pertinentes con la SdI e impulsara la continuidad del negocio de la empresa.

4. Crear un aplicativo móvil para el dominio de Recursos Humanos que permita potencializar la divulgación, aprendizaje y concientización de las políticas de seguridad de la empresa.

En la estipulación inicial del proyecto y en el alcance del mismo, se acordó que la intención principal del aplicativo móvil, sería netamente informativa. Con el transcurrir del desarrollo de los objetivos, la empresa realizó una petición de convertir la APP y el OVA, en herramientas complementarias, es decir, se planteó que el OVA debía ser utilizado para impartir y adquirir conocimientos sobre las políticas de SdI, mientras que la APP debía ser utilizada para la evaluación de dichas políticas. Para hacer esto posible, la APP dejó de ser informativa, para convertirse en un juego de preguntas que permite evaluar a los empleados de la empresa. Teniendo en cuenta este cambio, se realizó su desarrollo.

Para la creación del aplicativo móvil, se requirió de un método de desarrollo común que permitiera organizar las tareas de una forma ágil. Para ello, se empleó un método de desarrollo software orientado a aplicaciones móviles llamado **Mobile-D,** basado en metodologías conocidas

pero aplicadas de forma estricta, tales como Extreme Programming (XP)[8], Crystal Methodologies[9] y Rational Unified Process[10]. En el ciclo de vida que plantea esta metodología, se creó un estado del arte sobre temáticas relacionadas con el desarrollo de aplicativos móviles y/o la utilización de la metodología Mobile-D, como forma de representar la fase de levantamiento de información. Con la realización de este estado del arte, se tuvo información relevante que, a razón de los investigadores de este proyecto, tenían mayor afinidad, importancia y trascendencia para el desarrollo del aplicativo.

En la etapa de exploración e inicialización, se centró la atención en la planificación y los diferentes conceptos básicos que fueron necesarios para llevar a cabo el desarrollo del aplicativo móvil. A su vez, en estas etapas se examinaron el alcance y su relación con las funcionalidades y los requisitos. El establecimiento de los requisitos y funcionalidades se realizó mediante una entrevista de levantamiento de requerimientos realizada a la jefa de TI y a dos empleadas pertenecientes a la división de Comunicaciones *(ver anexo 4)*, y la cual fue profundizada en otra reunión realizada *(ver Anexo 5).* Con estos requerimientos, se obtuvieron los requisitos y se crearon los modelos pertinentes que sirvieron para desarrollar el aplicativo móvil.

Ya en etapas posteriores, se evaluaron los diferentes recursos con los cuales se contó para llevar a cabo las distintas tareas estipuladas. En la etapa final o de pruebas, se repararon los errores y se verificó que la aplicación fuese estable, es decir, que se integrara de forma correcta los diferentes módulos necesarios dentro del programa. No obstante, se debió hacer una revisión a nivel general que permitió entregar a la empresa soluciones de calidad.

5. **Construir y anexar un OVA al LMS empresarial para la evaluación de los conocimientos sobre las políticas de seguridad de la empresa.**

Como se mencionó en el alcance, en la etapa del anteproyecto, se había planteado desplegar el OVA en el LMS empresarial, pero en la etapa de desarrollo del mismo, por petición de la

[8] XP: Es una metodología ágil centrada en potenciar las relaciones interpersonales como clave para el éxito en desarrollo de software.
[9] Crystal Methodologies: Son una familia de metodologías ágiles, donde cada una de ellas está adecuada para un tipo de proyecto distinto, orientado hacia empresas grandes.
[10] Rational Unified Process: Es una metodología ágil que utiliza el enfoque de la orientación a objetos en su diseño y está documentado el uso de UML para ilustrar los procesos en acción.

empresa, se cambió su plataforma de implementación, es decir, se dejó a un lado el LMS empresarial y se utilizó el Servidor de Archivos. Quedando el OVA alojado en este último.

En la construcción del OVA, se aplicaron técnicas para la recolección de información y revisión de datos, y después se definieron los contenidos temáticos requeridos en la construcción del objeto virtual de aprendizaje, mediante un acta de levantamiento de requerimientos (*ver anexo 4)*. Posterior a la creación del OVA, se realizaron una serie de pruebas internas que permitieron verificar el funcionamiento de la herramienta. Se resalta que, en el proceso de implementación del OVA, se contó con el apoyo del personal competente de BIOFILM S.A para el despliegue de los contenidos temáticos multimediales y, así mismo, para la formulación del contenido de enseñanzas que permiten impartir el conocimiento de la temática de la SdI.

10. RESULTADOS Y DISCUSIÓN

Como procedimiento para la obtención de los controles para el fortalecimiento y potencialización de los procesos desarrollados por los dominios de RRHH y Telecomunicaciones en cuestiones de SdI, se realizaron cada uno de los objetivos planteados, respetando lo mencionado en la metodología con respecto al desarrollo por objetivos, así:

10.1. IDENTIFICAR LAS POLÍTICAS DE SEGURIDAD DE LA EMPRESA SOBRE LAS CUALES ESTARÁN SOPORTADOS LOS CONTROLES A DESARROLLAR.

Realizando lo planteado en la metodología para el desarrollo de este primer objetivo, se realizó una reunión en las instalaciones de BIOFILM S.A. con la jefa de la división de TI de la empresa, Ingeniera Yenis Álvarez Jiménez, con el fin de identificar las políticas de seguridad que los controles a desarrollar deben respetar para no violar o estar en contra de las normatividades que la empresa maneja, con la finalidad de hacer que estos controles no conduzcan a los empleados a violar las reglas indirectamente.

En el proceso de creación y desarrollo de los controles para la seguridad de la información de BIOFILM S.A., y su puesta en marcha, existen políticas y normatividades que rigieron la disponibilidad de los recursos que la empresa dispuso a los investigadores de este proyecto, para la realización del mismo. Por tanto, para saber el procedimiento correcto que se debió realizar al momento de solicitar y consumir un recurso de la empresa, los investigadores y el personal encargado por la misma, determinaron las políticas que estuvieron relacionadas con el proyecto *(ver anexo 2).* Estas políticas están reseñadas en la siguiente tabla.

POLITICA GENERAL DE SEGURIDAD
1. CONSIDERACIONES GENERALES
• Los usuarios internos y externos estarán obligados a cumplir con las normas y políticas dadas por BIOFILM para el uso de los equipos de cómputo y comunicaciones e internet.
2. POLÍTICA DE USO DE TECNOLOGÍA
• Tanto el equipo que le fue entregado como el software que éste posee es propiedad de

BIOFILM S.A. y está bajo completa responsabilidad del usuario. la compra de equipos y software en general se debe tramitar únicamente por medio del proceso de gestión de tecnología de información (GTI), mediante la solicitud de equipos.
• Cumplir con las políticas de acceso a las aplicaciones, como buscar entrenamiento y autorización por parte del administrador de la aplicación y/o el líder funcional.
• Todo software que se desee adquirir o desarrollar internamente debe ser aprobado por la gestión de tecnología de información, este se debe solicitar, con el fin de analizar previamente los requisitos para su instalación, compatibilidad con el sistema operativo y mantenimiento, así como su ajuste al plan estratégico. así mismo, el usuario es responsable de respetar la ley de derechos de autor, no abusando de los servicios para distribuir de forma ilegal licencias de software o reproducir información sin conocimiento del autor, las licencias deben reposar únicamente en la gestión de tecnología de información.
• Por ninguna razón los funcionarios de la empresa podrán copiar ni retirar programas o archivos de la empresa con fines particulares
• Todas las copias de respaldo del software oficial de BIOFILM S.A. deben reposar en sus instalaciones.
3. POLÍTICA DE ACCESO A LOS SERVICIOS DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES
• El acceso a los servicios de tecnología de información y comunicaciones de la compañía debe ser solicitado por medio del formato correspondiente y debe ser autorizado por el jefe inmediato o por la instancia correspondiente de acuerdo con el servicio requerido, este procedimiento debe ser seguido inclusive si el usuario trae su computadora personal a las instalaciones de BIOFILM.
• Los dueños de proceso, deben definir los perfiles de usuario, roles y aprobar, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos. así mismo, frente a cambios organizacionales deben verificar y ratificar todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.
• Los dueños de proceso son responsables de definir los requerimientos de protección para su

información y de garantizar que existan controles adecuados para proteger su información de modificaciones no autorizadas o destrucción al igual que de divulgaciones no autorizadas.

- No se debe intentar utilizar ningún recurso de tecnología de información y comunicaciones de la compañía o cualquier otra entidad o persona a menos que haya recibido la autorización apropiada para hacerlo.
- Una vez que el usuario tenga acceso a los sistemas de BIOFILM, contará con carpetas de acceso compartido por departamento en la intranet o Servidor de Archivos, toda la información debe ser almacenada única y exclusivamente en esta vía.
- La conectividad de la red hacia los servidores que ofrecen los servicios de ti se encuentra protegida por un Firewall para evitar accesos no autorizados a las aplicaciones. las conexiones que se deban hacer hacia estos dispositivos desde internet serán únicamente a través de CITRIX.

3.1. ACCESO REMOTO

- La única plataforma aprobada para conexión remota a las aplicaciones es CITRIX.
- Para consultores de aplicaciones externos a BIOFILM, en caso de que se requiera acceso temporal, se otorgara acceso únicamente a la aplicación durante el desarrollo de la actividad específica, la cual debe ser monitoreada por el especialista técnico de la aplicación.

3.2. ACCESO REMOTO A LOS EQUIPOS DE PRODUCCIÓN EN BIOFILM CARTAGENA

- Es importante mencionar que el uso inapropiado de los recursos dispuestos para los usuarios, expone a la empresa a riesgos innecesarios como los virus informáticos, interrupción de las redes y sus sistemas, como también riesgos en la operación de las líneas.

ALCANCE

Las normas mencionadas en este apartado cubren el uso apropiado del sistema de acceso remoto para los equipos de producción y aplica a todos los funcionarios, proveedores, contratistas y en general cualquier usuario que haga uso de forma autorizada.

- Mediante el uso de la tecnología de acceso remoto, los usuarios declaran conocer que sus computadores y equipos móviles, ya sea institucionales o personales son una extensión de las redes de la empresa y como tales, están sujetos a las mismas normas y reglamentos que se aplican a los equipos dentro de las dependencias de la empresa.

4. POLÍTICA DE USO DE INFORMACIÓN

4.1. ACTIVIDADES NO PERMITIDAS

- Mal uso del software: los usuarios no podrán efectuar cualquiera de las siguientes labores sin previa autorización escrita del director de su departamento:

  (1) copiar software para utilizar en sus computadores en casa;

  (2) proveer copias de software a contratistas, empleados temporales, amigos, parientes o cualquier otra tercera persona;

  (3) instalar software en cualquier computador o servidor de la empresa;

  (4) descargar software de internet u otro servicio en línea a cualquier computador o servidor salvo que exista un contrato de BIOFILM S.A. con un proveedor de servicios, y esté autorizado por el jefe del área y el gerente de servicios de tecnología de información y comunicaciones;

  (5) modificar, revisar, transformar o adaptar cualquier software;

  (6) descompilar o ingeniería de reverso en cualquier software. los usuarios deberán informar a su jefe inmediato cuando tengan conocimiento de cualquier violación al uso adecuado y legal del software o de los derechos de autor.

- Sistemas de información: se considera como falta grave, el modificar o agregar información, sin la debida autorización, a cualquiera de los sistemas de información de BIOFILM de manera que se viole cualquier otra política o procedimiento oficial de la compañía previamente establecidos.

4.2. MANEJO DE INFORMACIÓN CONFIDENCIAL

- Toda información clasificada como confidencial debe ser manejada bajo responsabilidad de quien la origina o produce y su conocimiento debe ser limitado estrictamente a quienes "necesitan conocer" buscando que sea en lo posible al más alto nivel gerencial solamente.

5. SALIDAS DE EQUIPOS DE CÓMPUTO, DOCUMENTOS Y EQUIPOS

- Cualquier activo de BIOFILM S.A. para salir de las instalaciones debe tener una autorización del respectivo jefe. dicha autorización se debe presentar a la salida para que quede registrado el retiro del activo. el hecho que el personal de seguridad no exija la

presentación del formato diligenciado no exime a nadie del deber de diligenciar y entregar al personal de seguridad dicho formato.

- Los usuarios que requieran para el buen desempeño de sus funciones retirar activos de la compañía deberán portar un documento "permanente" que conste que dicho activo es utilizado como herramienta de trabajo, y debe tener la autorización de su jefe inmediato, y para casos de computadores portátiles tener el visto bueno de la gestión de tecnología de información (GTI).

6. POLÍTICA DE USO DE EQUIPOS DE ESCRITORIO Y PORTÁTILES

- Siempre deberá guardar su información en la intranet. esta estará físicamente centralizada en el servidor y de esta manera estará más segura en caso de pérdida o daño del equipo. en caso de almacenar información en el disco duro de su equipo de escritorio, portátil o cualquier otro equipo, el usuario es responsable de guardar copias de seguridad apropiadas de la información importante.
- Ninguna información de la compañía debe ser almacenada ni procesada en computadores u otro equipo de propiedad de los usuarios.

7. POLÍTICA DE SOFTWARE

- Va en contra de esta política la instalación de software o cualquier otro material en la infraestructura de tecnología de información y comunicaciones de la compañía que no sea obtenido de forma que se autorice a BIOFILM a usarlo en sus sistemas.
- La instalación de cualquier software diferente en una estación o portátil sin la debida autorización de tecnología de información, será considerada una violación a las políticas de seguridad. el software será borrado inmediatamente y traerá consigo la aplicación de sanciones disciplinarias.

8. POLÍTICA DE USO DEL CORREO ELECTRÓNICO

- No debe considerarse las comunicaciones electrónicas como privadas o seguras. el correo electrónico puede ser almacenado en un número indefinido de computadores y copias de sus mensajes pueden ser reenviados a otros, ya sea electrónicamente o en papel. así mismo, el

correo electrónico enviado a usuarios inexistentes o equivocados implica que esa información pueda ser de conocimiento de terceras personas.

9. POLÍTICA DEL USO DE INTERNET

- El acceso a internet dentro de las instalaciones de la compañía está permitido únicamente por medio de la conexión proporcionada por BIOFILM bajo ninguna circunstancia los usuarios podrán acceder a internet por medio de conexiones dial-up, servicios Wireless o cualquier otro método de conexión diferente al proporcionado o autorizado por BIOFILM.

No se debe:

- Tratar de burlar la seguridad, el control de acceso o los mecanismos de filtrado de contenido utilizados en la red de BIOFILM.
- Interferir intencionalmente con la operación normal de la red, incluyendo la propagación de virus de computación, hacking y generar volúmenes de tráfico que afecte sustancialmente el desempeño de la red afectando otros usuarios.
- Usar el correo electrónico, web u otras facilidades para la creación de obligaciones legales o contractuales a menos que sea específicamente autorizado por la gerencia.
- Conectar los equipos de cómputo de BIOFILM directamente a internet por ningún medio (ras, módem, Wireless, vía telefónica, cable, etc.). a menos que esté expresamente autorizado por la gestión de tecnología de información y comunicaciones (GTI) como es el caso de los usuarios móviles y virtuales.

10. POLÍTICAS DE SEGURIDAD DE LOS DATOS Y COPIAS DE SEGURIDAD

- Información no propia: ningún usuario deberá alterar o copiar un archivo perteneciente a otro usuario sin el previo consentimiento del dueño del archivo. la capacidad de poder leer, alterar o borrar un archivo perteneciente a otro usuario, no implica que se tenga el permiso o autorización para leer, alterar o borrar ese archivo. los usuarios no deben utilizar el sistema de computación para alterar la integridad de los archivos y correos de otros.

- Acceso a otros computadores y redes: la capacidad de un usuario para conectarse a otro sistema de cómputo, a través de la red o de módem, no implica que tenga el derecho de conectarse a esos sistemas de hacer uso de los mismos a menos que tengan autorización

específica por parte de los operadores de esos sistemas y de BIOFILM para dicho proceso deberá tener en cuenta que durante su conexión deberá estar desconectado de la red corporativa de BIOFILM.
11. RELACIÓN DE ESTA POLÍTICA CON OTRAS DISPOSICIONES DE BIOFILM O LEGALES
• Conformidad con leyes aplicables y licencias: en la utilización de los recursos de tecnología de información y comunicaciones, los usuarios deberán guardar conformidad con todas las licencias de software, derechos de autor y todas las leyes nacionales e internacionales que regulen la propiedad intelectual y las actividades en-línea.
• El envío y recepción de software por el personal de BIOFILM proveniente o no del exterior remitido por compañía y/o personas relacionadas o no con BIOFILM deberá ser previamente conocido y autorizado por escrito por la gestión de tecnología de información y comunicaciones y por el gerente general.
• Otras políticas aplicables: en la utilización de los recursos de tecnología de información y comunicaciones, los usuarios deberán guardar conformidad con todas las demás políticas y pautas de la empresa.

Tabla 4. Políticas de seguridad a respetar por los controles. (BIOFILM S.A.).

Dentro de las políticas de uso de tecnología, hay puntos normativos que informaron el procedimiento correcto para la compra, uso de herramientas y equipos que ayudaron en el desarrollo del proyecto. De igual modo, existen políticas que indicaron el inicio del mismo y el guardado de los resultados de cada proceso llevado a cabo en su desarrollo. Todos estos métodos debieron estar avalados y aprobados por la Gestión de Tecnología de Información y en general por la empresa. Para no ir en contra de esta norma, los investigadores del proyecto diligenciaron el permiso correspondiente para poder realizar este proyecto y contar con los recursos necesarios para el desarrollo del mismo, lo cual puede ser verificado con la carta de aval de la empresa presente en los anexos *(ver anexo 1).* También existe un convenio de cooperación, firmado entre la Universidad de Cartagena (UdeC) y BIOFILM S.A., el cual puede ser validado ante el Centro de Inserción Laboral y Responsabilidad Social de la UdeC.

Las políticas de acceso a los servicios de Tecnología de Información y Comunicaciones, se establecieron como marco de control para el proyecto, debido a que cada vez que los investigadores se movilizaron a la empresa para hacer pruebas, reuniones y capacitaciones que ameriten el uso de los servicios dispuestos por la división de TI de la compañía, estos recursos debieron ser solicitados previamente mediante un formato debidamente diligenciado y autorizado.

Las otras normatividades hacen referencia a la forma tangible o intangible en que se encuentran repartidos los recursos, su buen uso, la disponibilidad y los permisos para su utilización. Con el cumplimiento de todas las normativas presentes en la tabla anterior, se garantizó el buen desarrollo y puesta en marcha de los controles desarrollados.

10.2. SELECCIONAR UNA HERRAMIENTA SIEM DE ACUERDO A SUS CARACTERÍSTICAS Y LAS NECESIDADES DE BIOFILM S.A., PARA IMPLANTAR EN LA EMPRESA.

Como desarrollo de este objetivo, se realizó un estudio investigativo en el cual se lograron identificar las herramientas que, a criterio de los investigadores de este trabajo y de los empleados de TI puestos a disposición por la empresa BIOFILM S.A., son las más utilizadas en la industria para la gestión y administración de redes, y en el que se resaltaron las necesidades básicas que debía cumplir la herramienta a implantar en la empresa para soportar las exigencias actuales que acarrea el mercado con respecto a redes. Este estudio permitió hacer un cuadro comparativo en el que se destacaron las características que cada una de las herramientas cumple con respecto a requisitos específicos que plantea la infraestructura de red de la empresa. De este modo, el cotejo de ellas arrojó como resultado la más adecuada para ser implantada en la infraestructura de red de la compañía.

Como aspectos comparadores y diferenciadores, se tuvieron en cuenta aquellos que permiten identificar que la herramienta a implantar no sólo funcione para monitorizar redes, sino también que permita escalar y gestionar más elementos de la organización como aplicaciones, servidores y procesos de negocio. También se valoraron aquellas características que permiten identificar y contrarrestar los nuevos ataques que generan las actuales tecnologías y el desarrollo del

conocimiento malintencionado de terceros, con el fin de aminorar el impacto negativo que esto puede causar a la red. De igual modo, se contemplaron los aspectos que permiten brindar una visión global y en tiempo real de la empresa y a su vez, otorgan el beneficio de saber en qué momento la red necesita la adición o sustracción de hardware que ayude a un mejor funcionamiento de la misma.

Este estudio se desarrolló sobre la documentación guardada directamente en las páginas web oficiales de cada uno de los productos[11], debido a que los escritos encontrados en otras fuentes, se encuentran desactualizados con respecto a los beneficios que actualmente otorgan las herramientas.

A continuación, se muestra el cuadro comparativo creado por los investigadores, a partir de los resultados arrojados por dicho estudio.

ASPECTOS COMPARADORES	**SIEM**	**NAGIOS**	**PRTG**	**SOLARWINDS**	**ZABBIX**	**ICINGA**	**PANDORAFMS**
Licencia gratis	**X**	**X**			**X**	**X**	**X**
Licencia paga			**X**	**X**			**X**
Copia de seguridad en la nube	**X**		**X**				**X**
Correlación de eventos	**X**						
Creación de bases del conocimiento	**X**	**X**			**X**		

[11] Fuentes de búsqueda. SIEM: (SIEM Alien Vault Enterprises, 2009); NAGIOS: (Nagios Enterprises, 2017); PRTG: (AG, 2018) ; SOLARWINDS: (SolarWinds, 2014); ZABBIX: (Zabbix Enterprise, 2005);ICINGA: (Icinga, 2017); PANDORAFMS: (PandoraFMS Enterprises, 2009). Para más información, acceder a las páginas web puestas en las referencias bibliográficas.

Escalabilidad	**alta**	**alta**	**baja**	**Media**	**baja**	**media**	**alta**
Evitar alertas falsas	**X**		**X**			**X**	**X**
Generación de reportes integrales de redes	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Generar alertas	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Gestión de enrutadores	**X**		**X**	**X**			
Identificación de patrones de ataques	**X**	**X**		**X**		**X**	**X**
Monitoreo de la disponibilidad y desempeño de las redes	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Monitoreo de la infraestructura de otros dispositivos	**X**		**X**			**X**	
Monitoreo de la infraestructura de TI	**X**	**X**	**X**		**X**	**X**	**X**
Monitoreo de la web	**X**		**X**	**X**	**X**	**X**	**X**
Monitoreo de servicios en la red	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Monitoreo de servidores	**X**	**X**	**X**			**X**	**X**

Monitoreo del tráfico en la red	**X**	**X**	**X**	**X**		**X**	**X**
Priorización de eventos	**X**			**X**	**X**		**X**
Recolección de métricas	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Representación gráfica de las redes a tiempo real	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Usabilidad de interfaz gráfica	**X**		**X**	**X**		**X**	**X**

Tabla 5. Cuadro comparativo entre herramientas de gestión de redes. (Creado por los Investigadores).

La correlación de eventos, como aspecto comparador, marca la diferencia entre todas las herramientas analizadas y, respetando lo que se planteó en la justificación del proyecto, fue el aspecto más determinante para la selección de la herramienta; debido a que este talante indica la herramienta más competente contra las nuevas amenazas, los nuevos softwares y la actualización de los conocimientos malintencionados de terceros, mediante la aplicación de relación de eventos anómalos y dañinos que se encuentren dispersos en la red, asociándolos a un ataque para luego alertar al supervisor de la red y éste realice el control necesario. Del mismo modo, es importante la creación de bases del conocimiento a partir de la detección de amenazas, puesto que permite optimizar el proceso de correlación, al existir antecedentes registrados de amenazas y su control pertinente. También es importante tener en cuenta la detección e identificación de patrones de ataques, por ser un proceso complementario a la correlación de eventos. Los demás aspectos comparadores proporcionan una visión de los beneficios específicos otorgados por cada herramienta y son el complemento para la correcta elección de la misma.

Por lo anterior y por lo reflejado en el cuadro comparativo, se concluyó que la tecnología SIEM es la que mejor se ajusta a las necesidades que tiene la empresa BIOFILM S.A., para la gestión de las redes. La SIEM supera las prestaciones que brindan las herramientas pagas, lo que directamente permite una disminución de costes de adquisición y potencializa la protección de la infraestructura de red debido a las características destacadas en la comparación. Por tanto, en

consenso con los empleados competentes de la empresa, se decidió implantar este tipo de herramienta para la gestión de la red y su supervisión desde la división de Telecomunicaciones.

Posteriormente, se escogió la herramienta más adecuada dentro de las múltiples SIEM presentes en el mercado, debido a que cada una de ellas se desenvuelve mejor en escenarios específicos. Por tal motivo, mediante el estudio de las herramientas SIEM que, a criterio de los investigadores, son las más utilizadas en el sector industrial, se realizó otro cuadro comparativo que sirvió para determinar la más pertinente para su implantación en la empresa.

CARACTERISTICAS ANALIZADAS	**OSSEC**	**OSSIM**	**GRAYLOG**	**LOGRHYTHM**
Descubrimiento de activos		**X**		
Gestión centralizada	**X**	**X**	**X**	**X**
Recolección de Logs y eventos de seguridad	**X**	**X**	**X**	**X**
Correlación de Eventos	**X**	**X**	**X**	**X**
Análisis de Logs	**X**	**X**	**X**	**X**
Clasificación y Prioridad de eventos	**X**	**X**	**X**	**X**
Monitoreo en tiempo Real	**X**	**X**	**X**	**X**
Normalización	**X**	**X**	**X**	**X**
Reportes	**X**	**X**	**X**	**X**
Interfaz Gráfica de administración	**X**	**X**	**X**	**X**
S.O SOPORTADO				
LINUX/UNIX	**X**	**X**	**X**	**X**
MAC	**X**	**X**		
BSD	**X**	**X**		
WINDOWS	**X**	**X**		**X**

Tabla 6. Comparativos entre herramientas SIEM. (Tomada y modificada de Avella Coronado et al., 2015).

Todas las herramientas que fueron motivo de comparación en la tabla anterior, ofrecen características que permiten escoger cualquiera de ellas para su implantación, sin embargo, los detalles mínimos ayudaron a la inclinación hacia una en específico. En este sentido, los sistemas operativos soportados por las herramientas, se establecieron como una característica determinante para la elección, puesto que la herramienta no debe ligar a la división de TI al uso de un solo sistema operativo para la gestión de la red, sino más bien a la diversificación de opciones. Del mismo modo, la característica de descubrimiento de activos fue otro factor importante para escoger la herramienta, debido a que otorga la facilidad al administrador de la red de realizar variadas opciones con los nuevos dispositivos y softwares anexados a la red y detectados posteriormente, lo que simplifica aún más el trabajo de los operarios de la infraestructura de red. Mientras tanto, las otras características o aspectos comparadores, son propios de la tecnología SIEM.

Por último, después de establecer todos los criterios de selección, el consenso de los investigadores de este trabajo y los empleados de TI dispuestos por la empresa, arrojó como resultado que AlienVault OSSIM enmarcada dentro de la herramienta OSSIM y perteneciente a la tecnología SIEM, sería la herramienta a implantar en la empresa como sistema para la gestión de las redes y dispositivos asociados a ella.

10.3. IMPLANTAR UNA HERRAMIENTA SIEM EN EL DOMINIO DE TELECOMUNICACIONES PARA LA GESTIÓN DE LA INFRAESTRUCTURA DE RED EN LA EMPRESA BIOFILM S.A.

Después de haber escogido la herramienta SIEM correspondiente, se procedió a implantarla en la red principal de la empresa, sin deshabilitar las otras herramientas de monitoreo y seguridad que la red posee. Esto de manera global se plantea como un marco controlado de pruebas para la realización de uno de los requisitos estipulados.

En este marco de pruebas se hicieron todos los ajustes de la herramienta, mediante la determinación de eventos claves para la seguridad en los dispositivos Windows, Fortinet y Cisco utilizados para conformar la red y relacionar todos los equipos que la componen. También se realizaron procedimientos de monitoreo a dichos equipos para la recolección de logs, métricas y

el fortalecimiento de la base de conocimientos. Luego de haber culminado con todas las configuraciones pertinentes de la herramienta, el marco de pruebas se hizo a un lado y se procedió a colocar la herramienta en pleno funcionamiento.

Lo anteriormente mencionado hace referencia, de manera general, a las tareas desarrolladas a lo largo de todo el proceso. Estas se detallan a partir del literal 7.3.1.

Para la creación del marco de pruebas, se tuvieron presentes las recomendaciones mínimas que brinda el fabricante de AlienVault OSSIM para la instalación de la herramienta. Estas son:

- Procesador de 1.5 GHz doble núcleo o superior.
- Memoria RAM de 2GB o superior.
- Tarjeta de Red 100/1000 Mbps.
- Espacio de almacenamiento de 250 GB.

Las características anteriores, se utilizan para redes de pequeña envergadura y con un pequeño flujo de eventos. Por lo cual, por tratarse de la red de la empresa BIOFILM S.A. que posee un flujo grande de movimientos y transacciones entre los distintos software y hardware asociados a la red, ameritó que la máquina virtual creada en uno de los equipos contara inicialmente con las siguientes características:

- Espacio de almacenamiento de 350 GB.
- 2 tarjetas de Red 100/1000 Mbps.
- Memoria RAM de 8 GB.
- Procesador de 8 núcleos a 2,66 GHz.

Estas características pueden ser verificadas en la siguiente figura.

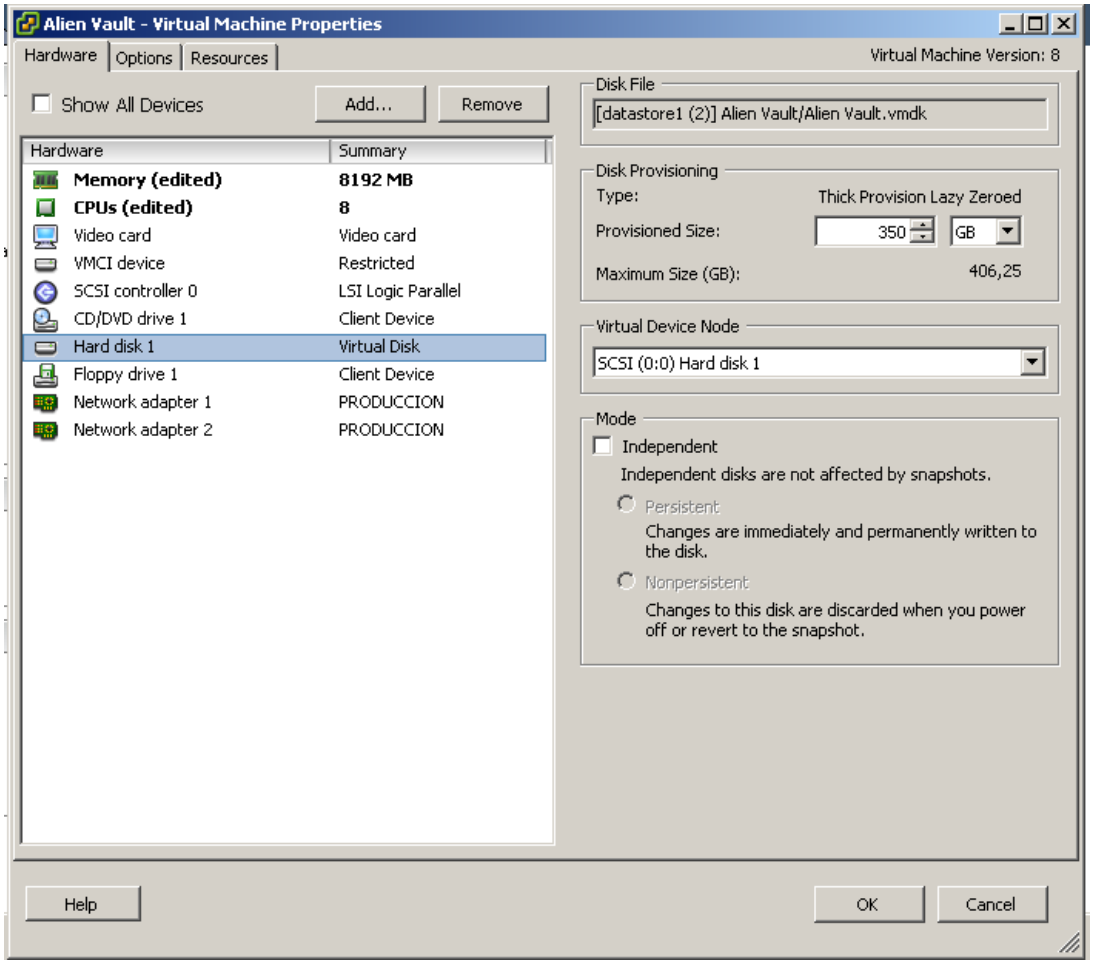


Figura 6. Características de la máquina virtual utilizada para la instalación de la herramienta SIEM.

Estas características de la máquina virtual pueden incrementar dependiendo de la cantidad de eventos que se desarrollen en el transcurso de uso de la herramienta.

10.3.1. INSTALACIÓN

Lo primero que se debió realizar para el proceso de instalación, fue la selección de la versión de AlienVault OSSIM. Fue elegida la primera opción debido a que es la versión servidor que se encarga de la recolección y tratado de eventos, y de la gestión de la red. Además, presenta la interfaz de administrador de red.

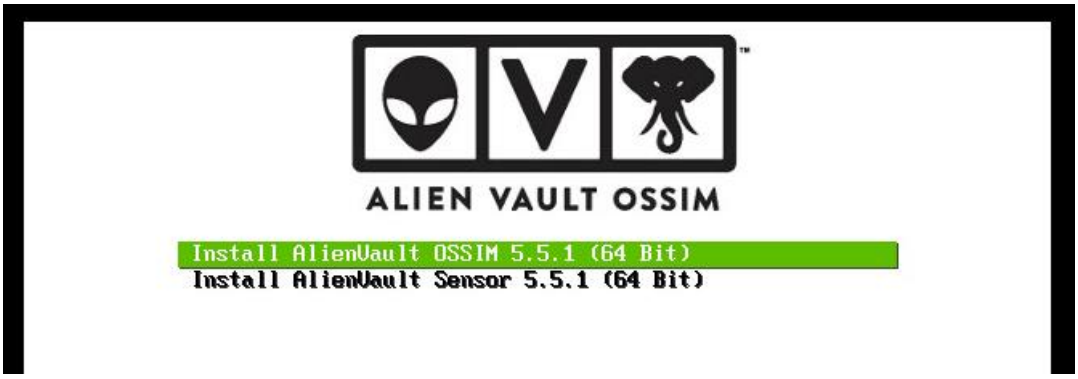


Figura 7. Instalación de AlienVault OSSIM. Selección de la versión.

Luego se seleccionó la tarjeta de red principal y la dirección IP del servidor.

Figura 8. Selección de la tarjeta de red principal.

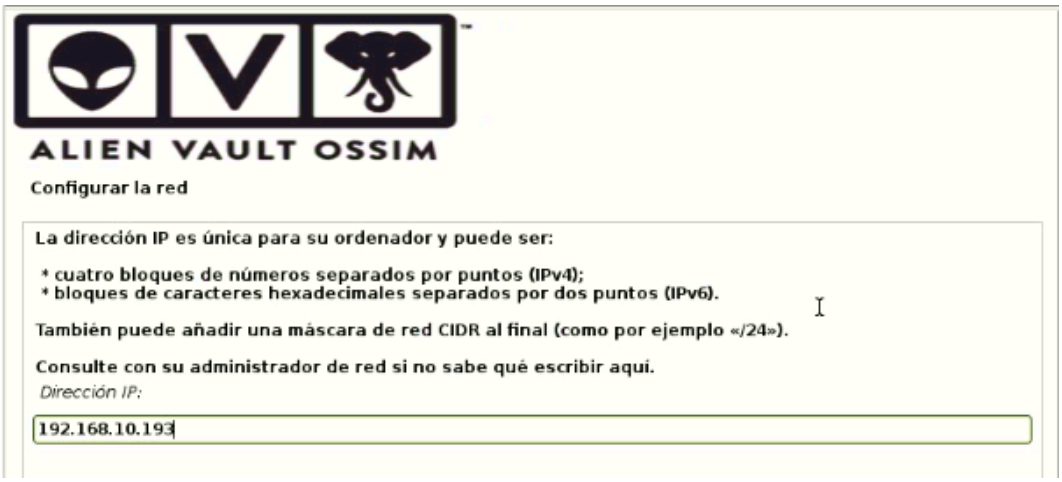


Figura 9. Selección de la dirección IP del servidor OSSIM.

Los demás procedimientos correspondieron a la selección del idioma de instalación, selección del idioma del teclado, anexo de la máscara de subred, puerta de enlace, creación de la contraseña de seguridad para la consola de usuario y configuración de la región. Luego de realizar cada uno de estos procedimientos, se empezó a configurar la plataforma web de administración, a la cual se accede mediante la IP ingresada.

En la siguiente figura, se muestra la configuración de la plataforma web para el administrador. Esta ilustración fue tomada de *Villafuerte Quiroz & Bravo Bravo, 2015*, por petición de la empresa como método de seguridad para la preservación de la información.

Figura 10. Configuración del acceso web. (Tomado de Villafuerte Quiroz & Bravo Bravo, 2015)

Posteriormente a esto, se seleccionó el funcionamiento que tendrían las interfaces de cada una de las tarjetas de red. La interfaz eth0 correspondiente a la primera tarjeta, se utilizó como interfaz principal, para la administración de la red en general; la eth1 se empleó para la recolección de logs y el escaneo; y la eth2 se utilizó para el monitoreo de la red. Esto se puede evidenciar en la *figura 11*.

La tarjeta eth2 fue anexada al sistema posteriormente, para brindar independencia entre interfaces, es decir, que cada una de las interfaces de las tarjetas controlara un aspecto relevante del funcionamiento de la herramienta: Management, Network Monitoring o Log Colection & Scannig.

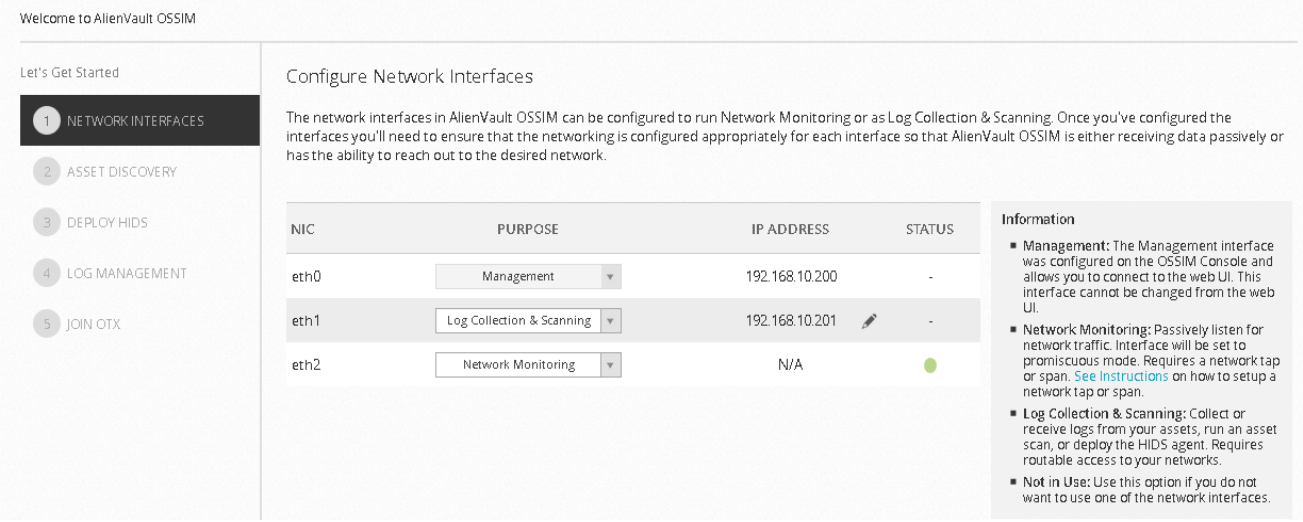


Figura 11. Configuración de las interfaces.

Para hacer que la interfaz eth2 pudiera escuchar y monitorear todas las actividades de la red e identificar los eventos anómalos, se debió agregar una interfaz física en el servidor y configurarla como SPAN[12]. La configuración utilizada se muestra en la siguiente figura:

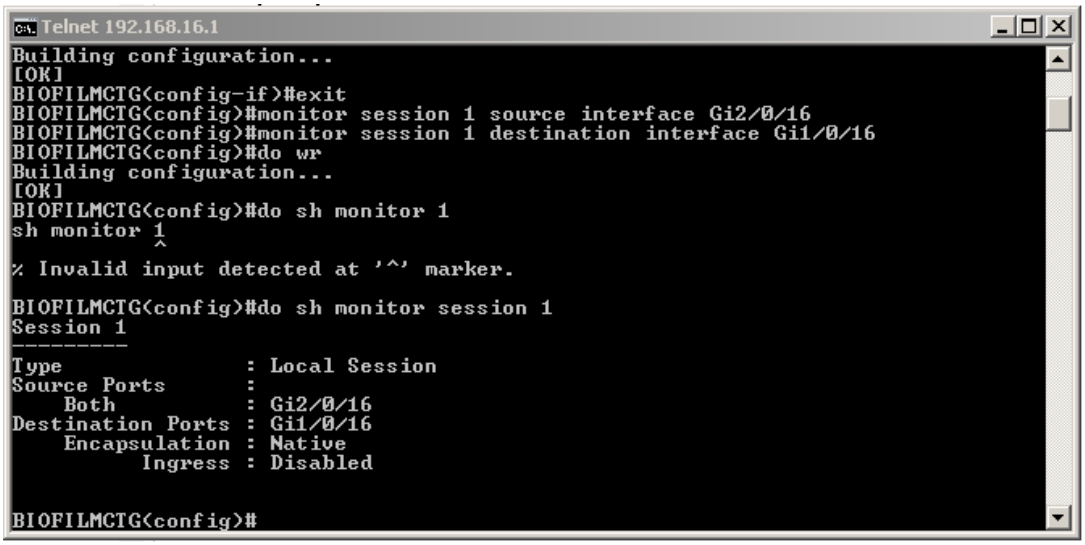


Figura 12. Configuración de la función SPAN en la interfaz Eth 2.

Finalmente, las figuras 14 y 15 muestran como quedó configurada la máquina virtual en la que se encuentra instalada la herramienta.

[12] SPAN: Switch Port Analizer, es una función de los switch que permite escuchar el tráfico a través de los puertos.

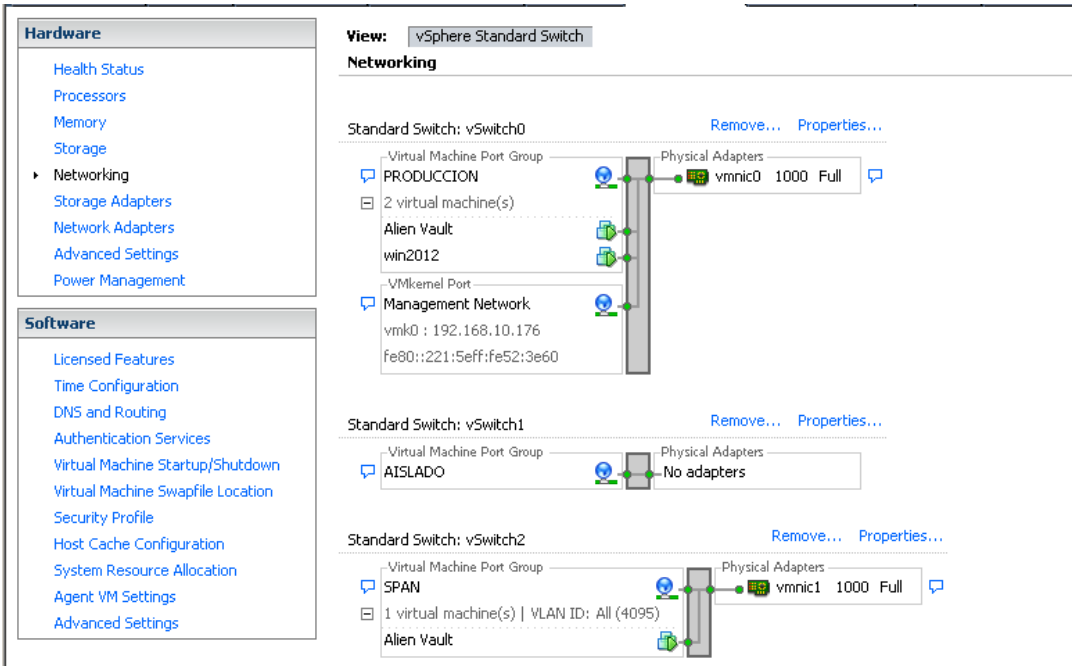


Figura 13. Estado final de la máquina virtual.

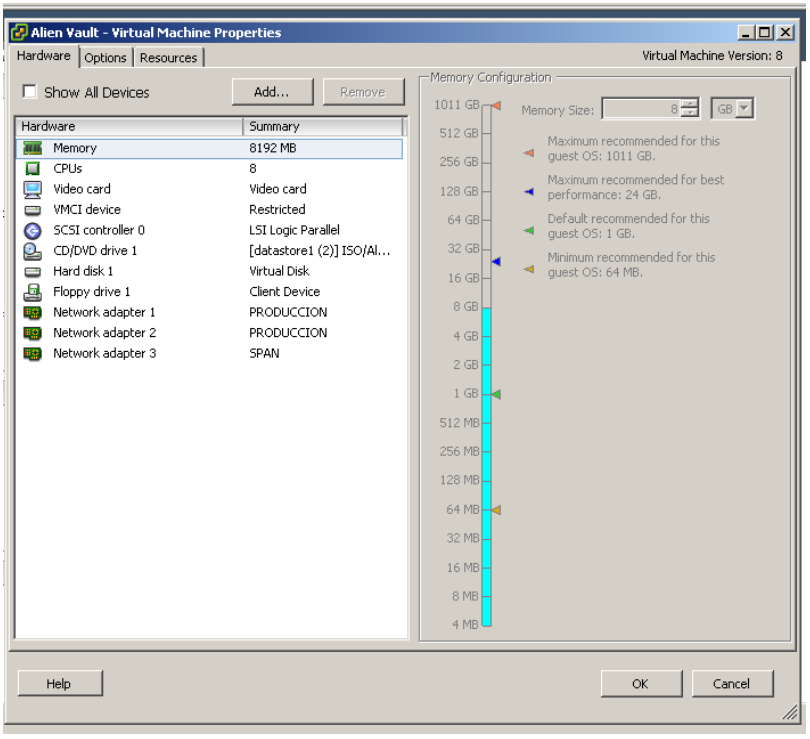


Figura 14. Estado final de la máquina virtual.

10.3.2. DEFINICIÓN DEL ALCANCE DE LA HERRAMIENTA

Antes de iniciar con el proceso de implantación de la herramienta, se hizo necesario definir el alcance que esta tuvo en lo concerniente a su funcionamiento, y el cual puede ser constatado en el *anexo 6*. El alcance de los dispositivos que se anexaron a la herramienta para su funcionamiento, estuvo delimitado así:

- Servidor del Directorio Activo y Servidor de Archivos, con Windows Server 2012 como sistema operativo.
- Switch Core Cisco 3750 G.
- Firewall Fortinet 90 D.
- Red principal de la empresa (192.168.10.0).

Los equipos mencionados anteriormente son los que la herramienta monitorea bajo los lineamientos de este trabajo. Otras configuraciones para los demás dispositivos, queda a disposición de la empresa y su equipo de trabajo pertinente.

10.3.3. DEFINICIÓN DE REQUISITOS

Teniendo en cuenta los requerimientos que debe cumplir la herramienta conforme lo interpuesto por la empresa, y las buenas prácticas para la implementación de la herramienta definidas por el fabricante, se establecieron las tareas o fases para el proceso de implantación, tratadas a partir del literal 7.3.3., las cuales también hacen referencia a los requisitos estipulados.

Los requisitos propuestos por la empresa, están reseñados en la siguiente tabla y pueden ser verificados en el a*nexo 6.*

ID REQUISITO	NOMBRE DEL REQUISITO	USUARIO	DESCRIPCIÓN
RF1	Alcance de la herramienta	No hay usuario determinado	El alcance inicial de la herramienta, se limita al monitoreo del servidor que maneja el Directorio Activo, el cuál es Windows server 2012; al Switch Core

			Cisco 3750 G; al Firewall Fortinet 90 D; y al Servidor de Archivos de Windows 2012 (opcional).
RF2	Inventario de equipos	Administrador de red	Realización del inventario de equipos y dispositivos que componen la red.
RF3	Extracción de logs	Administrador de red	Extracción de los logs de todos los equipos de la red, en específico a los mencionados en el RF1.
RF4	Auditoria de eventos	Administrador de red	Revisión de eventos a auditar: 1) Escaneo de puertos; 2) Bloqueos de usuarios; 3) Autenticaciones fallidas; 4) Creaciones de usuarios; 5) Umbrales.
RF5	Alertas	Administrador de red	Generación de las alertas de los eventos del RF4.
RF6	Cuadros de mando	Administrador de red	Permitir conocer el estado actual de la herramienta.
RF7	Creación de informes	Administrador de red	Generación de los informes de los monitoreos y acciones realizadas dentro de la herramienta.

Tabla 7. Requisitos de la herramienta SIEM.

10.3.4. INVENTARIO DE EQUIPOS

Como primer paso hacia la implantación y el correcto funcionamiento de la herramienta, se realizó la identificación e inventario de los distintos sistemas de información, como los sistemas operativos, productos de software y/o hardware de los que se desea colectar los logs para su posterior normalización y correlación.

Mediante la opción que brinda la herramienta con relación a la realización del inventario de hosts y demás, se detectaron todos los sistemas de información mencionados anteriormente que

pertenecen a la red principal de la empresa (192.168.10.0), con los cuales se pudo realizar la estructuración general de la red. Al mismo tiempo, mediante este proceso, se logró la detección de los equipos vulnerables y causantes de amenazas para el funcionamiento de la red.

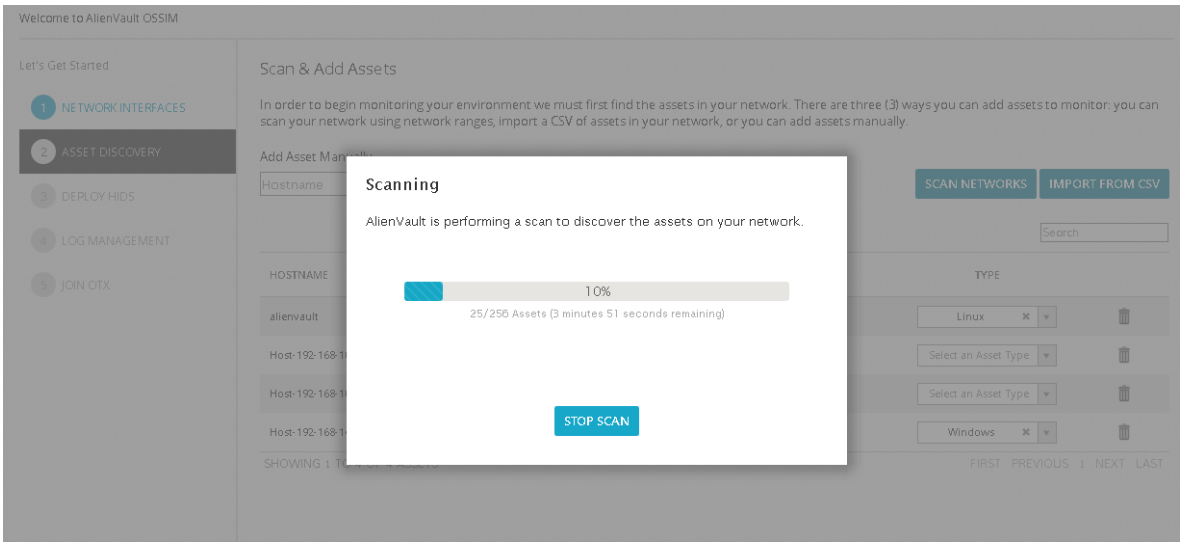
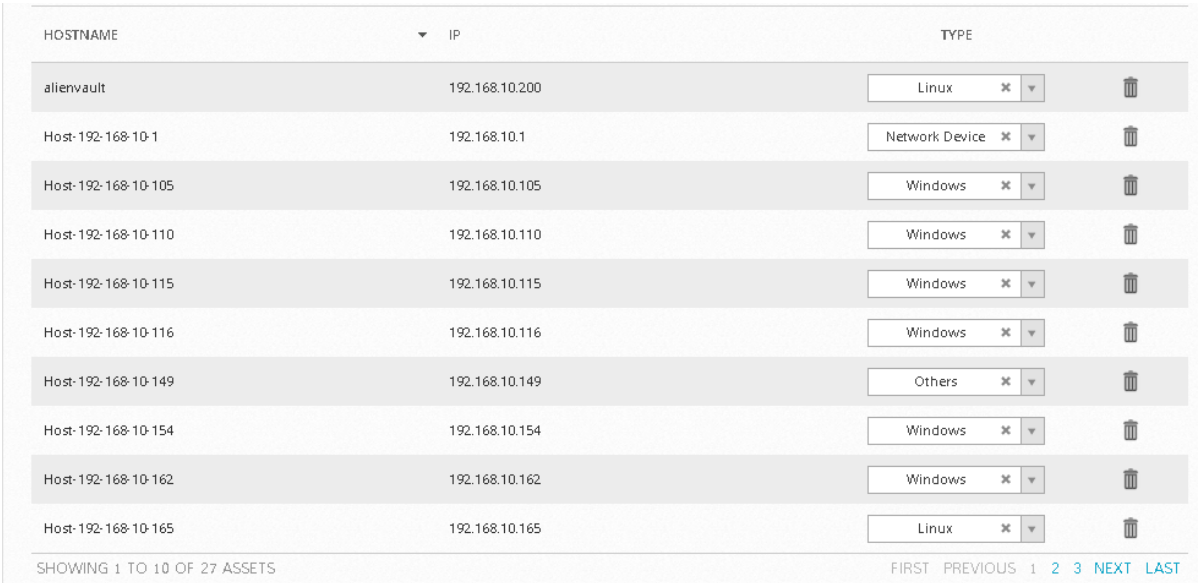


Figura 15. Proceso de realización del inventario de equipos de la red.

El resultado del escaneo y creación del inventario de equipos de la red principal, arrojó como resultado 27 hosts *(figura 17)*. Dentro de los cuales, se encontró el Directorio Activo y el Servidor de Archivos, que pertenecen a esta red, mientras que el Firewall y el Switch Core debieron ser agregados manualmente, por encontrarse en otro segmento de red.



HOSTNAME	IP	TYPE
alienvault	192.168.10.200	Linux
Host-192-168-10-1	192.168.10.1	Network Device
Host-192-168-10-105	192.168.10.105	Windows
Host-192-168-10-110	192.168.10.110	Windows
Host-192-168-10-115	192.168.10.115	Windows
Host-192-168-10-116	192.168.10.116	Windows
Host-192-168-10-149	192.168.10.149	Others
Host-192-168-10-154	192.168.10.154	Windows
Host-192-168-10-162	192.168.10.162	Windows
Host-192-168-10-165	192.168.10.165	Linux

SHOWING 1 TO 10 OF 27 ASSETS
FIRST PREVIOUS 1 2 3 NEXT LAST

Figura 16. Resultado del inventario de equipos de la red principal.

Para la adición del Firewall de Fortinet, se accedió a la ruta *"Environment > Assets > Scan for new assets"* de la interfaz web de administrador, e ingresar la dirección ip del dispositivo.

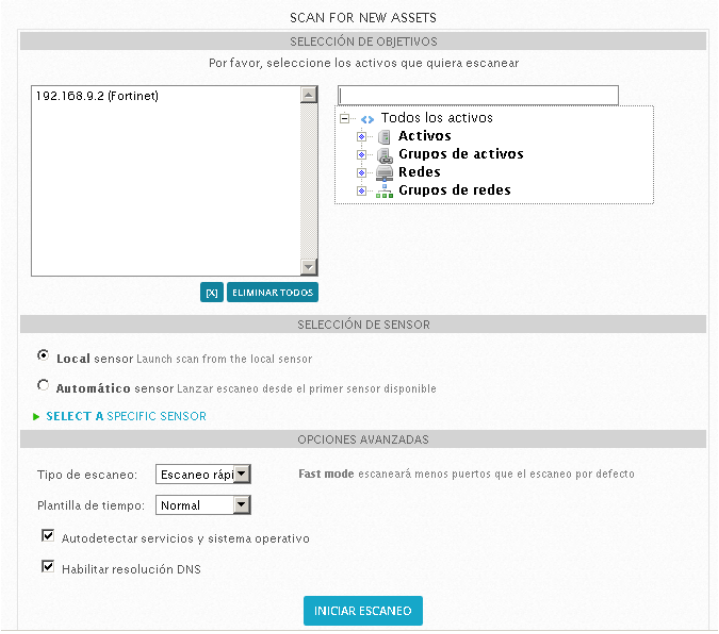


Figura 17. Adición manual del Firewall de Fortinet al inventario de red.

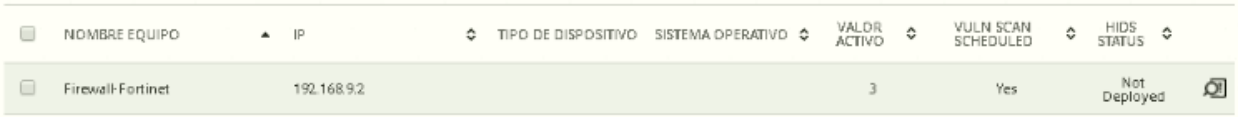


Figura 18.Resultado de la adición del Firewall.

Del mismo modo, se agregó el Switch Core que se encuentra en la red 192.168.16.0/24.

Figura 19. Adición del Switch Core.

Figura 20. Resultado de la adición del Switch Core.

Como último procedimiento, se creó un grupo de activos en el que se encuentran los activos que conforman el alcance del proyecto.

Figura 21. Agrupación de los activos del alcance del proyecto.

10.3.5. EXTRACCIÓN DE LOGS

Para la extracción y recolección de logs de los diferentes dispositivos asociados a la red, como switchs, routers, servidores, Firewalls y demás, se hizo necesario habilitar el servicio Rsyslog que proporciona OSSIM para dicha tarea.

10.3.5.1. CONFIGURACIÓN DE RSYSLOG

Cada uno de los dispositivos englobados en el alcance del proyecto, y en general todos los dispositivos, deben permitir la configuración de envío de logs a un servidor Rsyslog. Esta configuración se realizó en el servidor OSSIM, para cada uno de los dispositivos que conforman la red y que están dentro del alcance de la herramienta. A continuación, se muestran las configuraciones que se realizaron en los dispositivos estipulados en el requisito RF4, los cuales son: el directorio de activos y el Servidor de Archivos Windows server, y el Firewall Fortinet 90D. El Switch Core cisco 3750 G quedó exento de las configuraciones realizadas, debido a que, en esta etapa del trabajo de grado, la empresa cambió de propietarios. Esto conllevó a la misma a hacer transiciones de conexión para realizar empalmes con los nuevos clientes, y en este proceso por cuestiones de seguridad, el switch no podía ser intervenido por personal ajeno a los de la división de TI.

10.3.5.1.1. CONFIGURACIÓN RSYSLOG EN WINDOWS

Para la recolección de los logs procedentes de los dispositivos Windows, OSSIM utiliza el mecanismo HIDS como agente para la comunicación con los equipos y la recepción de los mismos. Como método de configuración, mediante la interfaz web de administración de la herramienta, se acceden a los dispositivos Windows en los cuales se instalará el agente y se selecciona "*Deploy HIDS agent"*, como se muestra a continuación:

Figura 22. Configuración del agente HIDS en el Servidor de Archivos y en el Directorio Activo.

Después se debieron ingresar los datos del usuario con el cual se tiene acceso como administrador a los dispositivos seleccionados.

Figura 23.Ingreso de datos de usuario administrador, para desplegar el agente HIDS.

Luego, para verificar si se habilitó el agente para estos dos dispositivos, se procedió a verificar que en "*Entorno > Detección"*, se listen y se muestren activos, así:

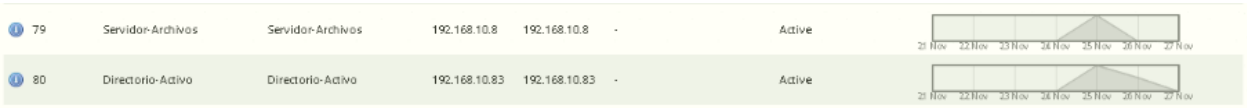


Figura 24. Verificación de despliegue del agente HIDS.

10.3.5.1.2. CONFIGURACIÓN RSYSLOG EN FORTINET

Utilizando la documentación que brinda el fabricante de la herramienta AlienVault OSSIM, se hicieron las siguientes configuraciones para que el Firewall Fortinet 90D permita la conexión con el servidor en el que se encuentra instalada la herramienta, y el envío de los logs generados.

Primero se accedió al Firewall mediante la interfaz web para crear las configuraciones que permiten el envío de logs al servidor OSSIM. Mediante la ruta *"Log & Report > Log Settings"*, se hicieron dichas configuraciones.

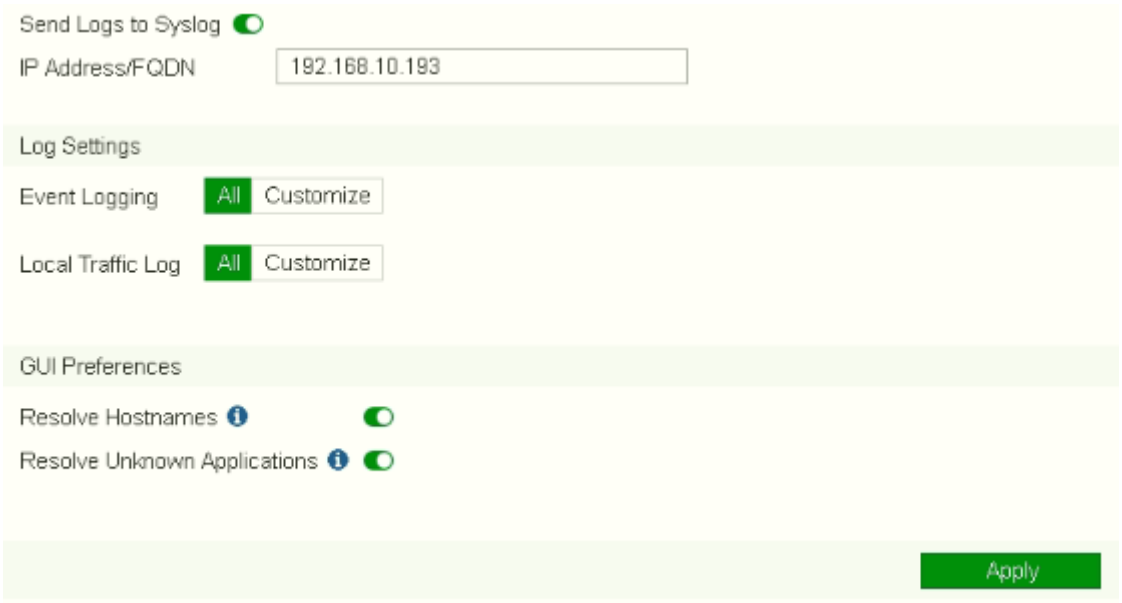


Figura 25. Configuración en el Firewall 90D para enviar logs al servidor OSSIM.

Luego se accedió a la consola de OSSIM con el fin de modificar el plugin de recolección de logs que posee la herramienta para hacer la recepción de los logs provenientes del Firewall. Para modificar este plugin, se ingresó a la ruta *"nano -w /etc/rsyslog.d/fortigate.conf"*, y se escribió lo siguiente:

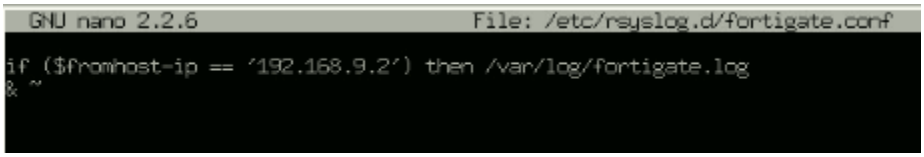


Figura 26. Configuración de Rsyslog para el Firewall.

Después de configurar el archivo, se reinició el servicio Rsyslog mediante el comando *"/etc/init.d/rsyslog restart"*, esto con el fin de que la configuración realizada sea aceptada.

Posteriormente, se creó un archivo de rotación de los logs en la ruta *"nano -w /etc/logrotate.d/fortigate"*, el cual permite manipular y gestionar de manera adecuada los eventos recibidos del Firewall. De igual modo, se procedió a verificar la lectura de los mismos mediante la instrucción *"tail /var/log/fortigate.log -f"*.

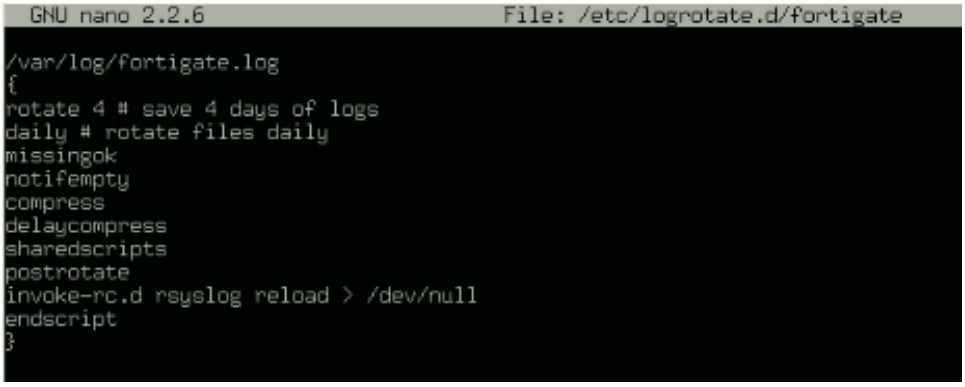


Figura 27. Configuración de archivo de rotación de los logs del Firewall.

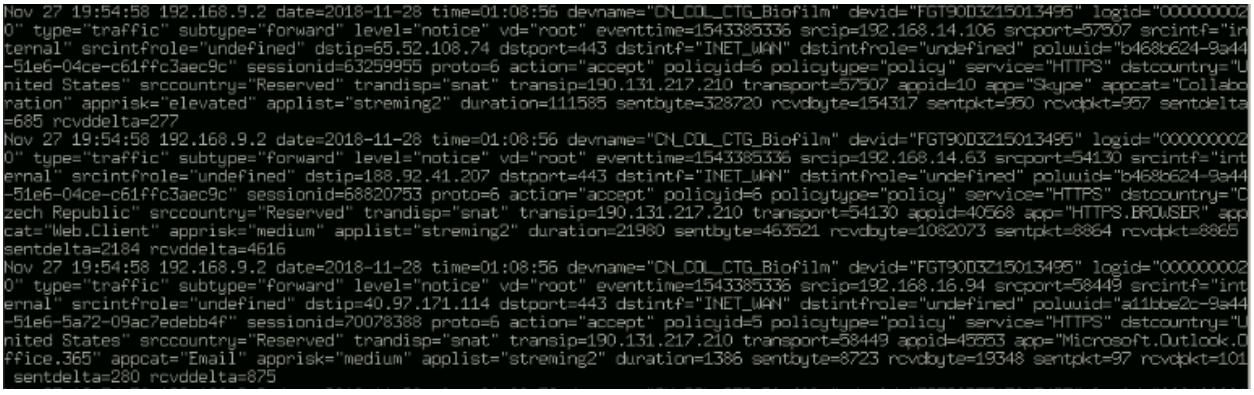


Figura 28. Lectura de logs del Firewall.

10.3.5.2. CONFIGURACIÓN DE LOS PLUGINS CFG Y SQL

Luego de haber configurado el proceso de envío de los logs generados desde los distintos dispositivos, se debió proceder con la configuración de los plugins que ayudarán a captar y almacenar los logs en la base de datos de OSSIM. Los plugins encargados de ese proceso, son CFG y SQL.

Esta configuración se debió realizar para cada uno los dispositivos distintos a los Windows configurados para el envío de los logs.

10.3.5.2.1. CONFIGURACIÓN CFG

Como paso inicial de configuración del plugin, se accedió a la dirección *"/etc/OSSIM/agent/plugins/"*, en la cual se encontraron todos los plugins configurados por defecto al momento de la instalación del servidor OSSIM, y se copió el plugin *fortigate* mediante

la instrucción *"cp fortigate.cfg FirewallFortigate.cfg"*. Luego se accedió al archivo copiado utilizando la instrucción *"nano /etc/OSSIM/agent/plugins/FirewallFortigate.cfg"*. Posteriormente, se modificó el parámetro *plugin_id*, asignándole el valor de *9002*. Del mismo modo, se cambió el parámetro *location*, con el valor de la ruta de dirección del archivo de configuración de logs correspondiente con el Firewall: *"/var/log/fortigate.log"*.

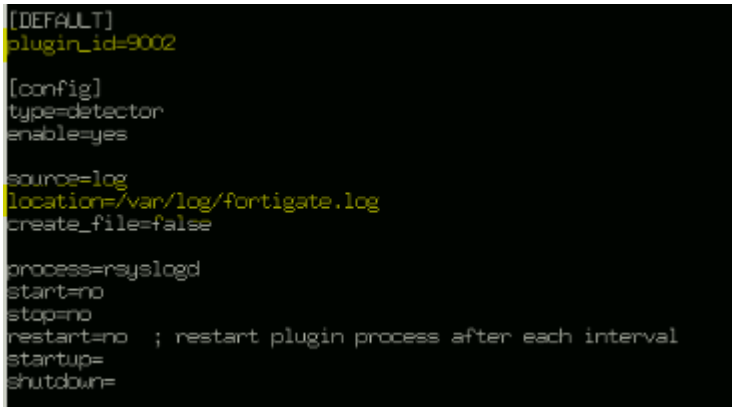


Figura 29. Creación del plugin CFG del Firewall.

Al finalizar esta configuración, se reiniciaron todos los servicios con la instrucción *"alienvault-reconfig -c -v -d"*.

10.3.5.2.2. CONFIGURACIÓN SQL

Para la configuración del plugin SQL del Firewall, se ingresó a la ruta *"cd /usr/share/doc/OSSIM-mysql/contrib/plugins/"*, y se descomprimió el paquete *fortigate.sql*, con la instrucción *"gunzip fortigate.sql.gz"*. Posteriormente, se copió el archivo descomprimido *"cp fortigate.sql FirewallFortigate.sql"*, y se accedió al mismo utilizando el comando *"nano /usr/share/doc/OSSIM-mysql/contrib/plugins/FirewallFortigate.sql"*, para modificar el parámetro *plugin_id* en toda la extensión del archivo, y hacer que coincidiera con el del archivo CFG configurado anteriormente para el Firewall, y de este modo la información se pudiera relacionar.

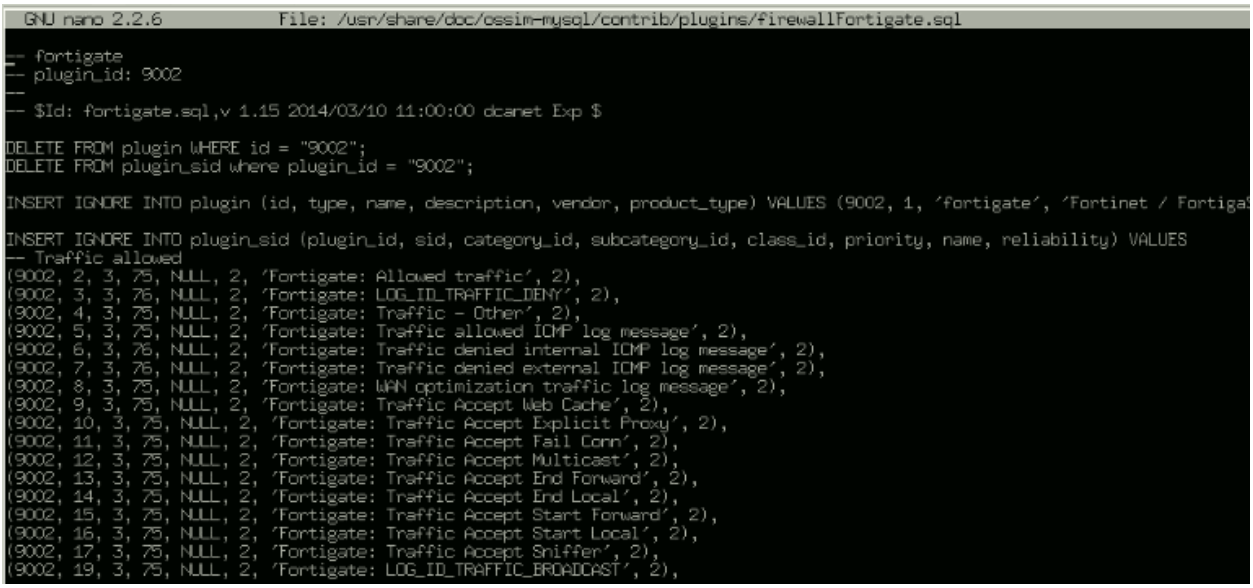


Figura 30. Archivo de configuración SQL del Firewall Fortinet 90D.

Después de realizar esta configuración, dentro de la misma ruta, se asignó el archivo a la base de datos de OSSIM utilizando el comando *"OSSIM-db < FirewallFortigate.sql"*, y se reinició el servicio: *"alienvault-reconfig -c -v -d"*.

Posteriormente, se activó el nuevo plugin en el setup de la consola, en la dirección *"Configure sensor > Configure data source plugins > FirewallFortigate"*.

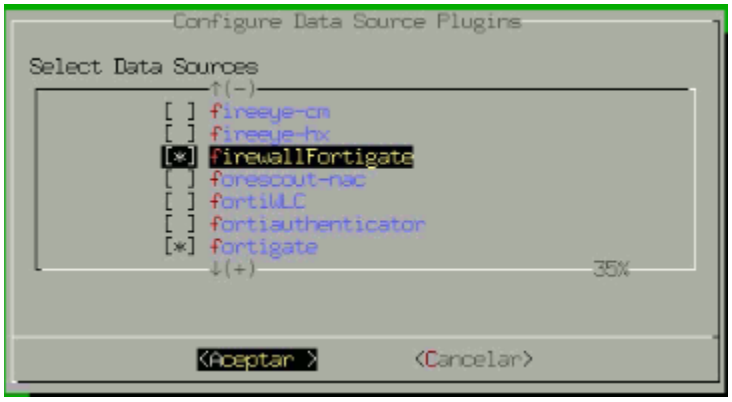


Figura 31. Activación del plugin SQL del Firewall.

Por último, verificamos la lectura de los logs, por parte del plugin creado, como se aprecia en las siguientes figuras:

Figura 32. Lectura general de los eventos.

DATE	SIGNATURE	SOURCE	DESTINATION	SENSOR	RISK
2019-03-08 00:02:10	Fortigate: Traffic Accept End Local	alienvault	Firewall-Fortinet	alienvault	0
2019-03-08 00:02:10	Fortigate: Traffic Accept End Local	alienvault	Firewall-Fortinet	alienvault	0
2019-03-08 00:01:33	Fortigate: Traffic Accept End Local	alienvault	Firewall-Fortinet	alienvault	0

Figura 33. Lectura en detalle de los eventos.

10.3.6. CUADROS DE MANDO DE OSSIM

Después de las configuraciones pertinentes en los distintos dispositivos y redes asociados al servidor OSSIM, se recolectan y extraen los logs, eventos y servicios encontrados mediante los escaneos constantes que realiza el servidor, para identificar toda información importante de interés del administrador de red. Los cuadros de mandos se encargan de hacer este proceso, le indican al administrador mediante la interfaz web, de todas las variables y datos importantes para la correcta gestión de la red.

Los cuadros de mando de mayor interés dentro del ámbito de este objetivo, son: 1) Seguridad; 2) Tickets; 3) Vulnerabilidades. Dentro del primer tipo, se puedieron observar los datos relacionados con seguridad, tales como el top 5 de alarmas y eventos producidos e identificados, los dispositivos con más registros de eventos, y la secuencia cronológica de los eventos de seguridad.

Figura 34. Cuadros de mando de seguridad.

En los cuadros de mandos de tickets, se observó toda la información pertinente con los tickets generados en los dispositivos. Dentro de los datos mostrados se pudo saber gráficamente, la cantidad y el tipo de los mismos atendidos por mes y el tiempo promedio empleado, el número por clases y el tipo que se encuentran abiertos, y el estado general de ellos.

Figura 35. Cuadros de mandos de tickets generados.

En el tercer tipo, se mostró toda la información concerniente con las vulnerabilidades que se presentan en el servidor, reportadas por los dispositivos y servicios anexos al mismo. Se ilustraron informes estadísticos que presentaron los equipos y las redes que más reportan vulnerabilidades. Del mismo modo, también se mostraron los resultados de los escaneos de vulnerabilidades programados.

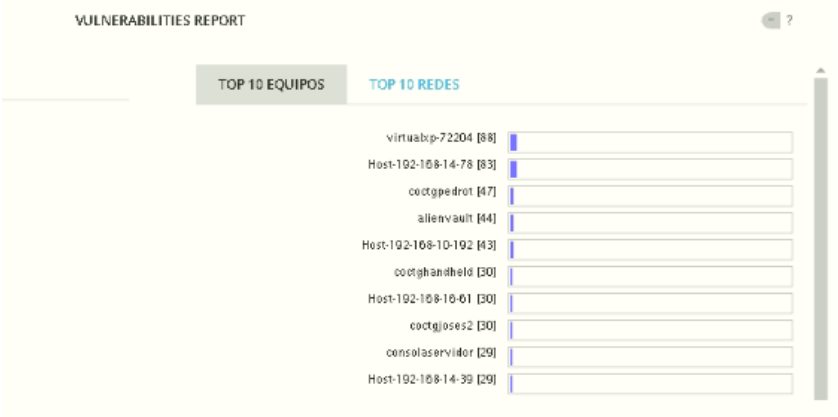


Figura 36. Cuadros de mando de vulnerabilidades detectadas.

10.3.7. CORRELACIÓN DE EVENTOS

El proceso de correlación de eventos es un mecanismo aplicado de forma automática por parte del servidor OSSIM, basándose en la sensibilidad, fiabilidad, escalabilidad, y visibilidad que tiene cada detector que provee el servidor para la detección de las anomalías. El proceso de correlación, se basa en el establecimiento de directivas integradas agrupadas a una categoría, o nuevas creadas por el administrador. Las directivas son el medio de recopilación y unión de patrones de ataques y amenazas, para la creación de alertas de seguridad en OSSIM.

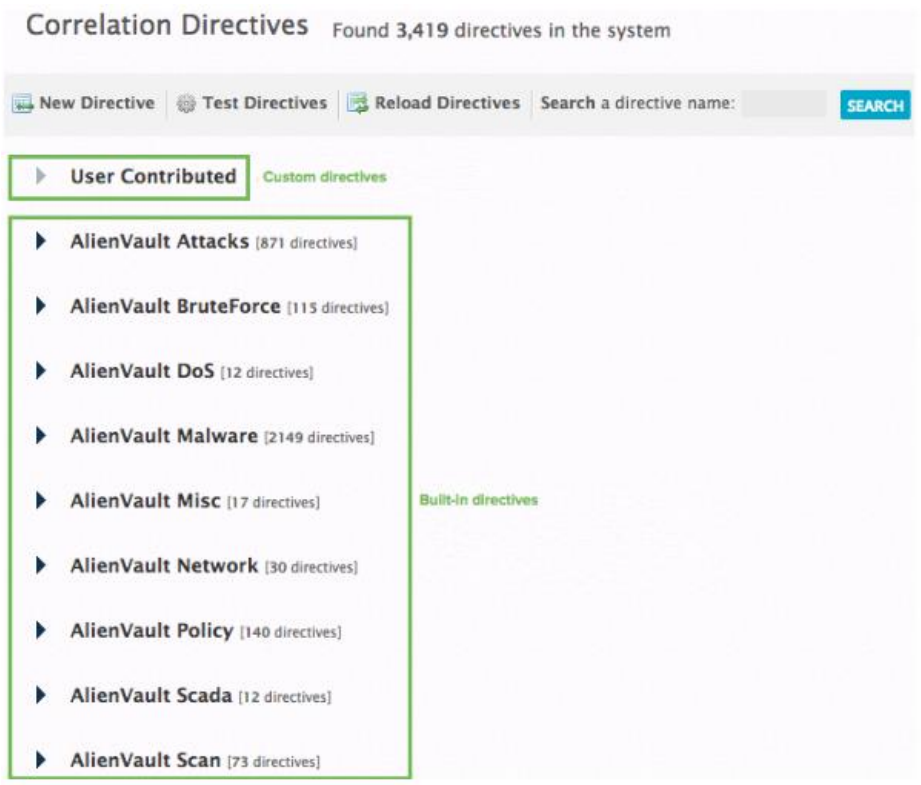


Figura 37. Directivas de correlación.

Dentro de la identificación del evento generado por la correlación, se obtienen los datos del dispositivo origen y del destinatario, la prioridad del mismo, la clasificación del riesgo, la fecha de detección, el evento que originó la detección y el tipo de dispositivo, la categoría y subcategoría en la que se clasificó el evento. A continuación, mostramos los eventos que el servidor OSSIM encontró mediante su sistema de correlación, después de la configuración de los dispositivos del alcance.

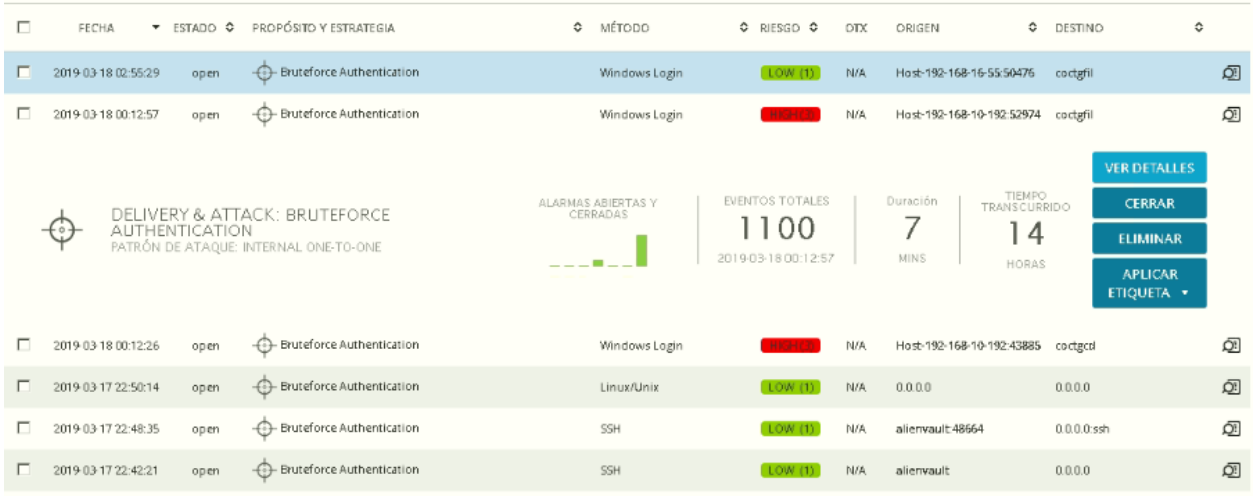


Figura 38. Eventos de seguridad encontrados mediante la correlación de eventos.

Dentro de las configuraciones realizadas en los equipos, la correlación de eventos logró detectar patrones de ataques relacionados que conforman eventos, concernientes en su mayoría con la directiva de "*Brutherforce Authentication"*. Lo anterior indica que este mecanismo de detección de eventos funciona correctamente y otorga una capa más de seguridad para la gestión de la red.

Al seleccionar unos de los eventos listados, se pudo apreciar la cantidad de eventos aislados estudiados para dar origen al evento, el patrón de ataque utilizado, el tiempo transcurrido para la identificación, y el riesgo. Con esta información suministrada por OSSIM, el administrador logró identificar las medidas necesarias para contrarrestar el ataque.

10.3.8. ALARMAS

El proceso de creación de las alarmas consiste en la utilización de directivas para la identificación y agrupamiento de los eventos y logs a tipos en específicos. El servidor OSSIM trae incorporadas directivas prestablecidas, que permiten la identificación de los eventos desde los distintos dispositivos.

Los tipos o propósitos de directivas que se encuentran por defecto, y las cuales pueden ser observadas en la ruta *"Configuración/ Información sobre amenazas/ Directivas"*, son:

1. **AlienVault Attacks**: Son las directivas que sirven para detectar diversos ataques contra servicios y aplicaciones vulnerables.
2. **AlienVault BruteForce:** Utilizadas para detectar ataques de fuerza bruta en servicios que requieren autenticación.
3. **AlienVault DoS:** Detectan ataques de denegación de servicio (DoS) en diferentes aplicaciones y servicios.
4. **AlienVault Malware:** Directivas para identificar malware.
5. **AlienVault Misc:** Directivas para detectar actividades que no entran en ninguna otra categoría.
6. **AlienVault Network:** Empleadas para detectar anomalías y ataques relacionados con la red.
7. **AlienVault Policy:** Directivas para detectar violaciones a las políticas.

8. **AlienVault Scada:** Detectan ataques en sistemas de control de supervisión industrial y adquisición de datos (SCADA).
9. **AlienVault Scan:** Directivas para detectar actividades de escaneo.

La empresa BIOFILM S.A. para la producción y realización de los deberes, cuenta con múltiples sistemas y servicios que ameritan autorización para su utilización. Debido a esto, existen demasiados registros de ataques de fuerza bruta sobre estos servicios, indicando que tratan de ser accedidos sin contar con las credenciales necesarias. Por lo anterior, la mayoría de los registros captados por el servidor OSSIM, provenientes de los medios mencionados, corresponden con el tipo *Bruteforce* mediante la directiva específica *Bruterforce Authentication*, como se aprecia a continuación:

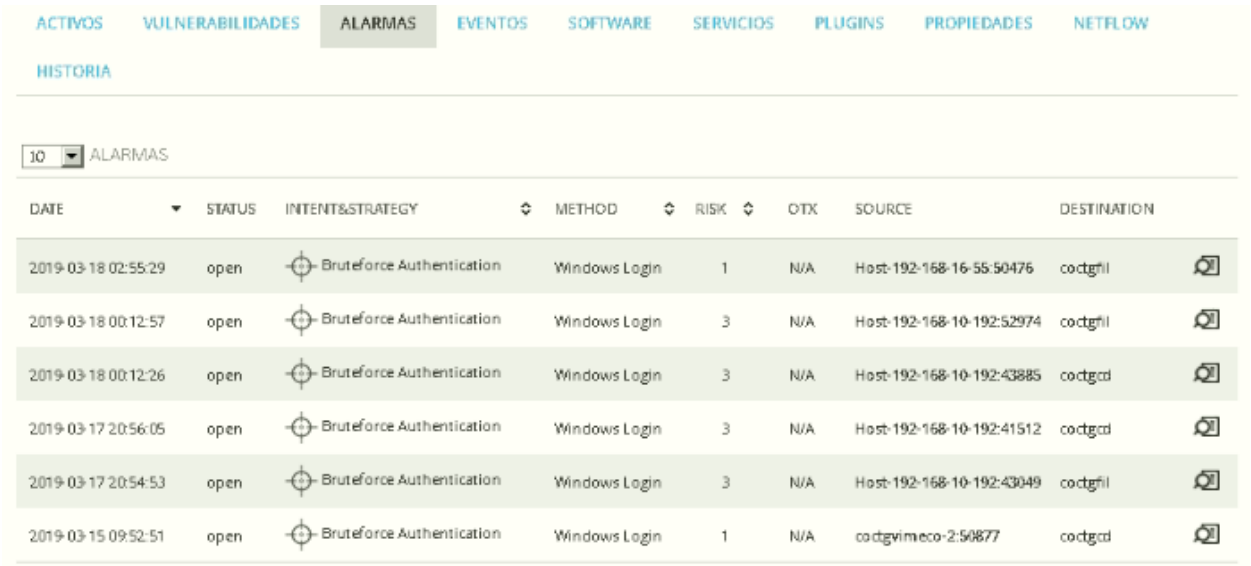


Figura 39. Alarmas identificadas por el tipo de directiva Bruterforce, en la red principal.

Del mismo modo, también se lograron identificar alarmas mediante otros tipos de directivas, como *AlienVault Attacks y Alien Malware*, respectivamente ilustradas.

Figura 40. Alarmas identificadas por el tipo de directiva AlienVault Attacks, en la red principal.

Figura 41. Alarmas identificadas por el tipo de directiva Alien Malware, en la red principal.

10.3.9. TICKETS

Como método de seguimiento a las alarmas registradas por los distintos dispositivos y servicios anexados a la red, OSSIM establece tickets que contienen información sobre las alarmas detectadas o cualquier otro problema administrado en un flujo de trabajo. Cuando se trata de alarmas y eventos, la mejor práctica es realizar un seguimiento del progreso y los conocimientos sobre el problema mediante la creación de un ticket. OSSIM no solo utiliza los tickets para ayudar en investigaciones de problemas presentados, también crea un registro de auditoría para rastrear lo que se observó, las acciones que se tomaron y el progreso del problema.

OSSIM además de poseer su propio sistema de gestión de tickets, también tiene la capacidad de obtener información de los tickets de sistemas de tickets externos, mostrarlos en la interfaz web, y hacer el proceso de diligenciamiento y acciones pertinentes sobre cada uno de ellos.

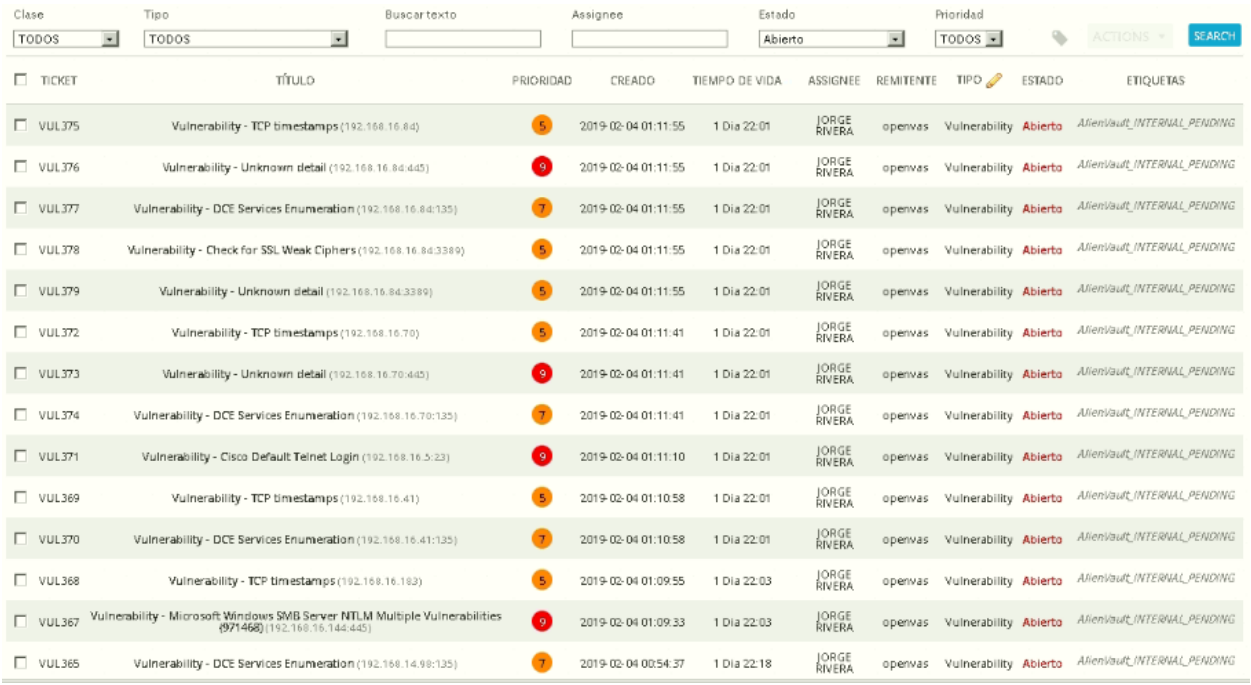


Figura 42. Tickets generados desde los equipos y servicios de la empresa.

Los tickets mostrados en la figura anterior, resultaron de la adición de la red principal al inventario de equipos, debido a que esta red presenta un sistema de tickets del cual OSSIM recopiló toda la información necesaria para la gestión en la interfaz web.

10.3.10. CREACIÓN DE INFORMES

AlienVault OSSIM incluye múltiples informes predefinidos para mantener informado sobre los activos, el nivel de cumplimiento, las alarmas y los eventos de seguridad que se están presentando en la empresa. Para obtener los informes, se debe acceder mediante la interfaz web, a la dirección *"Informes"*, donde están las múltiples opciones relacionadas con las categorías de informes, con las cuales se pueden generar los informes.

Los informes necesarios generados para comprobar el estado en el que se encuentran los dispositivos y redes anexadas al servidor, fueron los siguientes:

1. **Alarmas:** Este informe permitió generar un documento con las principales alarmas, los atacantes, los hosts atacados y los puertos de destino, ayudando a establecer la forma en que estaban representadas las alarmas a nivel de equipos y a nivel de redes. Para este informe se tuvo en cuenta un rango de tiempo de un mes, tiempo suficiente para analizar los datos obtenidos.

Figura 43. Creación del informe de alarmas.

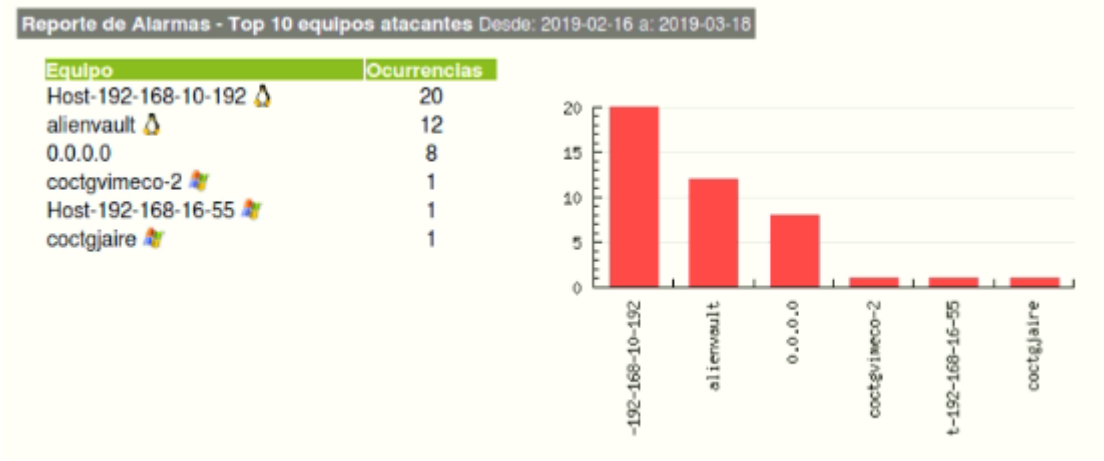


Figura 44. Informe de alarmas. Top 10 de equipos atacantes.

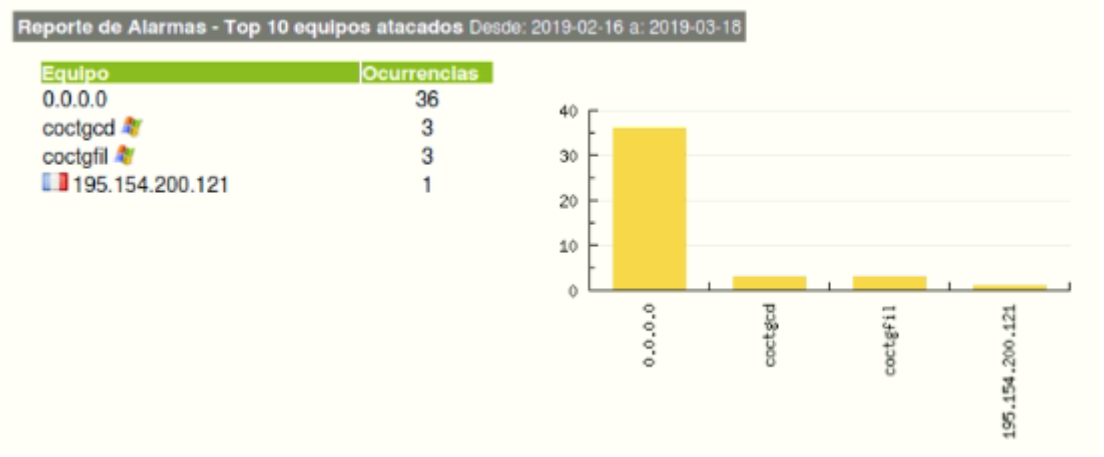


Figura 45. Informe de alarmas. Top 10 de equipos atacados.

De esta forma, se obtuvieron los equipos donde mayor énfasis en la seguridad se debió realizar para preservar la red y los demás equipos.

2. **Detalles de activos:** Para la realización de este informe, se utilizó la red principal (192.168.10.0), sobre la cual se mostró la información concerniente con los activos relacionados con la misma y sus propiedades, las vulnerabilidades, los eventos, las alarmas y los registros sin procesar que la red.

Figura 46. Creación de informe de los detalles de activos.

Figura 47. Informe de los detalles de la red principal.

Se pudo observar todos los datos estadísticos que arrojó la misma, donde se tuvieron que atender las vulnerabilidades y las alarmas que se presentaron, debido a que proponía un alto riesgo para la seguridad misma de la red.

3. **Conformidad:** Las regulaciones sobre el cumplimiento de la ISO 27001 son de importancia para constatar la correcta ejecución de las tareas en la red, por lo que este informe fue de gran utilidad para verificar que los eventos, alarmas y activos, estén orientados a los requisitos de cumplimiento de dicha norma.

Figura 48. Creación de informe de conformidad ISO 27001.

4. **Eventos SIEM:** Junto con el informe de las alarmas, el informe de detalles de los eventos SIEM proporcionó una vista general del estado de los equipos y redes anexados y analizados en el servidor OSSIM, debido a que informó sobre los equipos que más reciben eventos, los que más generan, los puertos utilizados en los ataques, los detalles de los eventos y sus agrupaciones por el tipo. De esta forma se pudieron analizar los datos para encontrar la forma correcta de gestión de los mismos.

Figura 49. Creación de informe de eventos SIEM.

Además de los anteriores informes, la interfaz web permite la creación de otros tipos de informes que pueden ser utilizados conforme a la intención que se tenga.

10.4. CREAR UN APLICATIVO MÓVIL PARA LA DIVISIÓN DE RECURSOS HUMANOS QUE PERMITA POTENCIALIZAR LA DIVULGACIÓN, APRENDIZAJE Y CONCIENTIZACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA EMPRESA.

Bajo el ciclo de desarrollo de la metodología **Mobile–D,** se definieron las actividades correspondientes en cada una de las fases del mismo, como se demuestra a continuación en los siguientes ítems.

10.4.1. LEVANTAMIENTO DE INFORMACIÓN

Como método de recolección de la información necesaria para el correcto desarrollo del aplicativo móvil, y respetando la fase del ciclo de vida correspondiente, se realizó un resumen a manera de estado del arte, con la temática del objetivo en cuestión, es decir, sobre la tecnología Android, el desarrollo de aplicativos para la misma y la utilización de la metodología Mobile-D en otros proyectos. Dicho estado del arte estuvo definido en tres ámbitos: internacional, nacional y local, a lo largo de un lapso de tiempo de 5 años atrás hasta la actualidad.

Para la creación del estado del arte, se tuvieron en cuenta aquellos escritos que, a razón de los investigadores de este proyecto, tienen mayor afinidad, importancia y trascendencia para el desarrollo de este proyecto.

10.4.1.1. PANORAMA INTERNACIONAL

En el año 2013, se desarrolló un trabajo por medio del cual se buscaba crear un aplicativo Android que permitiera motivar y aprender a través de una metodología lúdica, constructivista y social, para ello se empleó un método de aprendizaje llamado Serious Game, todo esto iría encaminado a buscar un enfoque pedagógico innovador y más eficiente (Lozano Ortiz, Vicent Safont, & Luque Hernández, 2013).

En el año 2016, en la universidad Técnica de Cotopaxi se llevó a cabo una tesis de grado en la que se desarrolló un aplicativo móvil para la geolocalización de centros de atención médica, bajo la implementación de la metodología Mobile-D. Dentro de este trabajo, se muestran cada una de las actividades/tareas que se deben desarrollar en cada una de las fases que ofrece la metodología, con la finalidad de cumplir con los objetivos propuestos (Ayala Guanina & Segovia Bedón, 2016).

En el año siguiente, se realiza un artículo que describe una experiencia educativa usando Realidad Aumentada (RA[13]) en dispositivos móviles para el aprendizaje de conceptos de diseño urbano en estudiantes de Arquitectura. Para la enseñanza, se creó una estrategia pedagógica práctica que permitía el aprendizaje en conjunto, basándose en parámetros del entorno y aprendizaje colaborativo. Al final de la aplicación de enseñanza, los resultados obtenidos indican que la utilización de herramientas tecnológicas para la enseñanza, potencializa la motivación para el aprendizaje. Este artículo es importante recalcarlo, por ser una herramienta de ayuda para el aprendizaje de temáticas concretas, lo que le otorga la potestad de servir como ayuda en el desarrollo del proyecto en curso, por el tipo de metodología empleada (Fonseca Escudero, Redondo Domínguez, Sánchez Riera, & Navarro Delgado, 2017).

10.4.1.2. PANORAMA NACIONAL

En el año 2013, en la Universidad Distrital Francisco José de Caldas, fue realizado un artículo en el cual se otorga una breve descripción de Android como tecnología, sus características y su arquitectura, así como el software necesario para el desarrollo de aplicaciones sobre la misma.

[13] RA: Es el resultado de la combinación de del mundo real con el virtual, mediante un proceso informático.

De igual manera, se expresan las ventajas que posee el desarrollo de aplicaciones sobre la tecnología Android, de gran auge y visión sobre el mercado moderno. La información contenida en dicho artículo es complementada con una aplicación para realizar algunas operaciones matemáticas (Vanegas, 2013).

Posterior a ese año, en el 2014 se hizo un escrito como trabajo de grado sobre la valoración del framework[14] de evaluación de seguridad de Android (ASEF). Ésta es una plataforma de Android, para evaluar automáticamente las aplicaciones instaladas en un dispositivo, recopilar sus datos de comportamiento, analizar su patrón de ejecución y, al mismo tiempo, proporcionar una interfaz para facilitar la gran mayoría de las pruebas de seguridad. En esta tesis, recalcan la importancia que tiene esta plataforma para ser escogida como punto de partida para el monitoreo de aplicativos para control de malware en teléfonos inteligentes con sistema operativo Android, por ser una herramienta poderosa, innovadora y de gran potencial. Por lo cual, ofrecen mecanismos para verificar que dicho framework tenga el nivel de avance y confiabilidad, buscando determinar su validez como base para la gestión de aplicativos y movimientos realizados bajo la plataforma Android (Fernando & Amaya, 2014).

En el 2016, se publicó un artículo en la revista Scientific Information System Network sobre un framework para análisis de software malicioso en Android. En él, informan sobre la cantidad de información sensible que se utiliza en estas tecnologías, lo que genera un interés particular de los cibercriminales para el desarrollo de técnicas y herramientas que permitan la adquisición de la información o alteren el buen funcionamiento del dispositivo, e informan sobre los múltiples esfuerzos realizados por entidades para afrontar esta problemática, pero cada una de las soluciones existentes hacen alusión a desarrollos de necesidades específicas, lo que indica que las soluciones están directamente enfocadas a la plataforma utilizada en un dispositivo en concreto y no sirven como método de generalización para todos los dispositivos Android. En este artículo, proponen un framework de análisis estático y aprendizaje de máquina para clasificación de software benigno y malicioso en Android, el cuál puede ser utilizado de forma general en cualquiera de los dispositivos con esta plataforma (Camilo & López, 2016).

[14] Framework: Es una estructura software compuesta de componentes personalizables e intercambiables, para el desarrollo de una aplicación.

En ese mismo año se realizó un trabajo orientado a mejorar la seguridad, análisis y verificación en Android a través de un sistema llamado SafeCandy, desarrollado en la facultad de ingeniería de la Universidad Icesi, en conjunto con la empresa Password Consulting Services, dicho sistema tendría como principal característica el trabajar con una arquitectura cliente – servidor, y el hacer uso de un análisis estático y dinámico de los ambientes arquitecturales (Londoño, Urcuqui, Fuentes Amaya, Gómez, & Navarro Cadavid, 2015).

10.4.1.3. PANORAMA LOCAL

En el año 2013 se realizó un trabajo de grado en la Universidad de San Buenaventura, por medio del cual se buscaba realizar un análisis forense al sistema Android afectado por un malware en específico, para este proyecto se tomaría fakelookout como software malintencionado, buscando a su vez las soluciones pertinentes a los problemas presentados por dicho malware (Morelo Madariaga & Betancur López, n.d.).

Más tarde, en el 2015 en la Universidad de Cartagena se llevaría a cabo un trabajo de grado que iría encaminado a la construcción de un aplicativo cliente - servidor para la detección de vulnerabilidades de red en Smartphone Android utilizando una herramienta de escaneo, la importancia de este estudio se centraría en el hecho de contribuir a proteger la información en uno de los sistemas operativos mundialmente más reconocidos, además de agregar características de adaptabilidad y fácil uso (Payares Guzmán & Ortega García, 2015).

En el 2017 en la misma Universidad de Cartagena, se trabajaría sobre el desarrollo de una aplicación móvil que serviría como herramienta educativa para la guía diagnostica de desórdenes potencialmente malignos y la prevención del cáncer oral, para ello se haría uso en gran medida de las nuevas tecnologías, pues esto considerando el acceso de gran parte de las personas a dispositivos inteligentes, convirtiéndose esto en una herramienta de aprendizaje debido a su portabilidad y acceso eficiente a la información (Rincón Flórez & Pájaro Arnedo, 2017).

10.4.1.4. CONCLUSIÓN DEL ESTADO DEL ARTE

En los escritos estudiados e investigados, no existió la creación de un aplicativo móvil para el aprendizaje de políticas de seguridad, pero sí se halló material que sirve como base para la creación de un aplicativo móvil útil para la enseñanza/aprendizaje de las políticas de seguridad que la empresa BIOFILM S.A. pone a disposición de sus empleados, debido a que algunos escritos están orientados a aplicativos móviles para la enseñanza de temas en específico, de los cuales se pueden tomar los procedimientos utilizados para los aspectos tácticos y técnicos en la parte visual y en la ubicación estratégica del contenido, con tal de convertir la APP desarrollada en este proyecto, en una herramienta del gusto de los usuarios (empleados de la empresa) y estos le otorguen el uso correspondiente. Del mismo modo, se encontró un proyecto de grado para la creación de un aplicativo móvil basado en la metodología Mobile-D, y por ser la misma que los investigadores de este proyecto implementan para el desarrollo de la APP, servirá como guía para el cumplimiento de las tareas y actividad pertinentes en cada una de las fases y etapas que plantea el ciclo de desarrollo de esta metodología.

10.4.2. FASE DE EXPLORACIÓN

Como corresponde en esta fase, se definió el alcance y la razón de este proyecto, por lo cual, con la realización del mismo, se pretende desarrollar un aplicativo móvil a manera de juego de preguntas para la potencialización del conocimiento de los trabajadores de la empresa BIOFILM S.A., mediante preguntas sobre la temática de las políticas de seguridad de la información que maneja la misma. De este modo, los trabajadores pueden contar con una herramienta de apoyo para el aprendizaje/evaluación fuera de la planta, de las políticas que la empresa dispone para promover la integridad empresarial y la continuidad del negocio. Mediante la utilización de tecnologías adecuadas para el desarrollo móvil, se logró desarrollar la herramienta de la cuál dispondrá todo el personal de la compañía.

10.4.3. FASE DE INICIALIZACIÓN

Luego de haber realizado el levantamiento de información pertinente, el equipo de trabajo conformado por los investigadores de este proyecto, empezó a interactuar con el personal de Telecomunicaciones y de RRHH de la empresa para establecer los requisitos de la aplicación a partir de los requerimientos planteados por ellos, y se identificaron todos los recursos necesarios para el desarrollo. Mediante la especificación de los requisitos funcionales y no funcionales, se detectaron las características que visionaron el proyecto y crearon un marco que sirvió como base para la inicialización del proyecto. La interacción se realizó mediante una reunión de levantamiento de requerimientos, como se puede verificar en el *anexo 4 y 5*. Estos anexos, son documentos de levantamiento y establecimiento de requerimientos, elaborado por los investigadores de este proyecto.

10.4.3.1. REQUISITOS FUNCIONALES

Los requisitos funcionales son las acciones características que realiza el aplicativo móvil al momento de ser usado por los empleados de BIOFILM S.A.

De manera general, se describe el proceso que realiza el aplicativo móvil, y con el cuál se establecieron los requisitos. La APP cuenta con un control de acceso (login), que permite identificar al usuario empleado que accede al sistema. Una vez identificado el usuario, se le muestran las campañas activas en las cuales él puede competir. Una campaña es un tiempo determinado por el administrador, en el que se hacen preguntas sobre un grupo o varios grupos de preguntas que el administrador relaciona con tal campaña; las preguntas pertenecientes a cada grupo de preguntas son del tipo falso y verdadero, o de selección múltiple con única respuesta, todas relacionadas con una temática en específica.

Durante la campaña, cada empleado puede hacer un número indeterminado de intentos. Un intento está controlado por un tiempo y/o un número de preguntas fijado por el administrador; lo que primero agote el usuario. Con los intentos realizados en una campaña, se establece una tabla general con los puntajes de cada jugador. En la realización de esta tabla, se tiene en cuenta de forma descendente, los jugadores que hayan alcanzado la mayor sumatoria de puntaje en la

menor sumatoria de tiempo y en el mayor número de intentos. Al finalizar la campaña, se seleccionan a los jugadores de las primeras posiciones de la tabla como ganadores, según lo estipule el administrador.

A continuación, se muestran los requisitos funcionales hallados a partir de lo anterior:

ID REQUISITO	NOMBRE DEL REQUISITO	DESCRIPCIÓN
RF 1	Jugar	El aplicativo móvil será a manera de juego de preguntas, en el cual se pondrán en práctica/evaluación los conocimientos adquiridos previamente por cada empleado.
RF 2	Login	El empleado ingresará al juego mediante un usuario y una contraseña que la empresa previamente le dispuso a cada empleado para su uso.
RF 3	Puntaje individual y general	El empleado como usuario del juego, debe poder saber en cualquier momento, el puntaje que alcance cada vez que juegue (llamado intentos) y el puntaje general de todos los empleados de la planta.
RF4	Administrador	El juego debe poseer una forma para ser alimentado, por medio de una persona designada que hará las veces de administradora del aplicativo. Esta persona debe poder crear las campañas, las preguntas y la designación de la cantidad de ganadores por cada campaña. El método para administrar, no necesariamente debe ser móvil.
RF5	Campaña de juego	El juego generará campañas de juego controladas por un tiempo, que determinará el administrador del juego. Dentro de esta campaña se guardarán todos los puntajes alcanzados y se escogerá el número de ganadores designados. Estas campañas se deben poder realizar por dominios o divisiones en específico, grupo de las mismas o para toda la empresa en general.

RF6	Banco de preguntas	Las preguntas que se realizarán en el juego, serán tomadas de un banco de preguntas almacenadas en la BD. La utilización de las preguntas se hará de manera aleatoria. Estas preguntas son del tipo de selección múltiple con única respuesta y de falso-verdadero.
RF7	Grupos de preguntas	Todas y cada una de las preguntas asociadas al juego, deben estar en categorías o grupos escogidos por el administrador. De este modo, poder hacer campañas con grupos de preguntas específicas.
RF8	Conexión con la base de datos (BD)	El aplicativo móvil debe ser capaz de conectarse con la BD para verificar los datos correspondientes a cada empleado. También para la consulta de las preguntas y sus respuestas. De igual modo, para el almacenamiento de los puntajes logrados por cada empleado al momento de jugar.

Tabla 8. Requisitos funcionales del aplicativo móvil.

10.4.3.2. REQUISITOS NO FUNCIONALES

Los requisitos no funcionales definidos para este proyecto, surgieron también a partir de los requerimientos plasmados en el a*nexo 4 y 5*, y estos ayudan al desarrollo de los requisitos funcionales definidos anteriormente y a su puesta en marcha, debido a que son características de funcionamiento que relacionan cada una de las acciones que el usuario del aplicativo realiza.

Los requisitos no funcionales que proporciona la aplicación móvil, están definidos en la siguiente tabla:

ID REQUISITO	NOMBRE DEL REQUISITO	DESCRIPCIÓN
RNF1	Colores del juego	Los colores de la vista del juego, son los colores Institucionales de BIOFILM S.A (Blanco y Rojo).

Tabla 9. Requisitos no funcionales del aplicativo móvil.

10.4.4. FASE DE PRODUCCIÓN

Como primera tarea de esta fase, se prosiguió a determinar mediante una investigación basada en los requerimientos previamente definidos, las herramientas y tecnologías adecuadas que permitieron desarrollar el aplicativo móvil. Una de las tecnologías que se decidió implementar fue la del desarrollo móvil a partir de un framework de desarrollo como IONIC[15], debido a que es una herramienta flexible y robusta para la creación de aplicativos móviles. Este framework permitió que la integración con el gestor de bases de datos mediante una API Rest[16], fuese dinámica. Como gestor de bases de datos se escogió MySQL[17] y la API desarrollada se creó con Node.js[18]. Estos dos últimos elementos, se encuentran alojados en un servidor de Microsoft Azure[19], que permite la producción y disponibilidad de la información alojada y suministrada.

Luego de haber definido las tecnologías que se utilizaron en el desarrollo del proyecto, se creó la implementación del sistema a partir de la generación de los modelos y diagramas basados en UML[20], normalmente llamado modelado, quienes guiaron el proyecto en su desarrollo. Este modelado se realizó bajo tres parámetros que permitieron segmentar la razón del proyecto: 1) Modelo de negocio; 2) Modelo de diseño; 3) Modelo de implementación.

Como primer procedimiento, para analizar el modelo de negocio se emplearon el modelo de dominio y el diagrama de casos de uso del mundo real, quienes reflejan la esencia del problema de la empresa BIOFILM S.A., en el mundo real. Con ellos se analizó la problemática aislada completamente de términos técnicos de programación, es decir, en lenguaje natural.

[15] IONIC: Es una herramienta gratuita para el desarrollo de aplicaciones híbridas basadas en HTML5, CSS y JS.
[16] API REST: Es una interfaz entre sistemas que utiliza directamente HTTP para obtener datos o indicar la ejecución de operaciones sobre los datos, en cualquier formato (XML, JSON, etc.).
[17] MySQL: Es un sistema de gestión de bases relacional.
[18] Node.js: Es un entorno JavaScript del lado del servidor, basado en eventos.
[19] Microsoft Azure: es una nube pública de pago por uso que te permite compilar, implementar y administrar rápidamente aplicaciones en una red global de datacenters de Microsoft.
[20] UML: El Lenguaje Unificado de Modelado, es un estándar para el diseño y la implementación de sistemas de software complejos, mediante diagramas. Los diagramas UML describen los límites, la estructura y el comportamiento del sistema y los objetos que contiene.

En el modelo de dominio *(figura 30)*, se representó la forma como se realizan los procesos en la empresa en el mundo real. Cada clase presente, identifica un ente o una acción real de la empresa.

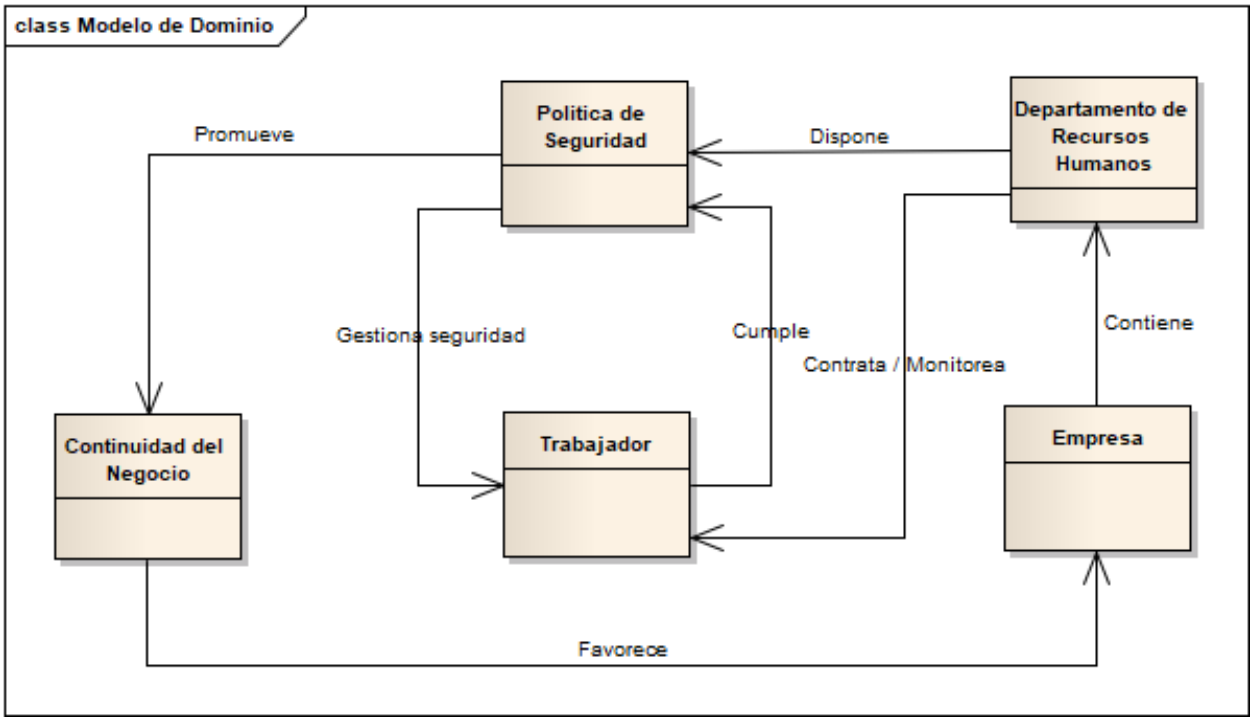


Figura 50. Modelo de dominio del aplicativo móvil. (Creado por los Investigadores).

La determinación de las clases que componen este modelo, se realizó mediante el análisis de las funciones que se desarrollan dentro de la empresa, con relación a los deberes concernientes al marco de la seguridad de la información. Este marco establece que el empleado cuando ingresa a la empresa, con la firma del contrato asevera conocer las políticas de seguridad de la empresa y está dispuesto a cumplirlas para promover la continuidad del negocio y, a la vez, para gestionar su propia seguridad. Por su parte, la empresa contiene a la división de RRHH que contrata a los empleados y se encarga de disponer las políticas de seguridad y de ejercer un control sobre su cumplimiento. Bajo estos supuestos, se creó el modelo en cuestión.

Del mismo modo y basándose en lo anterior, se creó el diagrama de casos de uso del mundo real, el cual refleja los procesos, funciones y/o consecuencias (casos de uso) que se desarrollan en BIOFILM S.A. en cuestiones de políticas de seguridad y su cumplimiento por parte de los trabajadores. Los casos de uso se identificaron teniendo en cuenta el contexto del mundo real,

viendo las necesidades que tienen los empleados al momento de realizar sus labores dentro de la empresa, y la división de RRHH a la hora de ejercer control sobre dichas labores.

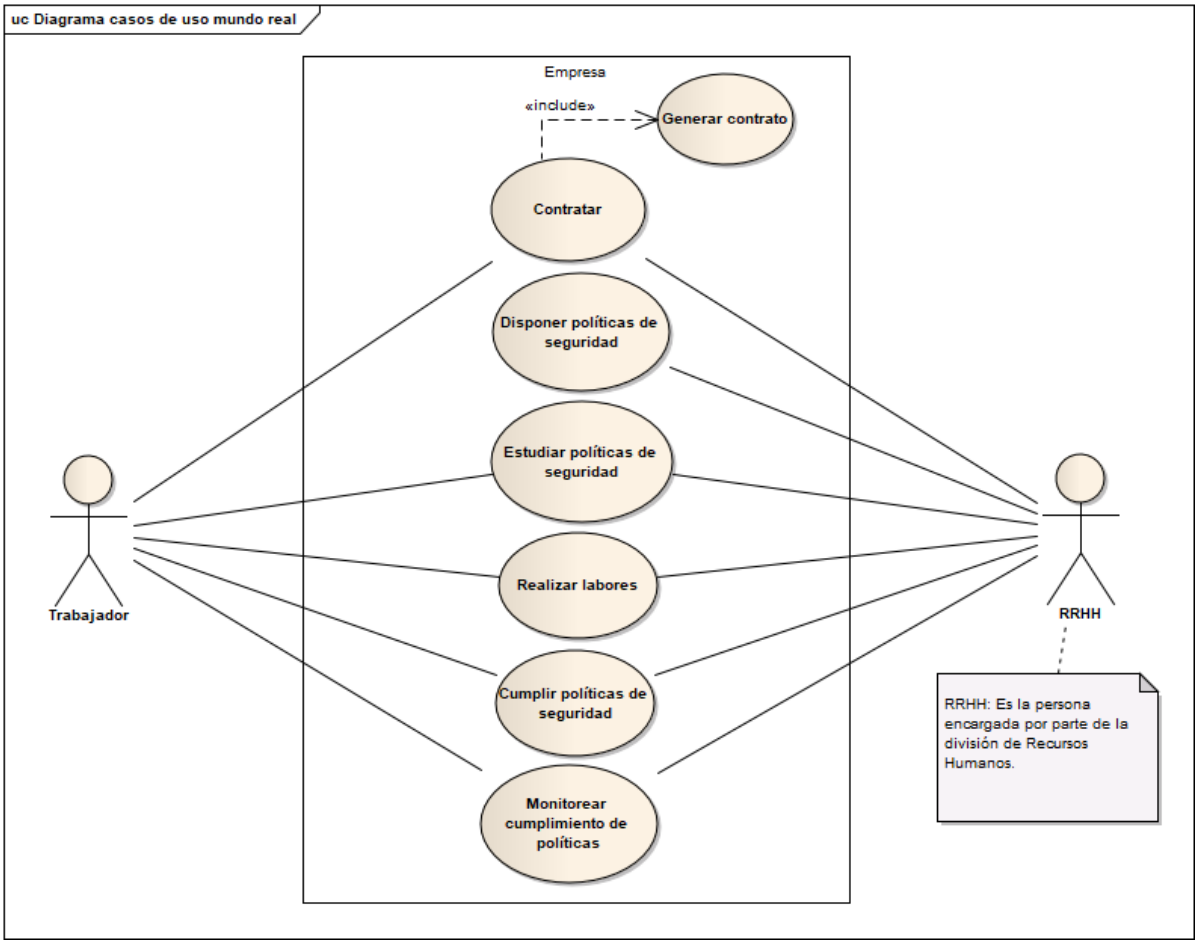


Figura 51. Diagrama de casos de uso del mundo real del aplicativo móvil. (Creado por los Investigadores).

En este diagrama se identificó al trabajador como actor, porque es el encargado de realizar las acciones dentro de la empresa. Los empleados de la división de RRHH conforman otro tipo de actor, debido a que, por ser trabajadores de la empresa, no están exentos del cumplimiento de las políticas, pero están en condición de ejercer control.

Como segundo procedimiento de la fase de producción, el análisis del modelo de diseño se desarrolló a partir del diagrama de componentes, diagrama de clases, diagrama general de casos de uso y diagrama de entidad relación.

En el diagrama de componentes, presente en la siguiente figura, se muestra la estructura básica de la solución a las necesidades de la empresa, representada en forma sistémica, y utilizando el patrón arquitectónico de capas. En él se pueden visualizar los componentes principales con los

que cuenta el sistema, agrupados en su capa correspondiente. Cada uno de los componentes contenidos en este diagrama, representan los paquetes y segmentaciones que tiene el aplicativo móvil.

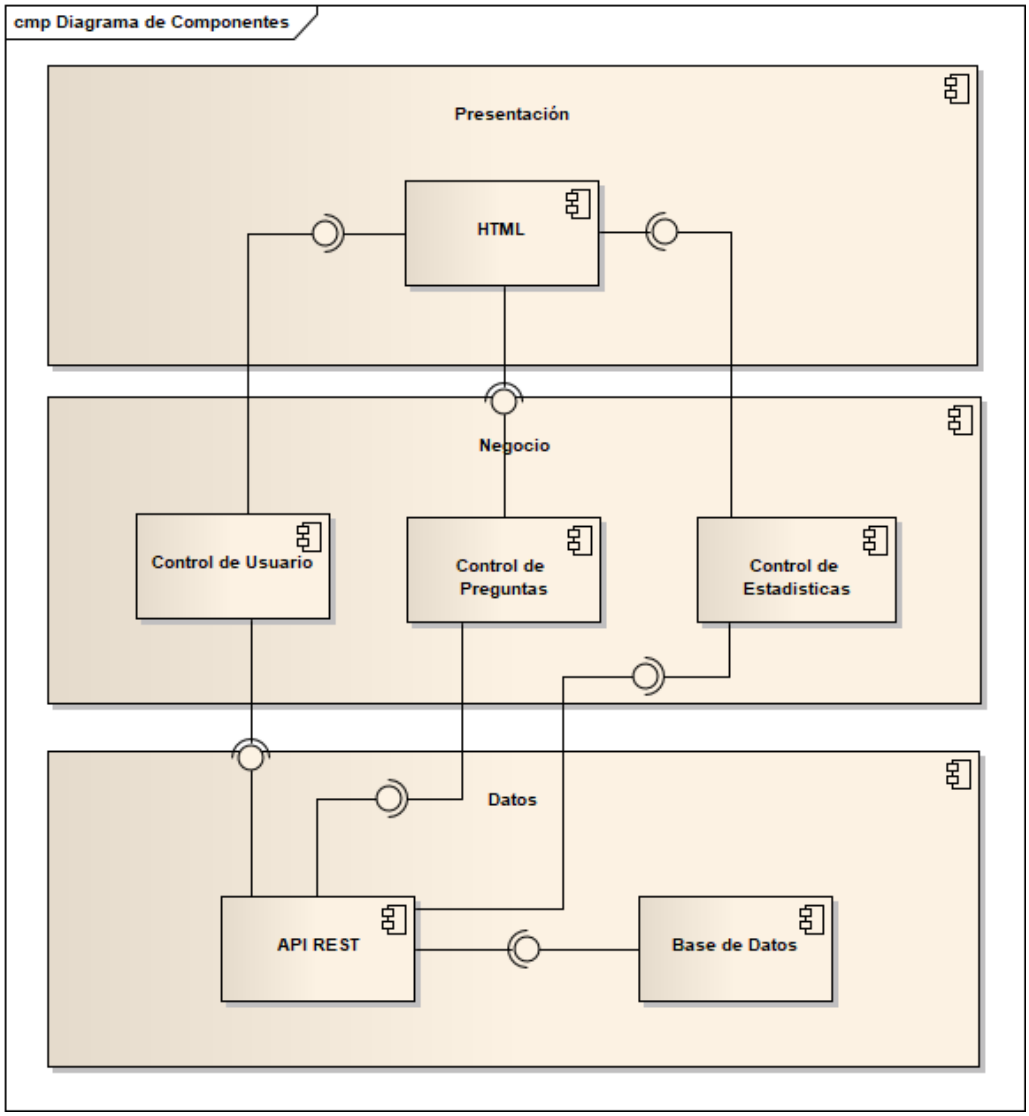


Figura 52. Diagrama de componentes del aplicativo móvil. (Creado por los Investigadores).

El patrón arquitectónico utilizado, ayudó a dividir la creación del aplicativo en capas esenciales, es decir, fraccionó la forma de desarrollo en características fundamentales. La capa de presentación otorga las características visuales al usuario para usar la aplicación, sin que éste tenga conocimiento de lo que sucede al interior. HTML[21] es el componente que dispone IONIC

[21] HTML: Es un lenguaje de programación que se utiliza para el desarrollo de páginas de Internet.

para la creación de las interfaces y vistas que el usuario de la aplicación utiliza. Las peticiones y acciones realizadas mediante estas vistas, son recogidas por la capa de negocio que se encarga de gestionar las peticiones, mediante la creación de un mecanismo de respuesta basado en los servicios de búsqueda de información en las bases de datos, ofrecidos por la API Rest quien se encuentra en la capa de datos.

Los componentes presentes en la capa de negocio, se desarrollaron a partir del conjunto de tecnologías que presenta IONIC para la creación de aplicativos móviles, como Angular[22] y CSS[23], redefinidos en formatos TypeScript[24], JavaScript[25] y SCSS o SASS[26]. La implementación de estas tecnologías se hizo con la finalidad de llevar el control sobre los usuarios, las estadísticas y las preguntas, es decir, atienden la lógica para el uso adecuado de la parte visual y de interacción del usuario al momento de utilizar la aplicación, y sobre la usabilidad de los componentes de la base de datos para el almacenamiento y recuperación de la información recopilada y producida.

Del mismo modo, el diagrama de clases se realizó utilizando el modelo arquitectónico de capas. Este diagrama, permite ver la estructura que tiene el aplicativo móvil a nivel de programación, y otorgó las relaciones existentes entre las capas implementadas en el patrón, por medio de las clases y entes inmersos en cada una de ellas. También encontramos como están organizadas las clases en cada una de las capas del patrón, las dependencias y las relaciones que hay entre ellas. Todo esto permitió crear las bases de diseño para la implementación del sistema.

Los componentes señalados en el diagrama de componentes, se describen en el diagrama de clases. En la capa de presentación se encuentra la parte visual de aplicativo que se define a partir del lenguaje y herramienta a utilizar, en este caso, IONIC basa el desarrollo de las vistas en HTML. En la capa de Negocio se estipula el mecanismo de respuesta a las peticiones realizadas por el usuario y le otorga la funcionalidad al sistema basándose en la información almacenada en la base de datos, quien es accedida mediante la API REST establecida en la capa de datos.

[22] Angular: Es un framework para desarrollo de aplicaciones web.
[23] CSS: Es un lenguaje de diseño gráfico para definir y crear la presentación de las aplicaciones hechas con base en lenguajes de marcado, como HTML.
[24] TypeScript: Es un lenguaje de programación de código abierto con herramientas de programación orientada a objetos.
[25] JavaScript: Es un lenguaje de programación que permite crear acciones en las páginas web.
[26] SCSS o SASS: Es una extensión avanzada de CSS.

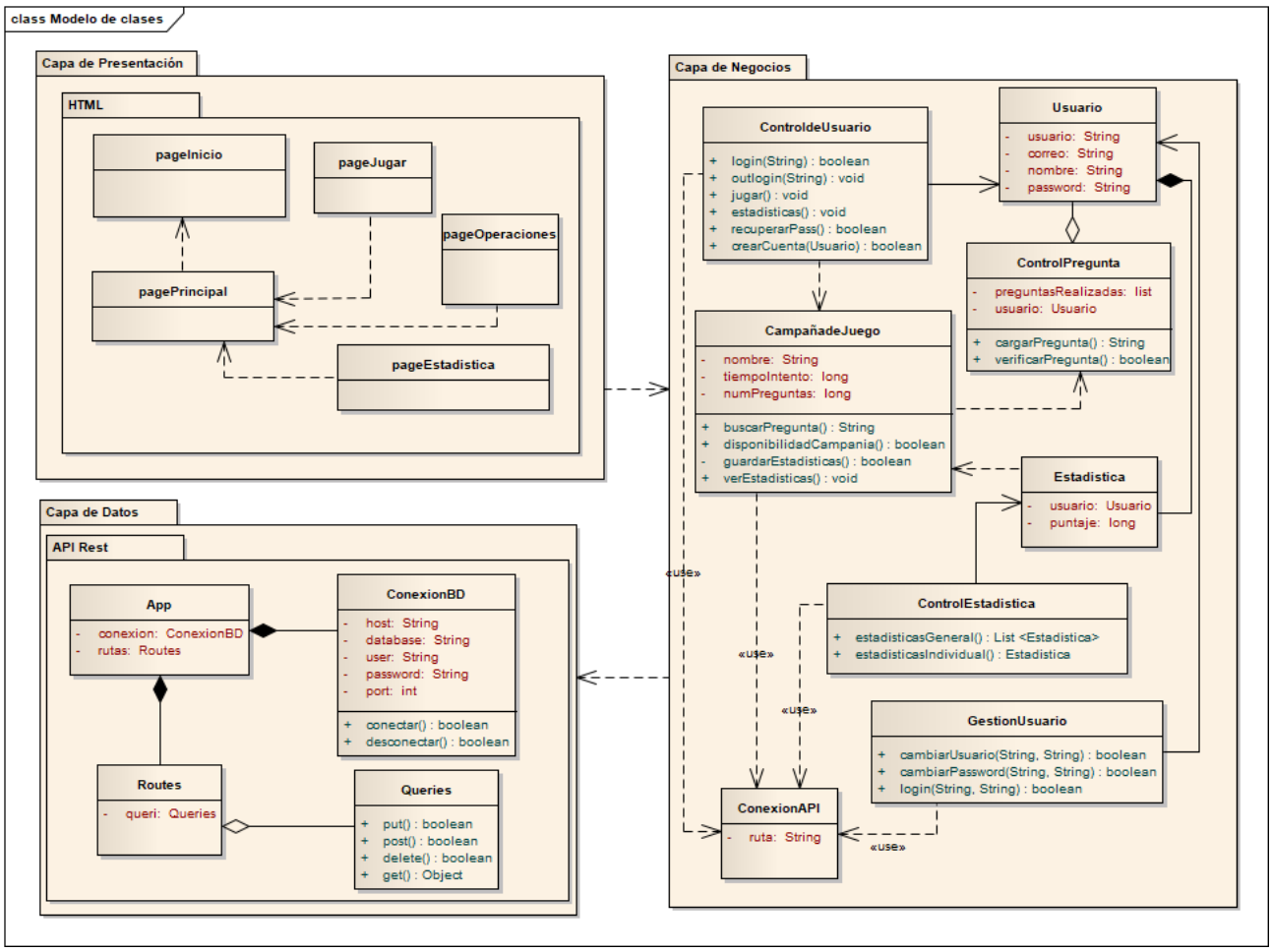


Figura 53. Diagrama de clases del aplicativo móvil. (Creado por los Investigadores).

En el diagrama general de casos de uso, se ilustran las operaciones que realiza el empleado al momento de utilizar el aplicativo. Cada uno de los casos de uso pertenece a un requisito funcional estipulado anteriormente. El actor relacionado con este diagrama, es el jugador, quien es el mismo empleado usuario.

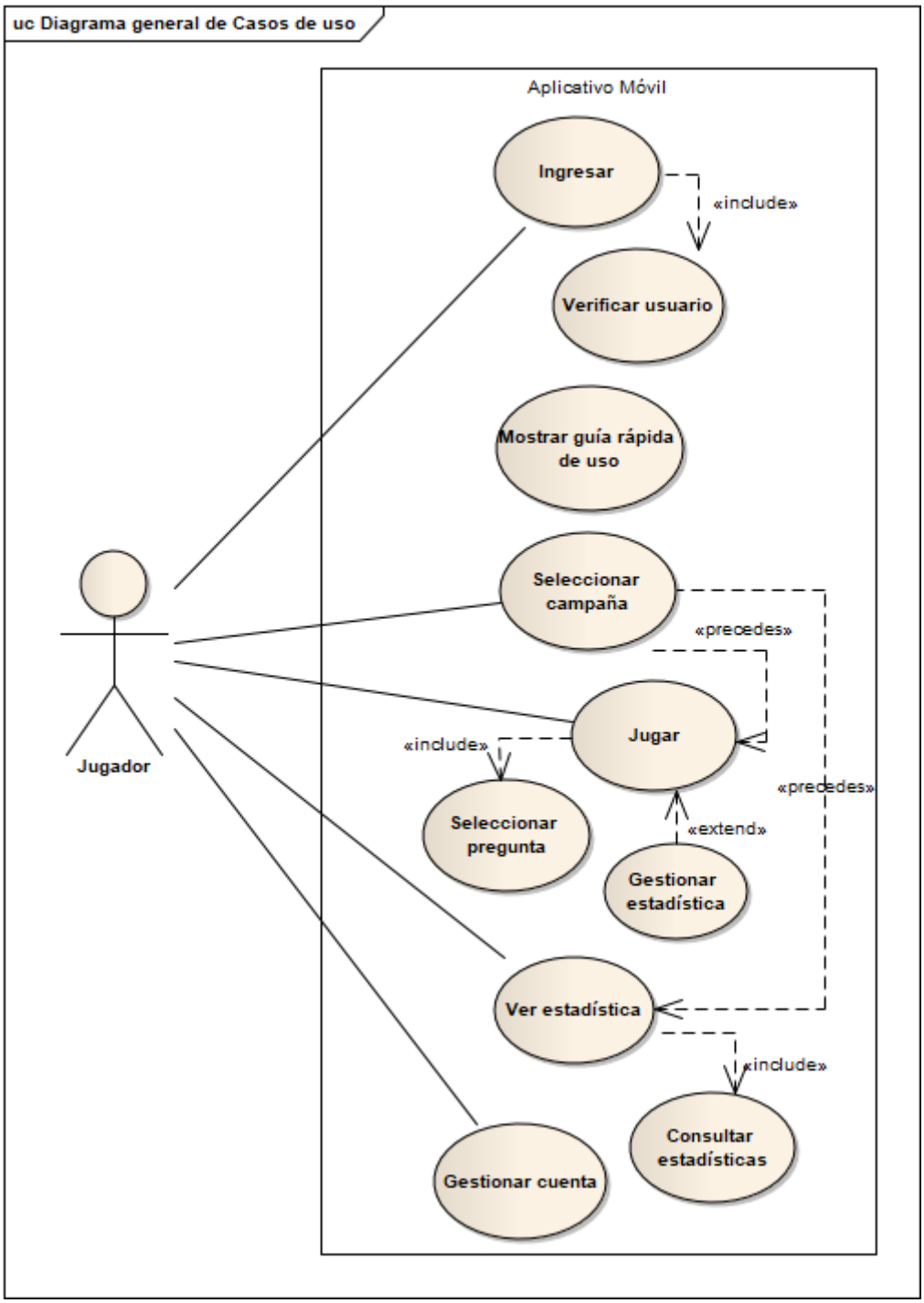


Figura 54. Diagrama General de casos de uso del aplicativo móvil. (Creado por los Investigadores).

Algunos casos de uso necesitan la inclusión y realización de otros para la obtención de los resultados de las peticiones hechas por el usuario. Sobre la figura anterior, se puede seleccionar a manera de ilustración, el primer caso de uso donde el usuario para ingresar al aplicativo, debe diligenciar un formulario, estos datos son capturados y verificados por la misma aplicación,

mediante una consulta a la base de datos. Lo anterior se resume en decir que el segundo caso de uso se hace necesario para la realización del primero.

Para la creación de la base de datos, se realizó el diagrama entidad relación (EER), el cual recolecta todas las características necesarias para el correcto almacenamiento de la información obtenida, procesada y recolectada en la aplicación.

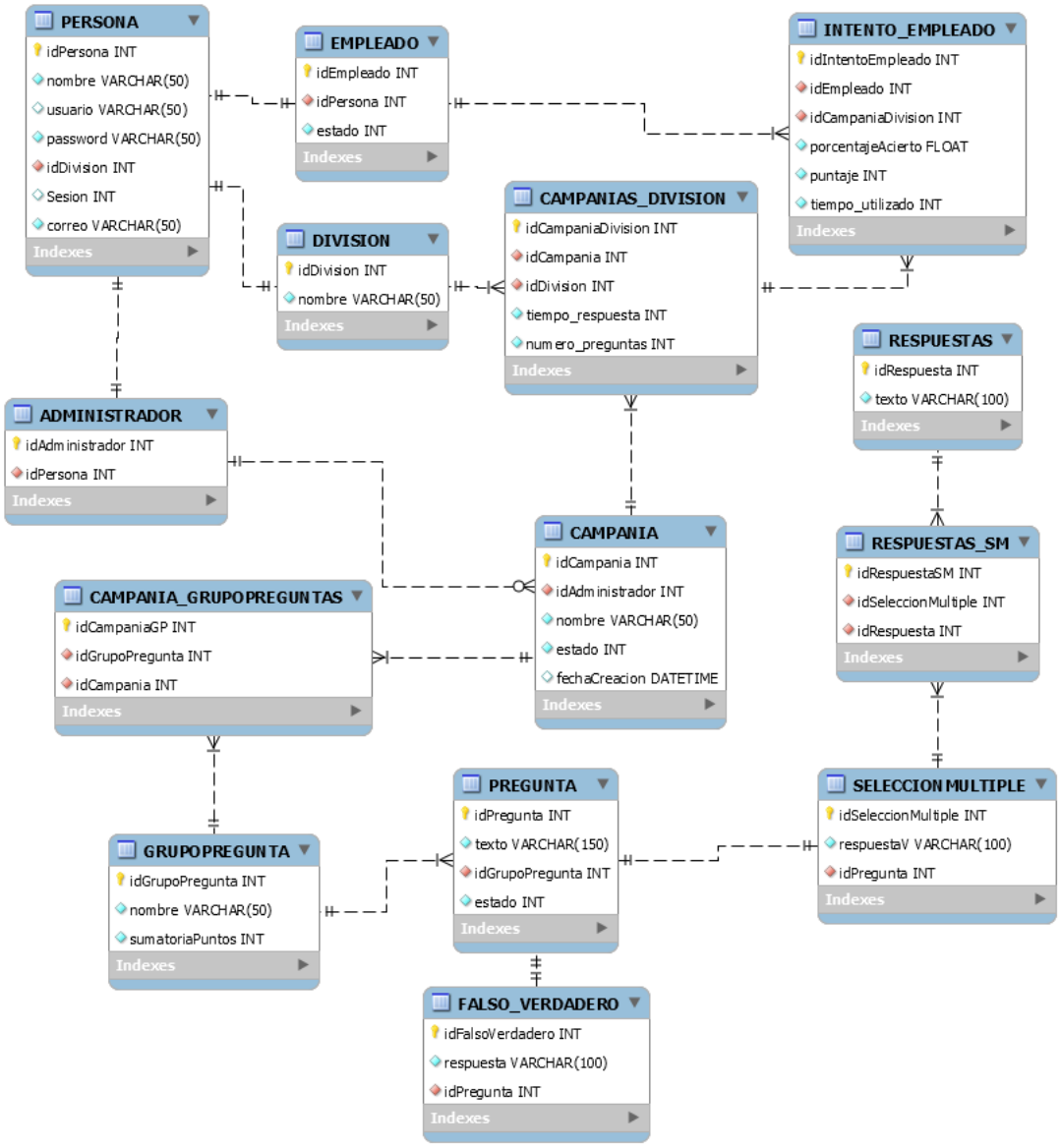


Figura 55. Diagrama entidad relación del aplicativo móvil. (Creado por los Investigadores).

Mientras que, como último procedimiento, en el modelo de implementación se emplearon la vista de desarrollo y la vista de despliegue, representados mediante un diagrama de paquetes y un diagrama de despliegue, respectivamente. Con el fin de definir la forma en

que se implementó el aplicativo móvil. El diagrama de paquetes mostrado en la *figura 45*, muestra las divisiones del aplicativo móvil en agrupaciones lógicas que se encargaron de particionar el desarrollo del aplicativo, es decir, cada paquete se pudo crear y desarrollar independientemente de los otros, aunque en la ejecución de este proyecto, las flechas (dependencias) indicaron la forma secuencial en que se realizó el desarrollo del mismo. La unión entre todos los paquetes desarrollados, conforman el aplicativo móvil.

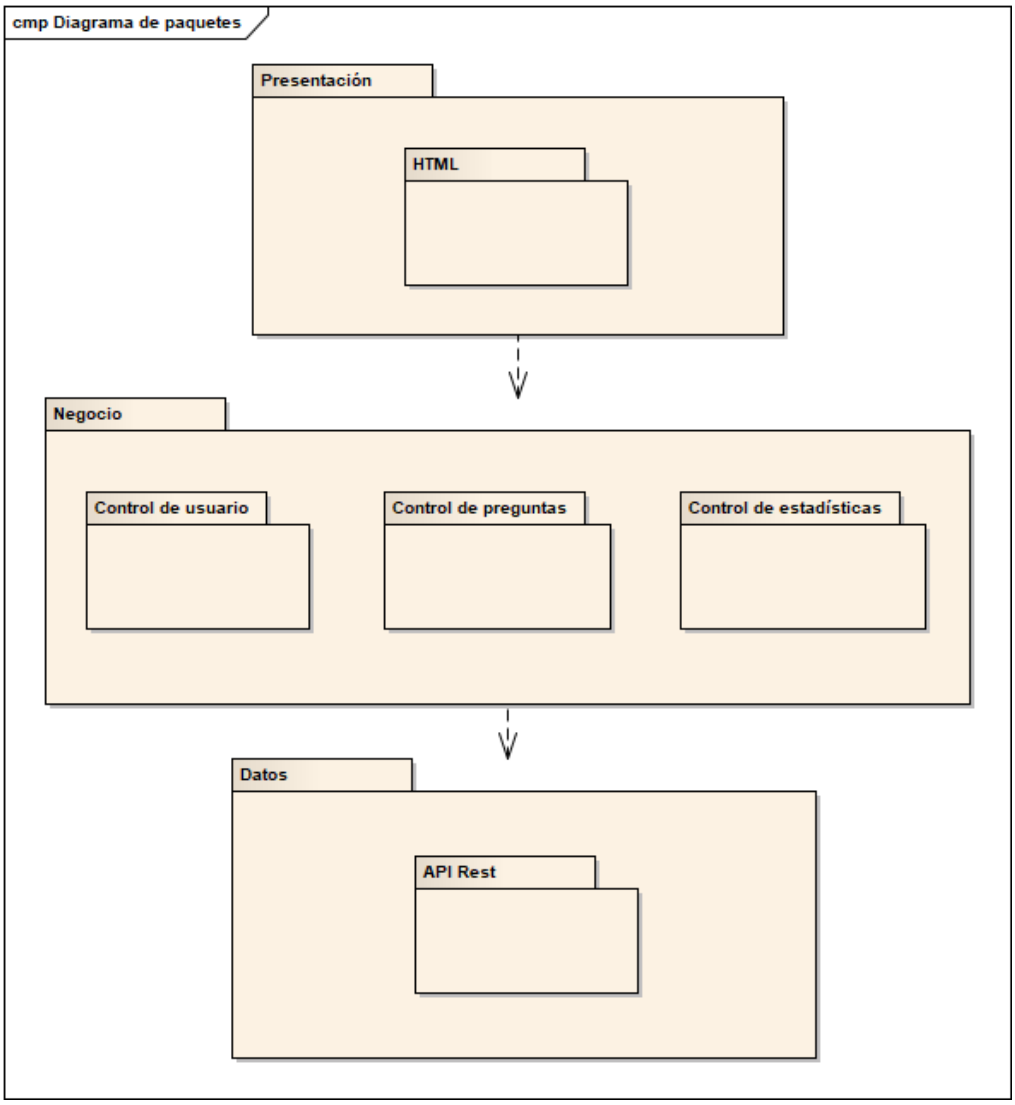


Figura 56. Modelo de implementación del aplicativo móvil, representado a partir de un Diagrama de paquetes. (Creado por los Investigadores).

En la vista de despliegue *(ver figura 46)*, se muestra la disposición física del aplicativo móvil y su componente web, como lo es la base de datos. Este diagrama representa los dos nodos que tienen la capacidad de almacenar componentes, y la habilidad de relacionarse entre sí por dichos

componentes. Los teléfonos con plataformas Android son una parte del diagrama de despliegue, estos teléfonos contarán con el aplicativo móvil que hará uso de una base de datos alojada en un servidor virtual de la empresa BIOFLM S.A. que se encuentra en Microsoft Azure.

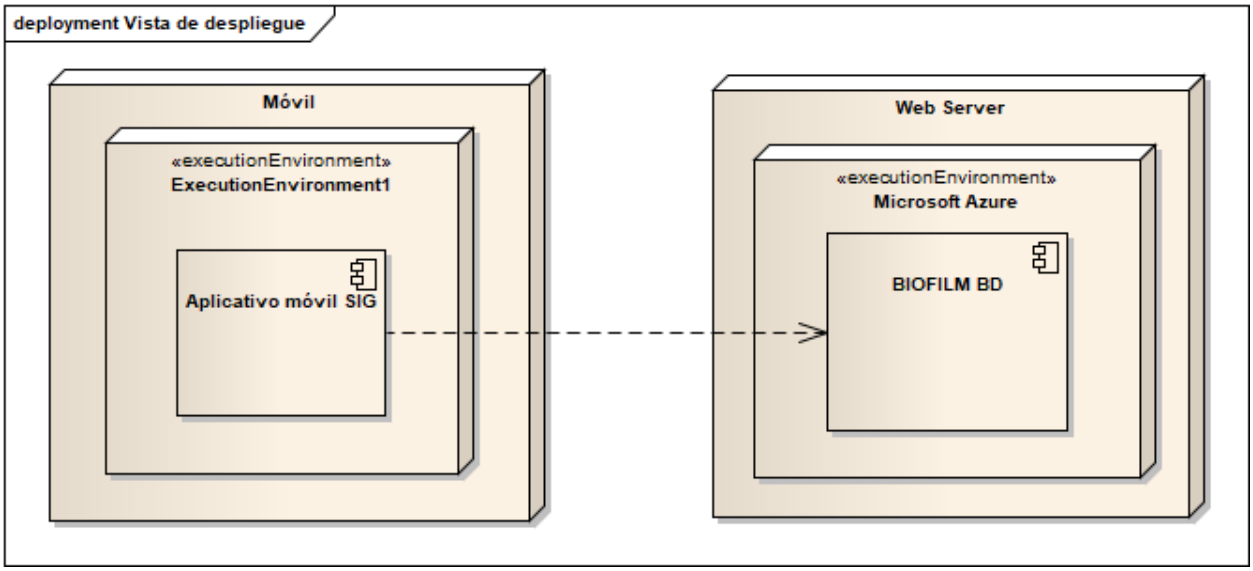


Figura 57. Vista de despliegue del aplicativo móvil, representada por un Diagrama de despliegue. (Creado por los Investigadores).

10.4.5. FASE DE ESTABILIZACIÓN

En esta fase se desarrollaron las últimas etapas de integración para asegurar el correcto funcionamiento del aplicativo móvil. Las integraciones aquí realizadas, hacen referencia a la unión entre el aplicativo móvil, la API REST que ofrece los servicios, y la base de datos. A continuación, se muestra el proceso de unificación entre las partes mencionadas:

10.4.5.1. CONEXIÓN DE LA API CON LA BASE DE DATOS

Como método para la configuración de la API, se importaron las librerías necesarias para la creación del servidor, se referenciaron los archivos de conexión con la base de datos, las rutas para acceder a los servicios, los permisos de acceso y se indicó el puerto por el cual se muestra la información.

```
var express = require('express');
var bodyparser = require('body-parser');


var app = express();
app.use(bodyparser.urlencoded({ extended: true }));
app.use(bodyparser.json());

var connection = require('./connection');
var routes = require('./routes');
var cors = require('./cors');
app.use(cors.permisos);
connection.inicia();
routes.configurar(app);

var server = app.listen(8000, function () {
    console.log('Base de datos de BIOFILM S.A., escuchando por el puerto ', server.address().port)
})
```

Figura 58. Configuración de la API REST.

El siguiente fragmento de código, muestra la forma en que se conecta la API con la base de datos. Las configuraciones realizadas, pertenecen a las credenciales necesarias que se deben suministrar para poder acceder a la información almacenada en la misma.

```
var mysql = require('mysql');

function Conexion() {
    this.pool = null;

    this.inicia = function () {
        this.pool = mysql.createPool({
            connectionLimit: 10,
            host: 'localhost',
            user: 'root',
            password: 'SIGBIOFILM2018',
            database: 'politicas_biofilm'
        })
    }

    this.obtener = function (callback) {
        this.pool.getConnection(function (error, connection) {
            callback(error, connection);
        })
    }
}

module.exports = new Conexion();
```

Figura 59. Conexión de la API con la base de datos.

10.4.5.2. CONEXIÓN DEL APLICATIVO MÓVIL CON LA API

Después de haber configurado y conectado la API con la base de datos y colocado a disposición los servicios, la aplicación móvil solo debe acceder a las rutas indicadas para recoger la información dispuesta. Esto se hace mediante la configuración mostrada a continuación:

```
constructor(public http: HttpClient) {
  this.headers = new Headers({
    'Content-Type': 'application/json; charset=utf-8'
  }
  );

  this.url = "http://37.117.84.141:8000";

}
```

Figura 60. Conexión del aplicativo móvil con la API.

La forma utilizada para obtener la información, es ingresando la IP pública en la que se encuentra alojada la API, junto con el puerto de salida de información. Además, se debe concatenar el nombre de la petición, junto con los parámetros de la misma (en caso de ser necesarios), como se muestra en la siguiente figura:

```
login(usuario: string, pass: string) {
  let url = `${this.url}/login/${usuario}/${pass}`;
  let headers = this.headers;

  return this.http.get(url, { headers })
    .map(data =>
      data);
}
```

Figura 61. Ejemplo de petición a la API.

10.4.6. FASE DE PRUEBAS

Para evaluar el comportamiento y funcionalidad del aplicativo móvil en un ambiente real e identificar fortalezas y posibles errores, se realizaron dos tipos de pruebas para que los empleados dispuestos por la empresa BIOFILM S.A., pudieran dar uso al aplicativo desde sus teléfonos móviles y detectaran fortalezas, y en caso de existir posibles errores, corregirlos

evitando la realización de cambios extras en la estructura de la aplicación. Una vez terminadas las pruebas, se obtuvo una APP cuya utilización queda a consideración de la empresa, según sus procesos administrativos.

10.4.6.1. PRUEBAS DE USUARIO

Para la realización de las pruebas de usuario, se hizo necesaria la interacción con un grupo de empleados que la empresa dispuso, a quienes se les entregó un formulario con preguntas para evaluar la identidad, contenido, usabilidad, navegabilidad, diseño y experiencia de usuario del aplicativo.

La metodología de la prueba consistió en reunir en una de las salas de capacitaciones que la empresa posee, a una muestra de 4 empleados que Recursos Humanos designó para hacer las pruebas, pertenecientes a 4 divisiones distintas *(ver anexo 7).* A estas personas se les instaló el aplicativo en sus teléfonos móviles con sistema operativo Android. Luego, el administrador creó una campaña en la que todos los citados fueron incluidos, y donde se hacían preguntas sobre las políticas de seguridad de la información. Inmediatamente, se procedió con la creación de la cuenta de usuario de cada uno de ellos, y su ingreso a la aplicación. Posteriormente, a los empleados se les informó que tenían la posibilidad de hacer 5 intentos, con los cuales se conformó la tabla general y las estadísticas individuales de todos. Por último, se entregó un formato de evaluación del aplicativo, que contenía preguntas cerradas a las que debían responder Si o No, enfocadas a la evaluación de las características de identidad, contenido, usabilidad, navegabilidad, diseño y experiencia de usuario. El formato utilizado para esta evaluación, se puede apreciar en el a*nexo 8.*

Con la finalidad de adquirir las facultades necesarias para evaluar el funcionamiento del aplicativo, los empleados fueron orientados a seguir un camino lógico de uso de la aplicación, el cual se ilustra a continuación:

1. El administrador, creó la campaña de prueba, en la que se anexaron las divisiones correspondientes con cada uno de los empleados citados, y los temas 1, 2 y 10 correspondientes con las políticas de seguridad de la información que la empresa maneja.

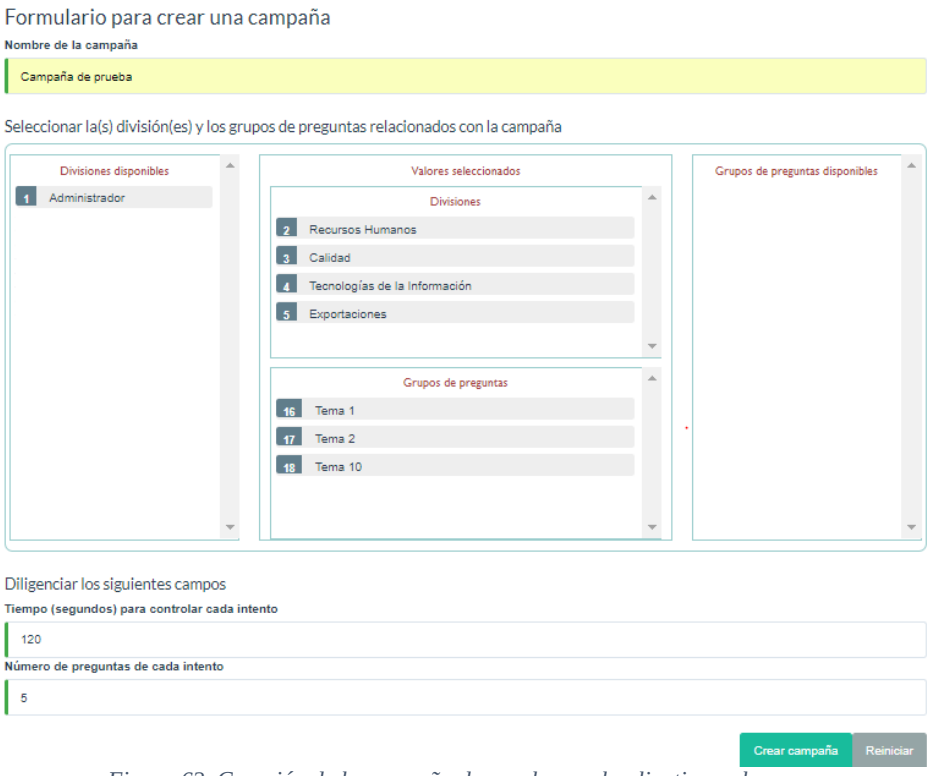


Figura 62. Creación de la campaña de prueba en el aplicativo web.

2. Seguidamente, los empleados diligenciaron el formulario de creación de cuenta, con los datos pertinentes. Cada campo indicó la forma de entrada de sus datos.

Figura 63. Creación de cuenta.

3. Durante el registro, la conexión a internet se perdió y el aplicativo lo hizo saber.

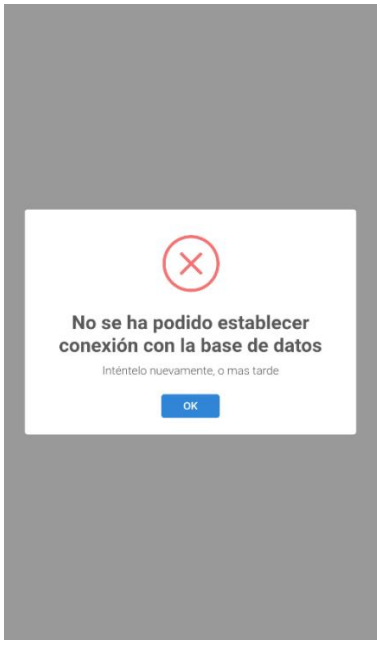


Figura 64. Error de conexión con la base de datos.

4. Una vez comprobados los datos ingresados, se indica que el usuario necesario para hacer el login, fue enviado al correo.

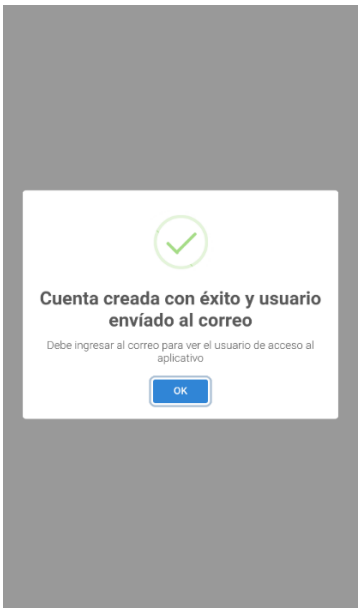


Figura 65. Éxito de creación de cuenta.

5. Se realizó el login con el usuario enviado al correo, y la contraseña diligenciada en el formulario de creación de cuenta.

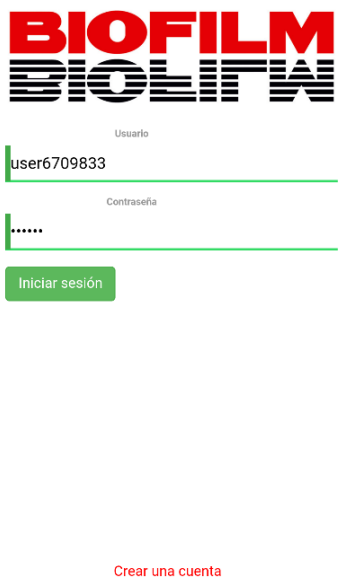


Figura 66. Login.

6. Al hacer el login, se muestra la ventana inicial del aplicativo.

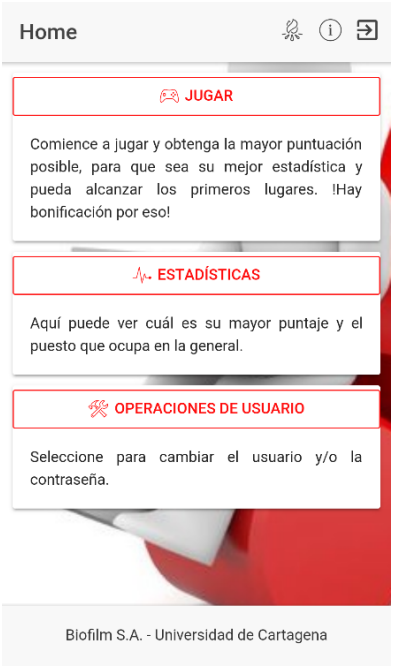


Figura 67. Página inicial.

7. Posteriormente, se seleccionó la campaña creada previamente por el administrador.

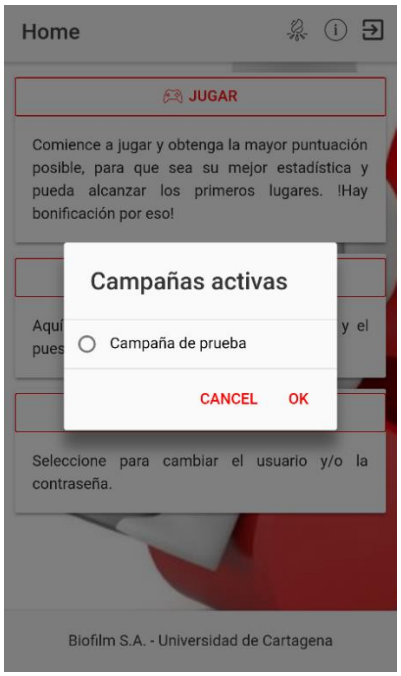


Figura 68. Selección de campaña.

8. Al seleccionar “Jugar”, se muestra la primera pregunta. Este proceso lo hicieron 5 veces, equivalente a 5 intentos.

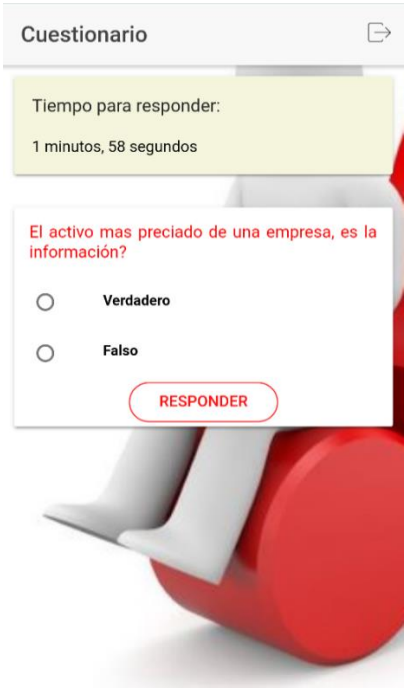


Figura 69. Estadísticas del intento.

9. Posteriormente, al finalizar cada intento, se muestran los detalles del mismo.

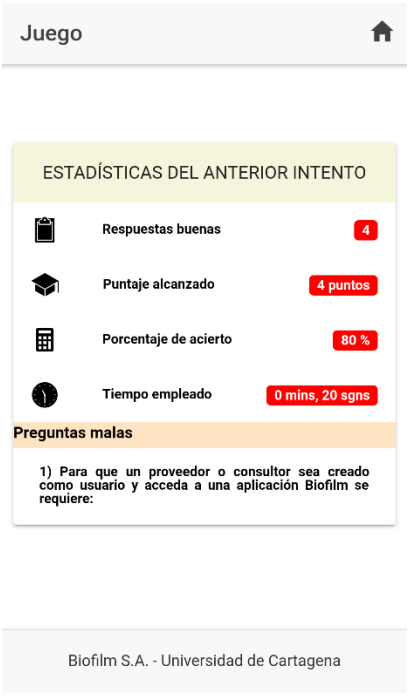


Figura 70. Cuestionario de juego.

10. Al haber finalizado los 5 intentos, se accedió a la estadística general, donde se ven reflejados los resultados generales de la campaña.

11. Del mismo modo, cada uno de los empleados citados, accedió a las estadísticas individuales, en la cual se muestran los resultados de cada intento realizado.

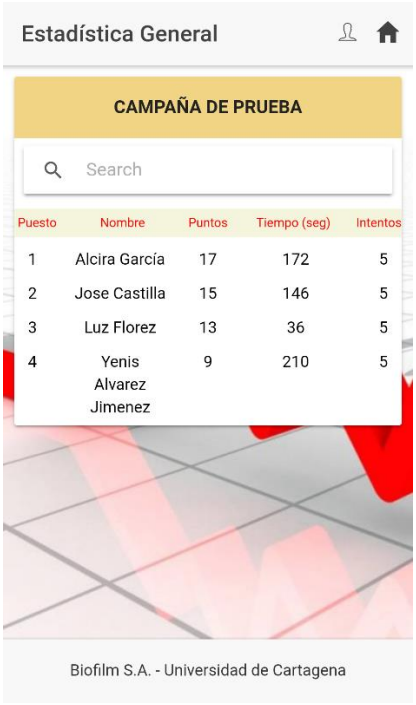


Figura 71. Estadísticas individuales.

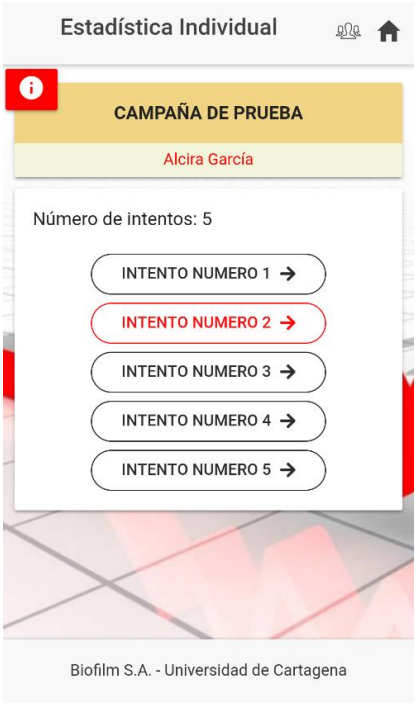


Figura 72. Estadísticas generales.

12. Al registrarse, el aplicativo otorga un usuario aleatorio a cada empleado, motivo por el cual, los citados modificaron sus usuarios por unos de interés.

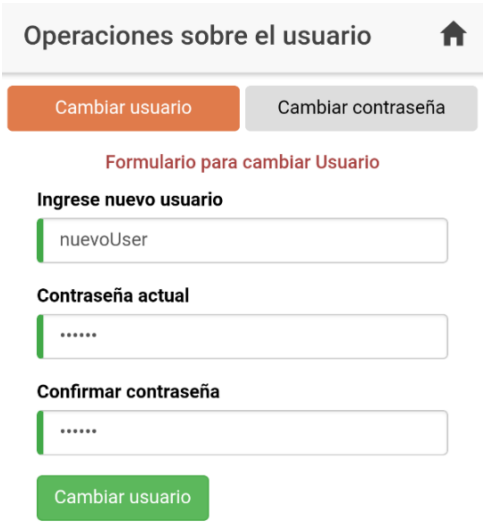


Figura 73. Cambio de usuario.

13. De igual forma, modificaron la contraseña.

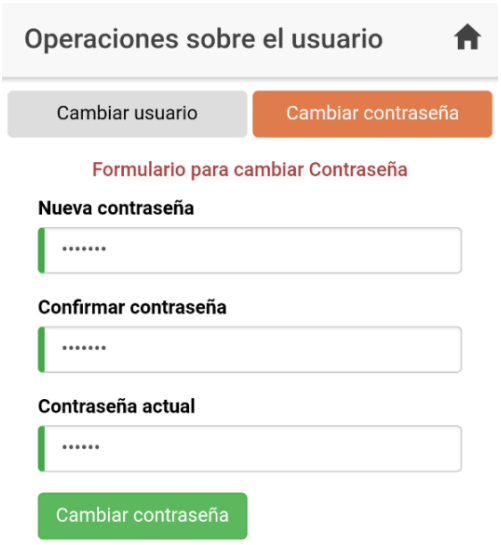


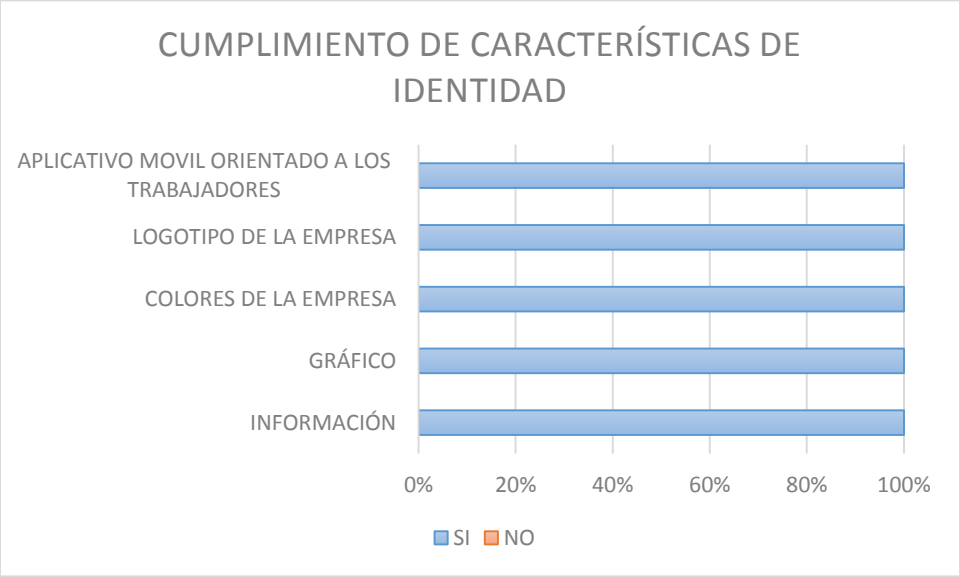
Figura 74. Cambio de contraseña.

10.4.6.1.1. CONSOLIDACIÓN DE RESULTADOS DE LA PRUEBA DE USUARIO

A partir de los resultados arrojados por el formato de evaluación del aplicativo móvil SIG, entregado y diligenciado en el marco de las pruebas de usuario, se realizó un análisis basado en las características fundamentales del aplicativo: identidad, contenido, usabilidad, navegabilidad, diseño y experiencia de usuario.

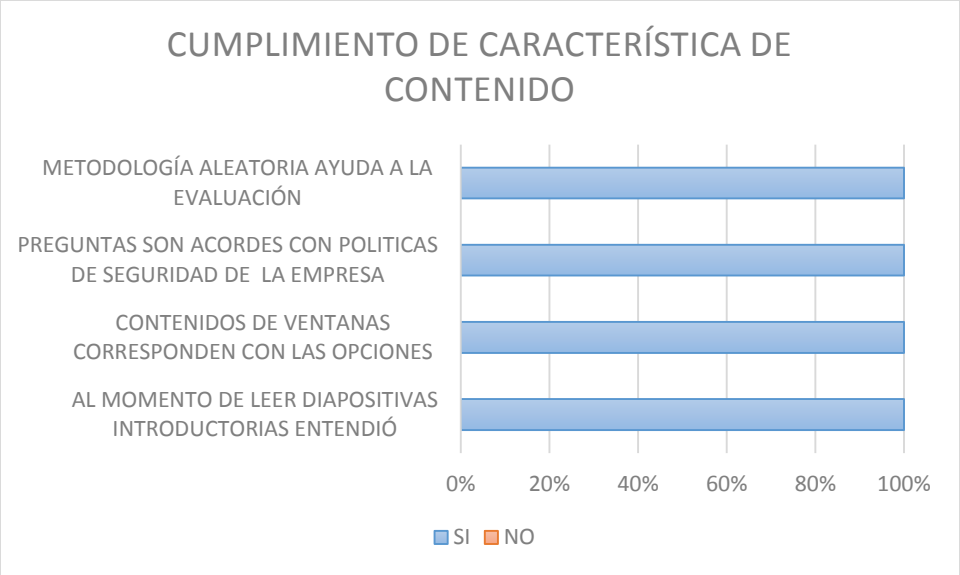
En el formato entregado había un total de 20 preguntas repartidas de la siguiente forma: 5 preguntas de identidad, 4 de contenido, 2 de usabilidad, 3 de navegabilidad, 5 de diseño, y 1 de experiencia de usuario *(ver anexo 8)*. Las respuestas a cada una de estas preguntas fueron agrupadas por el tipo de característica, y graficadas para una mejor ilustración.

La información que se muestra en la parte izquierda de cada fila de las siguientes gráficas, corresponde a un resumen concreto de una pregunta de la característica en cuestión.



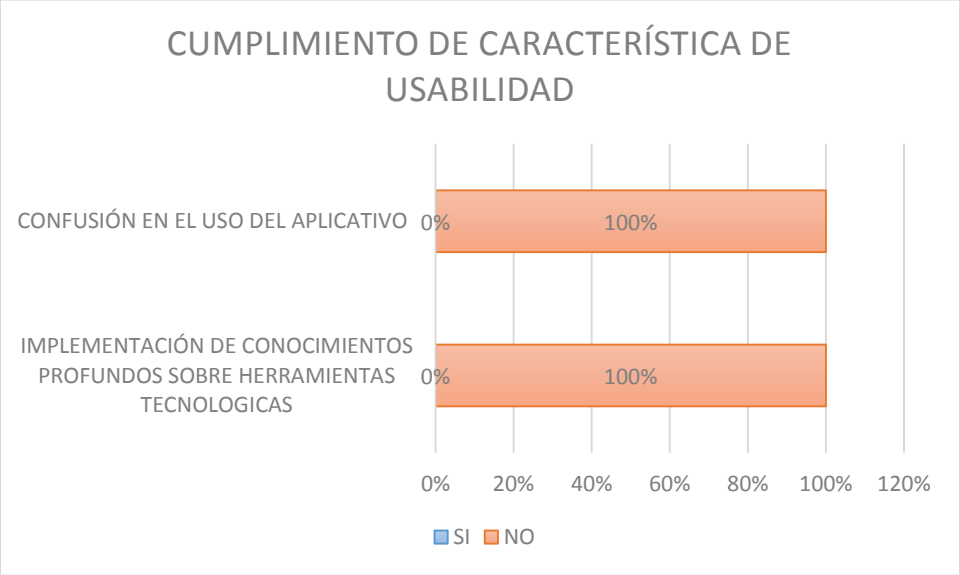
Gráfica 1. Cumplimiento de la característica de identidad del aplicativo móvil. (Fuente: encuestados)

De la muestra tomada para la elaboración de la prueba, el 100% de ella valida el cumplimiento de la característica de identidad estipulada en el formato, acorde con las expectativas planteadas al inicio de la evaluación, debido a que estos rasgos son importantes para orientar a los usuarios finales sobre el objeto de la solución desarrollada.



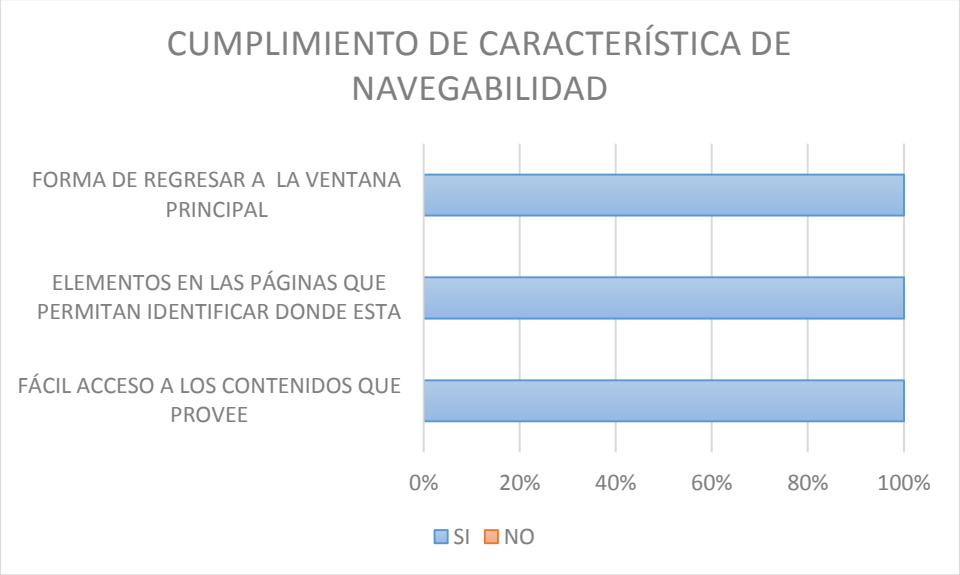
Gráfica 2. Cumplimiento de la característica de contenido del aplicativo móvil. (Fuente: encuestados).

Conforme a las características de contenido, la aprobación de la muestra fue total, debido a que el 100% de ella marcó las respuestas favorables con los contenidos que se presentan en el aplicativo móvil. Los resultados de esta característica, en caso de ser negativos, indicaban una reestructuración temática de los contenidos previstos, escenario que no ocurrió. A partir de lo anterior, se tiene certeza que la metodología adoptada para la enseñanza y/o aprendizaje de las políticas de seguridad, es adecuada.



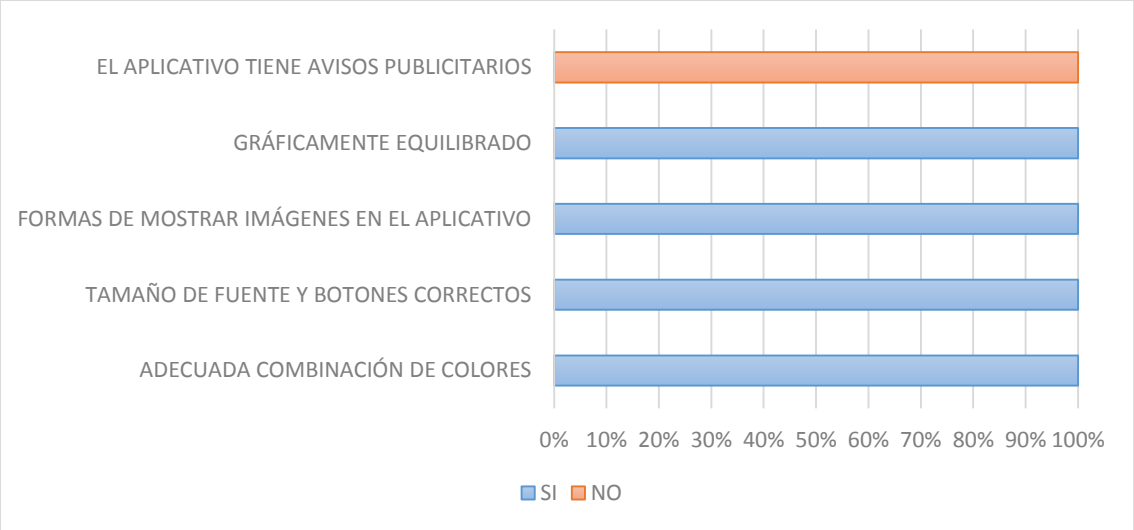
Gráfica 3. Cumplimiento de característica de usabilidad del aplicativo móvil. (Fuente: encuestados).

Las preguntas que se realizaron en el marco de las características de usabilidad, tenían como respuesta favorable el NO. Por lo que se deduce, a partir de la gráfica mostrada, que todos los empleados respondieron positivamente ante estas preguntas, indicando que el aplicativo móvil ofrece facilidad de uso y no exige manejo de otros conocimientos distintos a los de la temática.



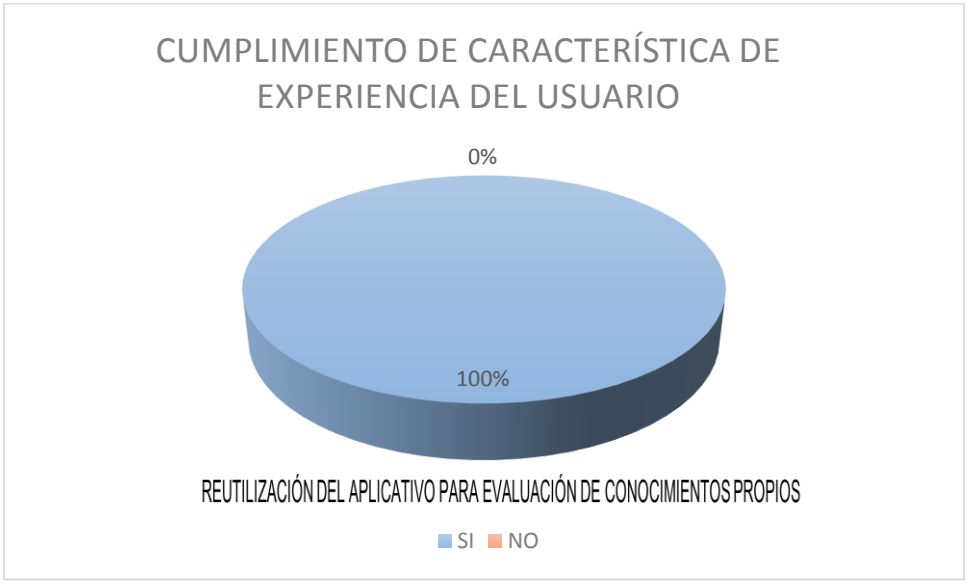
Gráfica 4. Cumplimiento de característica de navegabilidad del aplicativo móvil. (Fuente: encuestados).

La característica de navegabilidad revela la facilidad de acceso hacia los contenidos y características suministradas por la aplicación, al igual que la orientación de las páginas a las que se accede. Conforme a esto, las respuestas a las preguntas de este rasgo, brindadas por lo empleados que hicieron parte de la prueba y agrupadas en la *Gráfica 4*, indican que la disposición y ubicación de los contenidos es ideal para el buen aprovechamiento del aplicativo. Del mismo modo, lo es la orientación ofrecida para establecer el lugar en que se encuentran en determinado momento dentro de la APP.



Gráfica 5. Cumplimiento de característica de diseño del aplicativo móvil. (Fuente: encuestados).

Dentro de la característica de diseño, la pregunta "¿El aplicativo tiene banners o avisos publicitarios?", tiene como respuesta positiva un NO. Por lo que, apreciando la gráfica anterior, se concluye que, al igual como ha sucedido con las anteriores, el aplicativo cumple con las exigencias previstas de diseño. Esto tiene relación directa con los intereses de los investigadores en brindar una herramienta agradable visualmente para motivar su uso y el aprendizaje.



Gráfica 6. Cumplimiento de característica de experiencia de usuario. (Fuente: encuestados).

Como última característica se analiza la experiencia de usuario, la cual engloba las anteriores, y con ella se pretende saber si el usuario de sintió a gusto con la solución desarrollada y si ésta la

volverían utilizar para seguir evaluando los conocimientos que tienen acerca de las políticas de seguridad. Conforme a ello, todos los empleados informaron que este aplicativo lo utilizarían las veces necesarias, debido a que es una herramienta sencilla y de fácil uso.

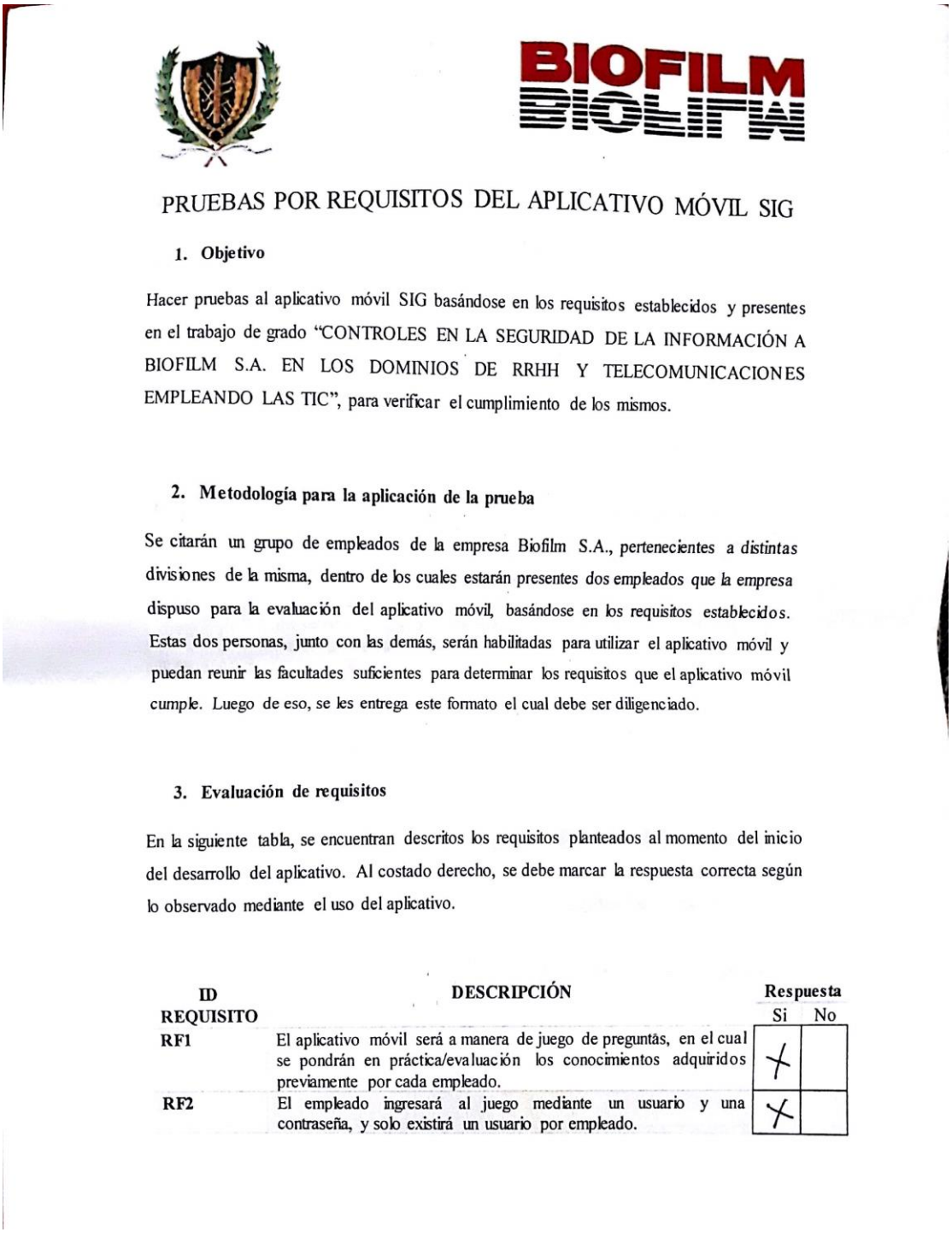
Después de haber descrito los resultados mostrados en cada una de las gráficas, de manera general se puede concluir lo siguiente:

- El éxito del desarrollo de un proyecto, se califica a partir de las expectativas y sensaciones de los usuarios finales. Por tanto, con los resultados planteados anteriormente, se concluye que el desarrollo del aplicativo móvil para la evaluación de los conocimientos que poseen los empleados de la empresa BIOFILM S.A., sobre las políticas de seguridad, finalizó exitosamente debido a que el 100% de la muestra otorgó la mejor calificación a las características tratadas en esta prueba.
- El desarrollo de las pruebas fue un éxito, debido a que se cumplieron con todas las expectativas de los usuarios finales.
- La totalidad de los empleados de la muestra, indicaron que el aplicativo móvil ayuda al aprendizaje y evaluación de los conocimientos sobre las políticas de seguridad, es decir, que la APP cumple con su razón.
- Del mismo modo, los empleados declararon que el aplicativo posee un alto grado de usabilidad, debido a que es sencillo y no amerita conocimientos avanzados de tecnología. Además, también expresaron que el aspecto estético es ideal, agradable a la vista y posee contenido gráfico apropiado para la temática tratada.

10.4.6.2. PRUEBAS POR REQUISITOS

Como otro método de prueba del aplicativo móvil, se realizó la prueba por requisitos, la cual consta de un formato en el que están enumerados cada uno de los requisitos funcionales estipulados. Este formato fue entregado a un empleado designado por la empresa, con la facultad de evaluar el aplicativo conforme a los requisitos planteados.

A continuación, se muestra el formato diligenciado y en cual se puede constatar el cumplimiento de los requisitos por parte del aplicativo móvil.



PRUEBAS POR REQUISITOS DEL APLICATIVO MÓVIL SIG

1. Objetivo

Hacer pruebas al aplicativo móvil SIG basándose en los requisitos establecidos y presentes en el trabajo de grado "CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC", para verificar el cumplimiento de los mismos.

2. Metodología para la aplicación de la prueba

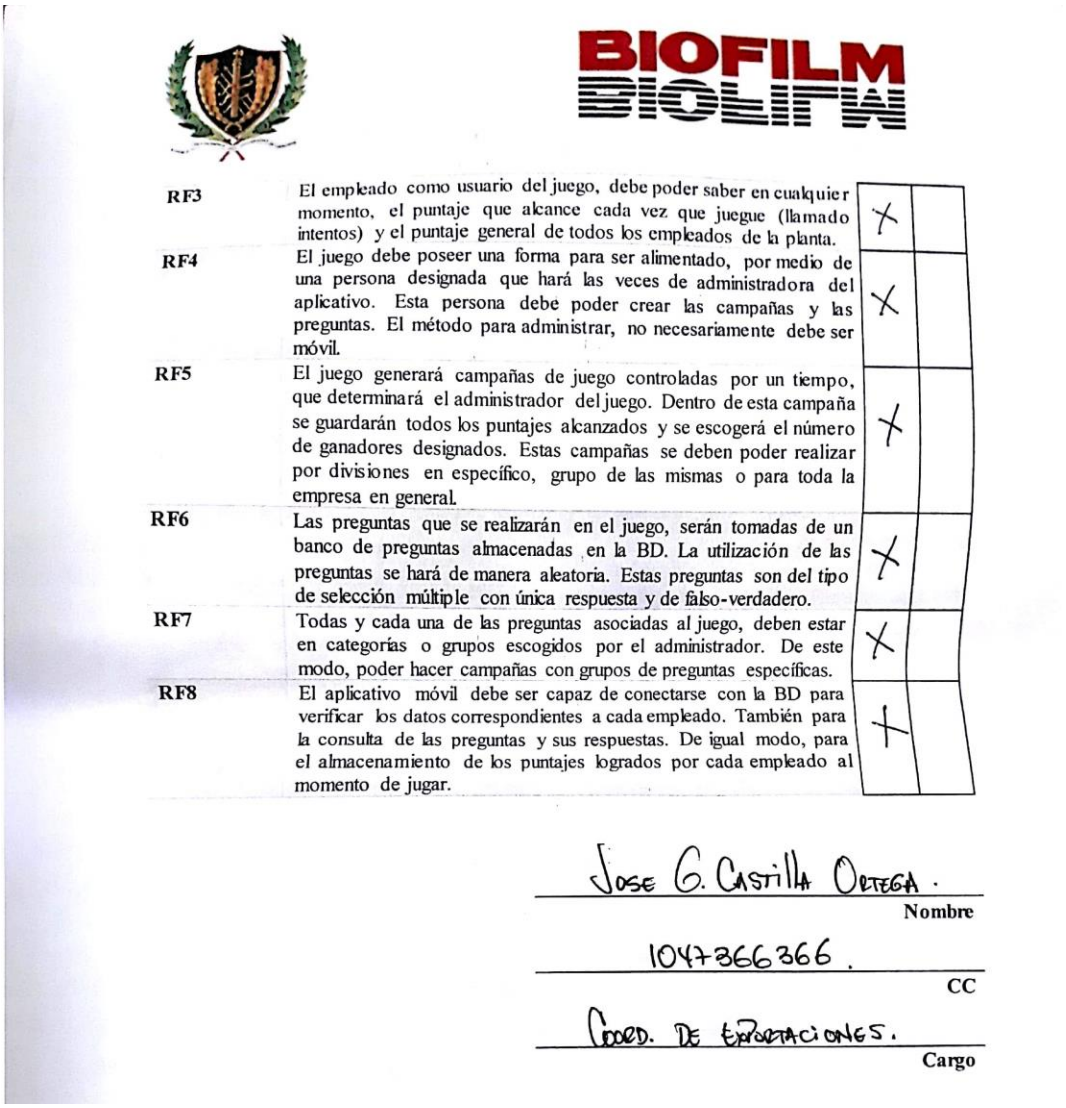
Se citarán un grupo de empleados de la empresa Biofilm S.A., pertenecientes a distintas divisiones de la misma, dentro de los cuales estarán presentes dos empleados que la empresa dispuso para la evaluación del aplicativo móvil, basándose en los requisitos establecidos. Estas dos personas, junto con las demás, serán habilitadas para utilizar el aplicativo móvil y puedan reunir las facultades suficientes para determinar los requisitos que el aplicativo móvil cumple. Luego de eso, se les entrega este formato el cual debe ser diligenciado.

3. Evaluación de requisitos

En la siguiente tabla, se encuentran descritos los requisitos planteados al momento del inicio del desarrollo del aplicativo. Al costado derecho, se debe marcar la respuesta correcta según lo observado mediante el uso del aplicativo.

ID REQUISITO	DESCRIPCIÓN	Respuesta Si	Respuesta No
RF1	El aplicativo móvil será a manera de juego de preguntas, en el cual se pondrán en práctica/evaluación los conocimientos adquiridos previamente por cada empleado.	X	
RF2	El empleado ingresará al juego mediante un usuario y una contraseña, y solo existirá un usuario por empleado.	X	

Figura 75. Formato de evaluación de requisitos del aplicativo móvil. Página 1.



BIOFILM

RF3	El empleado como usuario del juego, debe poder saber en cualquier momento, el puntaje que alcance cada vez que juegue (llamado intentos) y el puntaje general de todos los empleados de la planta.	X	
RF4	El juego debe poseer una forma para ser alimentado, por medio de una persona designada que hará las veces de administradora del aplicativo. Esta persona debe poder crear las campañas y las preguntas. El método para administrar, no necesariamente debe ser móvil.	X	
RF5	El juego generará campañas de juego controladas por un tiempo, que determinará el administrador del juego. Dentro de esta campaña se guardarán todos los puntajes alcanzados y se escogerá el número de ganadores designados. Estas campañas se deben poder realizar por divisiones en específico, grupo de las mismas o para toda la empresa en general.	X	
RF6	Las preguntas que se realizarán en el juego, serán tomadas de un banco de preguntas almacenadas en la BD. La utilización de las preguntas se hará de manera aleatoria. Estas preguntas son del tipo de selección múltiple con única respuesta y de falso-verdadero.	X	
RF7	Todas y cada una de las preguntas asociadas al juego, deben estar en categorías o grupos escogidos por el administrador. De este modo, poder hacer campañas con grupos de preguntas específicas.	X	
RF8	El aplicativo móvil debe ser capaz de conectarse con la BD para verificar los datos correspondientes a cada empleado. También para la consulta de las preguntas y sus respuestas. De igual modo, para el almacenamiento de los puntajes logrados por cada empleado al momento de jugar.	X	

Jose G. Castilla Ortega.
Nombre

1047366366.
CC

Coord. De Expectaciones.
Cargo

Figura 76. Formato de evaluación de requisitos del aplicativo móvil. Página 2.

Este método de prueba, arrojó como resultado, que todos los requisitos estipulados fueron realizados. Por lo que, el aplicativo móvil cumple con las expectativas generadas al momento de plantear los requisitos.

En el formato se indica que la evaluación del aplicativo basándose en sus requisitos, la realizarían dos empleados dispuestos por la empresa, pero debido a que uno de ellos no pudo asistir, entonces la determinación del cumplimiento de los requisitos estuvo a cargo del otro empleado.

Finalizada la etapa de pruebas, el aplicativo móvil fue entregado y recibido por parte de la empresa, mediante la ingeniera Yenis Álvarez Jiménez, jefa de la división de TI. Esto puede ser verificado en el *anexo 11*.

10.5. CONSTRUIR Y ANEXAR UN OVA AL LMS EMPRESARIAL PARA LA DIVULGACIÓN Y EVALUACIÓN DE LOS CONOCIMIENTOS SOBRE LAS POLÍTICAS DE LA EMPRESA.

De acuerdo a lo establecido en la metodología del proyecto, y con la finalidad de cumplir con el objetivo planteado, se desarrollaron las 5 etapas de la metodología AODDEI con sus actividades pertinentes, para lograr obtener un producto de calidad, respetando los 3 pilares fundamentales en el desarrollo OVA. Los pilares son: 1) Componente de taxonomía: referencia a la forma que toma el objeto virtual de aprendizaje con relación a su estructura; 2) Componente de contenido temático y multimedial: enfatiza en propiciar la información de una forma dinámica y llamativa para el usuario final; 3) Componente de retroalimentación: encargado de evaluar la información presentada previamente.

10.5.1. ETAPA DE ANÁLISIS Y OBTENCIÓN

10.5.1.1. ANÁLISIS

Según lo planteado en la etapa de análisis de la metodología, y contemplando el desarrollo del OVA, se consideró pertinente citar el objetivo sobre el cual se trabajó, para poder crear un punto de referencia al abarcar esta etapa.

- Construir y anexar un OVA al LMS empresarial para la divulgación y evaluación de los conocimientos sobre las políticas de la empresa.

En el análisis de la información, obtención y delimitación del material de aprendizaje a incluir en el OVA, concernientes con las políticas de seguridad de la información, se realizaron reuniones con el personal de recursos humanos de la empresa *(ver anexo 2 y 4)*, con el fin de definir los requisitos que permitieron guiar el desarrollo del OVA. Todo esto considerando la necesidad de aprendizaje por parte de los empleados de la planta de BIOFILM S.A con relación a dichas políticas.

10.5.1.1.1. REQUISITOS FUNCIONALES DEL OVA

A partir de la reunión realizada con la división de RRHH, se fijaron los requisitos funcionales necesarios en la etapa de desarrollo del OVA, los cuales se establecen en la siguiente tabla:

ID Requisito	Nombre del requisito	Descripción
RF1	Reproducciones sin sonido	Dentro de la empresa no deberán ser emitidos sonidos por parte del OVA.
RF2	Globos de idea	El despliegue informativo en el OVA, deberá hacerse a través de globos de idea, para seguir en la misma didáctica empleada por BIOFILM S.A.

Tabla 10. Requerimientos funcionales del OVA.

10.5.1.1.2. REQUISITOS NO FUNCIONALES DEL OVA

Los requisitos no funcionales definidos para el OVA, surgieron a partir de los requerimientos plasmados en el *anexo 4*. Estos ayudaron en el desarrollo de los requisitos funcionales definidos anteriormente y a su puesta en marcha, debido a que son características de funcionamiento que relacionan cada una de las acciones que el usuario del aplicativo realiza.

En la siguiente tabla, están definidos los requisitos no funcionales del OVA:

ID Requisito	Nombre del requisito	Descripción
RNF 1	Usabilidad	Debe ser lo más intuitivo posible, transmitiendo un mensaje claro.
RNF2	Seguridad	El ingreso a la parte operativa del OVA, estará limitado solo al administrador
RNF3	Desempeño	El OVA no deberá presentar problemas para su manejo e implementación.
RNF4	Colores Institucionales	Para el desarrollo del OVA deberán manejarse primordialmente los colores rojo y negro, por ser

		estos los colores institucionales.

Tabla 11 - Requisitos no funcionales del OVA.

Dentro la fase de análisis, se definieron los aspectos fundamentales en el desarrollo y creación del OVA, presentados a continuación:

Nombre del OVA	SIG OVA
Descripción de OVA	Con el fin de dar a conocer las diferentes políticas de seguridad de la información a nivel de la planta de BIOFILM S.A., se creó un OVA que permite comprender las diferentes políticas manejadas en la empresa, desde el uso de tecnología, hasta la seguridad de los datos y copias de seguridad, para generar conciencia de la aplicación de las mismas.
Nivel escolar al que va dirigido el OVA	Bachilleres, Técnicos, Tecnólogos y/o Profesionales
Perfil de las personas a las que va dirigido	Empleados de BIOFILM S.A.
Objetivo de aprendizaje	Generar conciencia en cada uno de los empleados de la planta de BIOFILM S.A., sobre la importancia de atender a las políticas de seguridad de la información establecidas por la empresa.
Granulidad	El OVA está dividido en 10 ramificaciones, correspondientes a las diversas políticas que se trabajan en el proyecto.

Tabla 12. Análisis del dominio.

Con relación a los aspectos fundamentales definidos, se hizo referencia a la contextualización de la herramienta de aprendizaje, mediante la descripción de la misma. También, se definió el grado de escolaridad que permitió identificar el nivel de los conocimientos impartidos por medio del material didáctico. Así mismo, se indicó el perfil de las personas a las cuales se orientó la

herramienta, y se destacó el objetivo de aprendizaje, que permitió identificar la finalidad al interactuar con el OVA, y se definió la estructura y comportamiento de los contenidos temáticos, mediante la característica de granulidad.

La tabla presentada anteriormente, permite identificar el cumplimiento del componente taxonómico, pilar importante en el desarrollo OVA.

10.5.1.2. OBTENCION DEL MATERIAL

Para cumplir con lo establecido en esta subetapa de la metodología, y considerando el desarrollo del OVA, la empresa proporcionó el material suficiente para concluir con el objetivo planteado. Dentro del material dispuesto por parte de la empresa, se contó con imágenes, diapositivas y documentos acordes con las políticas de la seguridad de la información.

Con el fin de una mejor organización en la obtención de la información a mostrar en la herramienta, se creó una tabla en la que se muestra el tipo de material y la fuente. Dicha tabla se establece a continuación:

TIPO DE MATERIAL	FUENTE
Material Electrónico	Empresa BIOFILM S.A.

Tabla 13. Obtención del material OVA

Toda la información necesaria que se publicó en la herramienta, pertenece estrictamente a la empresa, por lo cual fue la única fuente de suministro de material.

Con la obtención y delimitación del material proporcionado por BIOFILM S.A, se estaría cumpliendo con el componente de contenido temático y multimedial, esto queda en evidencia en la tabla anterior donde se indica el tipo de material obtenido y la fuente de información.

10.5.1.3. DIGITALIZACION DEL MATERIAL

A lo largo del desarrollo del OVA no fue necesario realizar un proceso de digitalización, debido a que todo el material didáctico utilizado fue proporcionado por la empresa de forma digitalizada, lo que permitió agilizar el proceso de creación del OVA en esta fase.

10.5.2. ETAPA DE DISEÑO

En esta etapa o fase se realizó el diseño para la estructura del OVA, y se delimitaron los contenidos temáticos a través de las distintas reuniones realizadas con el personal de TI y RRHH. Así mismo, se definió el aspecto visual del OVA y las estrategias de aprendizaje para apoyar los contenidos informativos.

De acuerdo a lo establecido en la etapa de diseño de la metodología AODDEI, se consideró necesario definir el objetivo principal a cumplir con la realización del OVA, reestructurado como objetivo pedagógico. A continuación, se muestra el objetivo enunciado anteriormente:

Objetivo Pedagógico: Generar conciencia en los empleados de BIOFILM S.A. sobre la importancia del buen uso de las políticas de seguridad.

Por otro lado, dentro de la fase de diseño establecida en la metodología AODDEI, se deben establecer los diferentes tópicos o contenidos a abordar en el OVA, los cuales complementaron el material informativo del mismo. Lo anterior, con el fin de tener claridad en la información que se pretende socializar con la puesta en marcha del objeto virtual de aprendizaje.

Contenido Informativo: Los tópicos abordados en la presentación de contenidos en el OVA, son:

- Consideraciones generales.
- Política de uso de Tecnología.
- Política de acceso a los servicios de tecnología de información y comunicaciones.
- Salida de equipos de cómputo, documentos y activos.
- Política de uso de equipos de escritorio y portátiles.

- Política de software.
- Política del uso de medios de almacenamiento extraíbles y puertos en los equipos.
- Política del uso del correo electrónico.
- Política del uso del internet.
- Política de seguridad de los datos y copias de seguridad.

A continuación, se presenta un bosquejo que muestra la forma en la que se ideó inicialmente el despliegue del contenido informativo en el OVA, y a su vez, en la posterior figura se muestra la forma en la cual se encuentra actualmente distribuido el contenido temático del mismo.

Figura 77 - Bosquejo inicial del contenido informativo

Figura 78 - Bosquejo final del contenido informativo

Diseño de la aplicación: A nivel arquitectónico de la aplicación se diseñaron algunos diagramas con el fin de tener una base de apoyo para desarrollar e implementar el OVA como estrategia de aprendizaje para las políticas de seguridad en BIOFILM S.A. A continuación, se presentan los diagramas empleados para modelar las funciones y comportamientos del objeto virtual de aprendizaje para este proyecto.

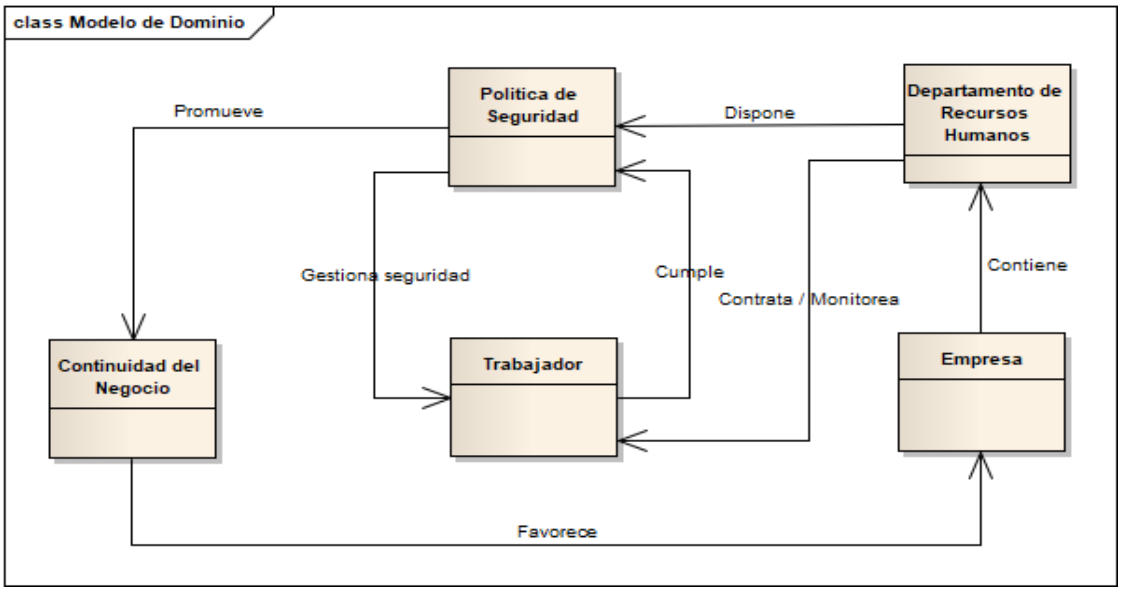


Figura 79 - Modelo de dominio del OVA

El diagrama representado en la figura anterior, corresponde al modelo de dominio del OVA. La determinación de las clases que componen este modelo, se realizó mediante el análisis de las funciones que se desarrollan dentro de la empresa, con relación a los deberes concernientes al marco de la seguridad de la información.

Como otro de los diagramas utilizados para representar el diseño arquitectónico, se utilizó el diagrama de casos de uso, que evidencia las acciones correspondientes con el empleado de BIOFILM S.A, quien accede a los contenidos informativos mostrados en el OVA mediante videos, imágenes y textos.

El empleado cumple con el papel de actor principal dentro del sistema, debido a que es la persona que está en constante interacción con el objeto virtual de aprendizaje, por ser el usuario final.

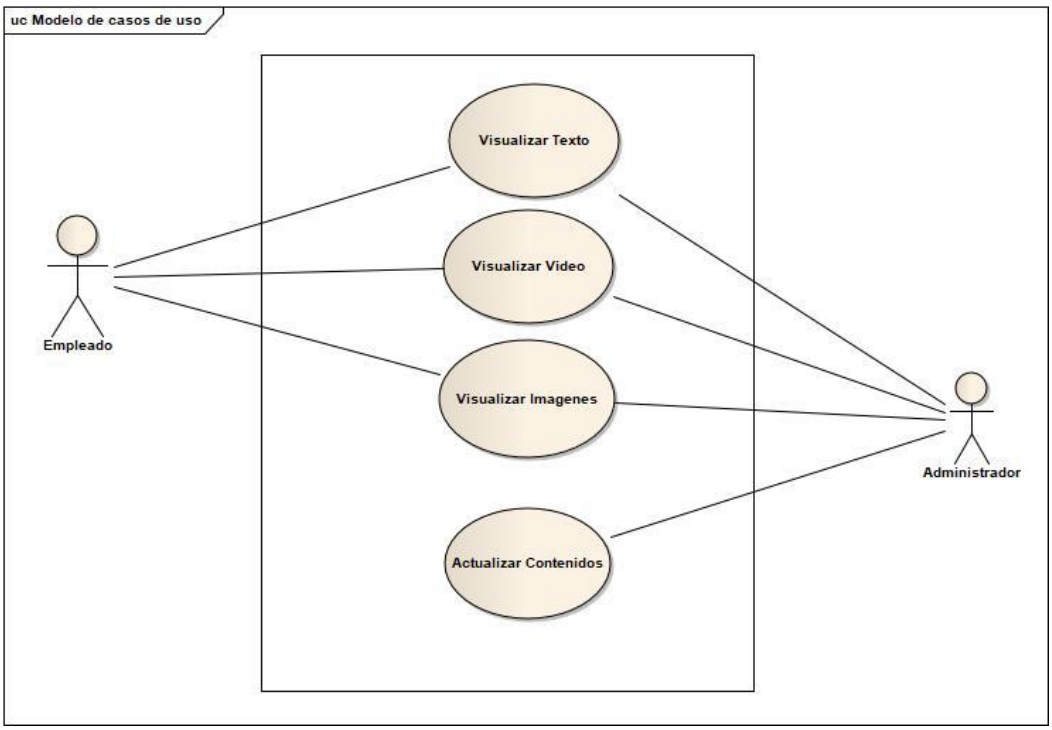


Figura 80 - Diagrama casos de usos

Dentro del diagrama se puede evidenciar que se asigna un administrador como actor, debido a que es la persona encargada de fortalecer el OVA conforme a las necesidades e intenciones de la empresa.

Por otro lado y considerando lo dicho al inicio de este capítulo con relación a los componentes fundamentales para el desarrollo OVA, se puede apreciar que a lo largo de la sección 7.5 y en particular en los diagramas o diseños arquitectónicos no se evidencia el componente de retroalimentación, esto se debe a que la creación del aplicativo móvil, es complementaria al OVA, siendo esta la encargada de evaluar y medir las competencias de los usuarios finales, una vez hallan echo uso del objeto virtual de aprendizaje. De esta forma se estaría cumpliendo con el último componente denominado retroalimentación.

10.5.3. ETAPA DE DESARROLLO

10.5.3.1. CONSTRUCCIÓN Y ADAPTACIÓN DE LOS COMPONENTES DE INGENIERÍA

En esta etapa se procedió al desarrollo del OVA, utilizando cada uno de los elementos generados en las etapas anteriores como fueron los contenidos teóricos, aspecto visual y demás elementos de contextualización, todo esto a fin de crear un entorno amigable e intuitivo para el usuario final.

Sumado a lo anterior, es importante destacar que el desarrollo del OVA se llevó acabo en su totalidad bajo la herramienta adobe captívate, la cual se soporta en SWF y HTML5, facilitando la creación e interacción con el material alojado en el objeto virtual de aprendizaje.

A continuación, se presentan los aspectos relevantes en el desarrollo del OVA.

Creación de paneles interactivos

Con el fin de brindar información de manera didáctica, y a través de menús llamativos, se consideró necesario hacer uso de los submenús de interacción, los cuales permitieron dividir el contenido, logrando así tener una mejor estructuración con relación a la información presentada al usuario final. A continuación, se pueden apreciar algunos de los submenús empleados para el despliegue de la información en el OVA.

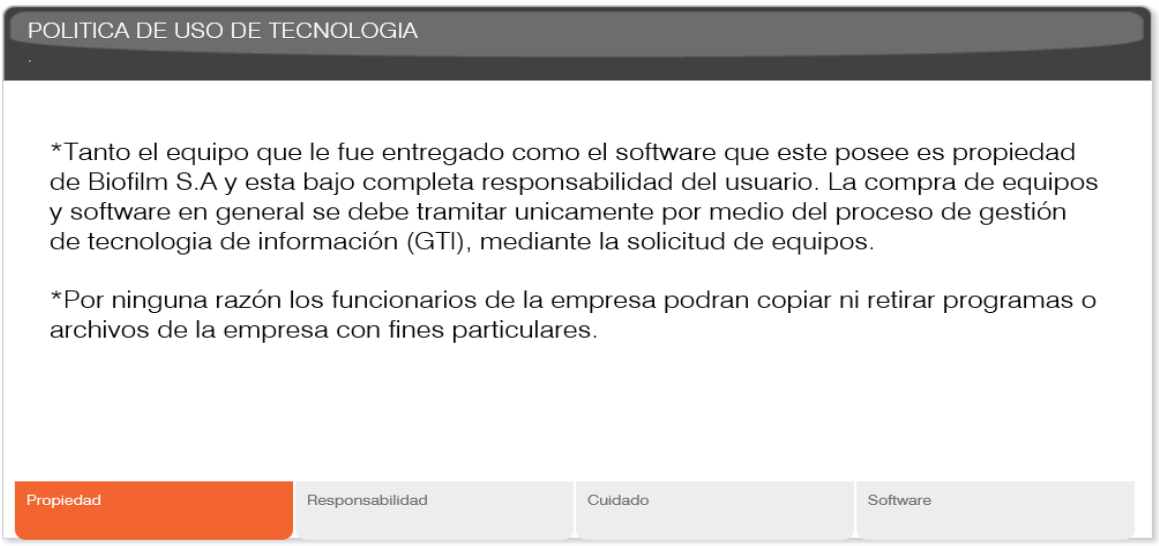


Figura 81 - Submenú de Etiquetas

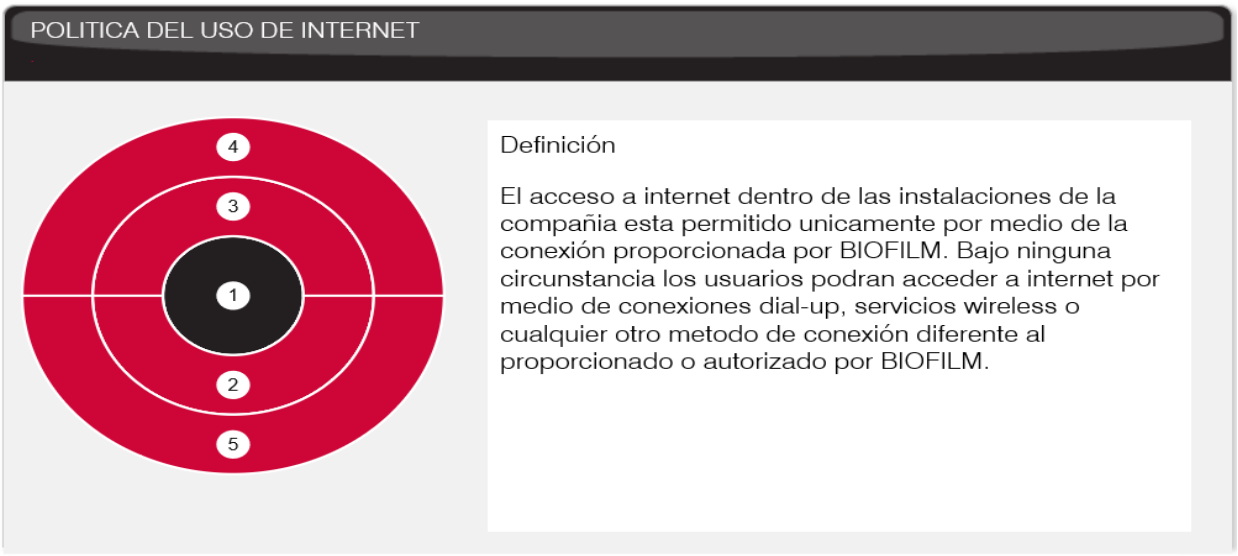


Figura 82 - Submenú circle matrix

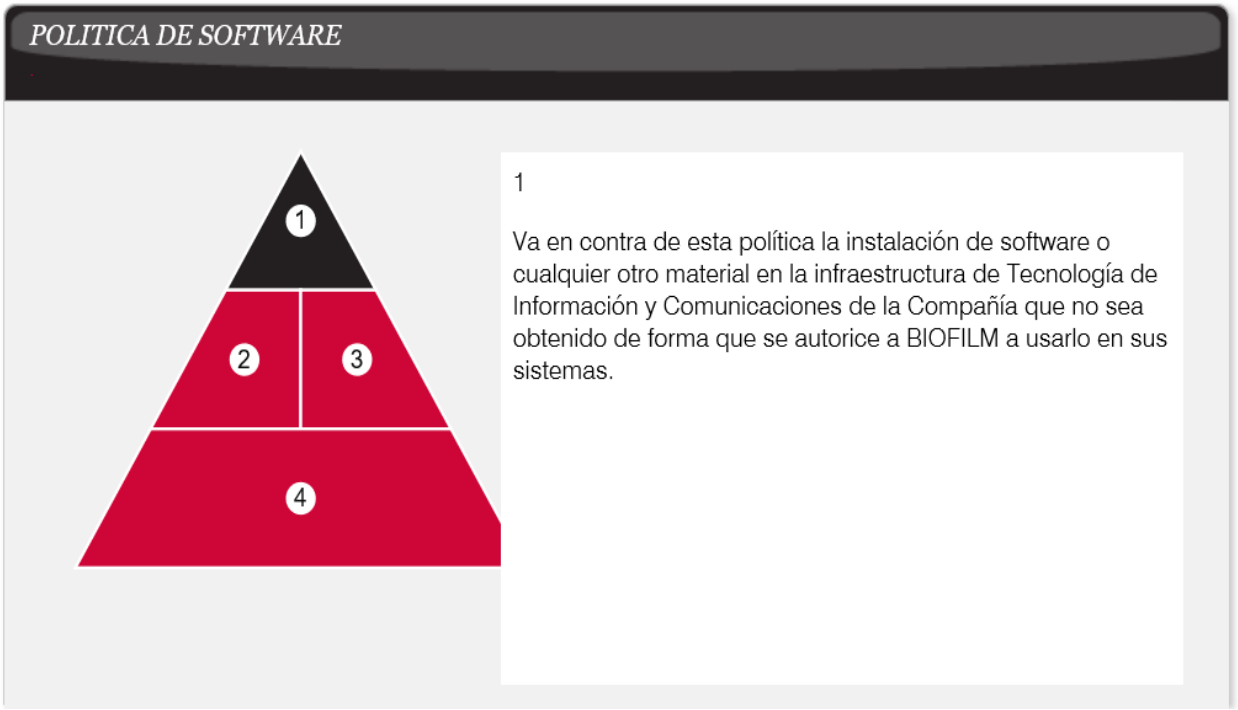


Figura 83 - Submenú pyramid stack

Creación de viñetas informativas

Teniendo en cuenta el objetivo de aprendizaje del OVA, se consideró pertinente presentar el contenido de una forma atractiva al usuario final, razón por la cual se pensó en las viñetas

informativas como una buena elección para garantizar el aprendizaje por parte de los empleados de BIOFILM S.A. A continuación, se presentan algunas de las viñetas empleadas para el despliegue de los contenidos temáticos.

Figura 84 - Viñeta 1

Figura 85 - Viñeta 2

10.5.4. ETAPA DE EVALUACIÓN

En este apartado se presentarán los resultados del proceso de evaluación por el cual paso el OVA, y teniendo en cuenta los requerimientos funcionales y no funcionales se determinara el grado de satisfacción por parte de los empleados y expertos en el tema, para ello se realizaron una serie de pruebas a una muestra de la población de la empresa, con el fin de identificar fortalezas y posibles errores en el desarrollo del OVA, además para verificar si se cumplieron con los requisitos previamente establecidos, y corroborar si en verdad sirve de apoyo el OVA al proceso de aprendizaje de las diferentes políticas de seguridad de la información.

10.5.4.1. EVALUACIÓN PERSONAL DE BIOFILM

Para la realización de las pruebas al personal de BIOFILM S.A., se tomó una muestra significativa de empleados, los cuales fueron designados por parte de la empresa, a estos se les entrego un formulario con preguntas a fin de evaluar la identidad, contenido, usabilidad, navegabilidad, diseño y experiencia de usuario con el OVA.

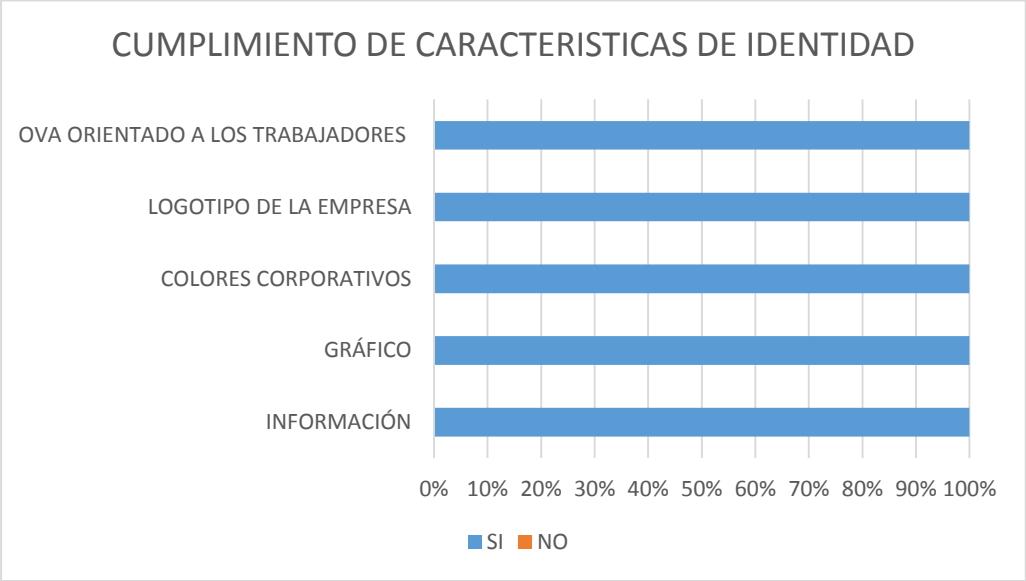
La forma en la cual se llevó a cabo el desarrollo de la prueba consistió en instalar la carpeta contenedora del OVA en los computadores de las personas designadas para realizar dicha prueba, luego se procedió a dar las indicaciones pertinentes para el buen uso y correcto funcionamiento del OVA. Para efectos prácticos la empresa solicito el OVA bajo el formato de HTML5, por ser más fácil en cuanto a su usabilidad. Luego de explicar las indicaciones, se procedió a la ejecución del objeto virtual de aprendizaje, por parte de las personas elegidas para la evaluación, lo cual no requirió de demasiado tiempo. Una vez finalizado el lapso de pruebas, se procedió a la entrega de un formato de evaluación del OVA, el cual estaba realizado a base de preguntas cerradas, en las cuales debían responder Si o No, las preguntas presentes en el formato, se enfocaban a la evaluación de las características de identidad, contenido, usabilidad, navegabilidad, diseño y experiencia de usuario. El formato empleado para esta evaluación, se puede apreciar en el *Anexo N°9.*

10.5.4.2. CONSOLIDACION DE RESULTADOS DE LA PRUEBA AL PERSONAL DE BIOFILM

Teniendo en cuenta los resultados arrojados por el formato de evaluación del OVA, entregado y diligenciando por el personal de BIOFILM S.A. en el marco de las pruebas, se realizó un análisis basado en las características fundamentales del objeto virtual de aprendizaje: identidad, contenido, usabilidad, navegabilidad, diseño y experiencia de usuario.

En el formato entregado había un total de 20 preguntas, las cuales estaban repartidas de la siguiente forma: 5 preguntas de identidad, 4 de contenido, 2 de usabilidad, 3 de navegabilidad, 5 de diseño, y 1 de experiencia de usuario. Las respuestas a cada una de estas preguntas se agruparon teniendo en cuenta sus características, además se graficaron las preguntas con el fin de tener mayor claridad en los resultados.

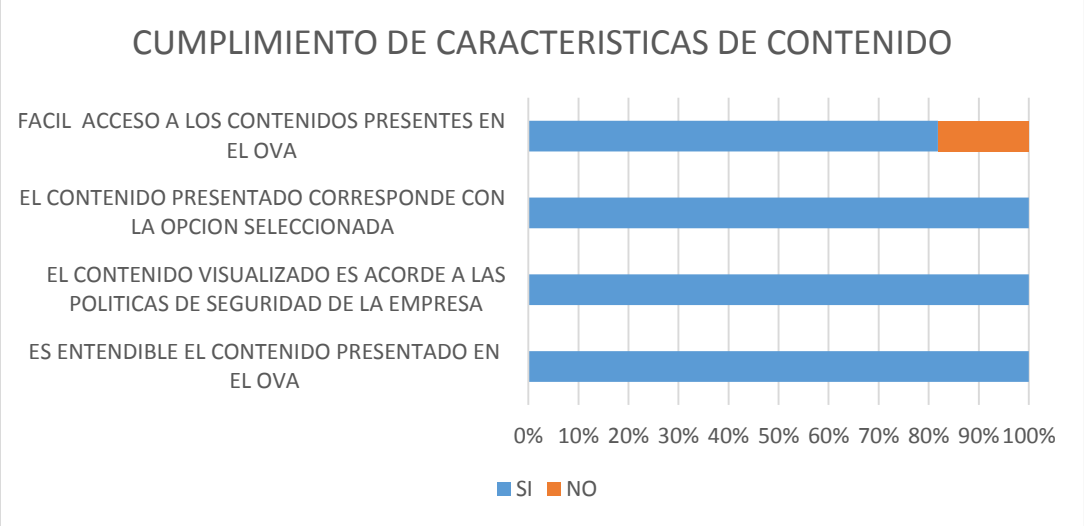
La información que se muestra en la parte izquierda de cada fila de las siguientes gráficas, corresponde a un resumen concreto de una pregunta de la característica en cuestión.



Gráfica 7. Cumplimiento de la característica de identidad en el OVA. (Fuente: encuestados)

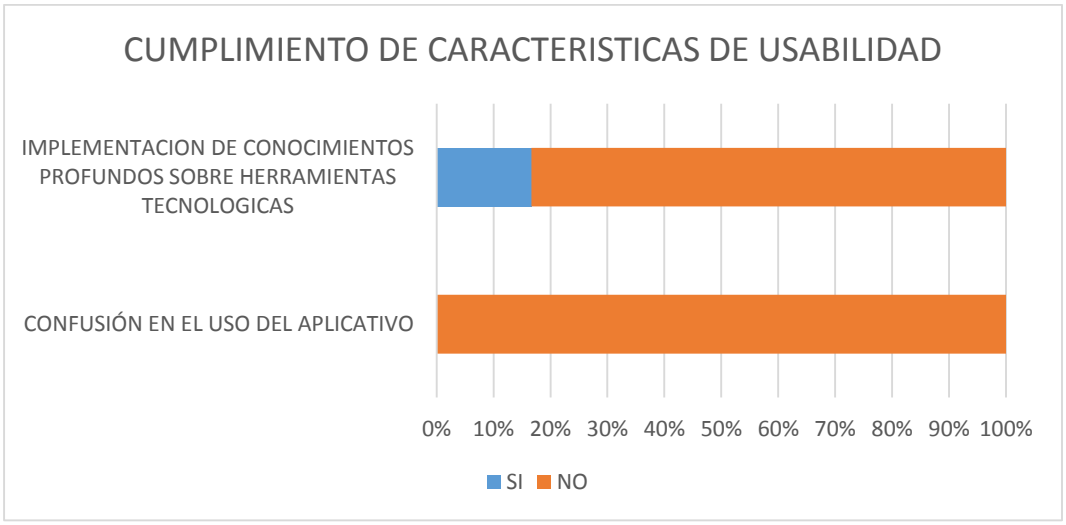
Considerando la muestra tomada para la elaboración de la prueba, el 100% de ella valida el cumplimiento de la característica de identidad estipulada en el formato a través de las distintas preguntas. Lo cual satisface las expectativas planteadas al inicio de la evaluación, debido a que

dicha característica es importante para orientar a los usuarios finales a la hora de hacer uso de la herramienta de aprendizaje.



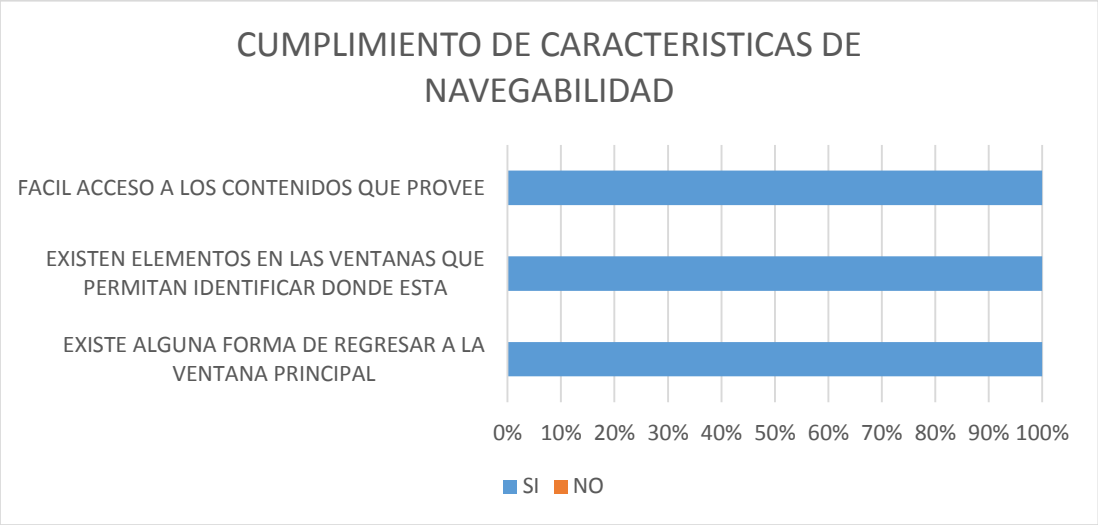
Gráfica 8. Cumplimiento de la característica de contenido. (Fuente: encuestados)

Teniendo en cuenta los resultados arrojados por medio de la gráfica anterior, podemos evidenciar que en términos generales se cumplió a cabalidad con la característica de contenido en el objeto virtual de aprendizaje. Sim embargo solo a una persona se le dificulto el acceso a los contenidos desplegados en el OVA, por lo que se hizo necesario revisar el funcionamiento mismo de este y corroborar que todo estuviera en orden, a su vez ajustar pequeños detalles que optimizaran el funcionamiento de la herramienta virtual de aprendizaje.



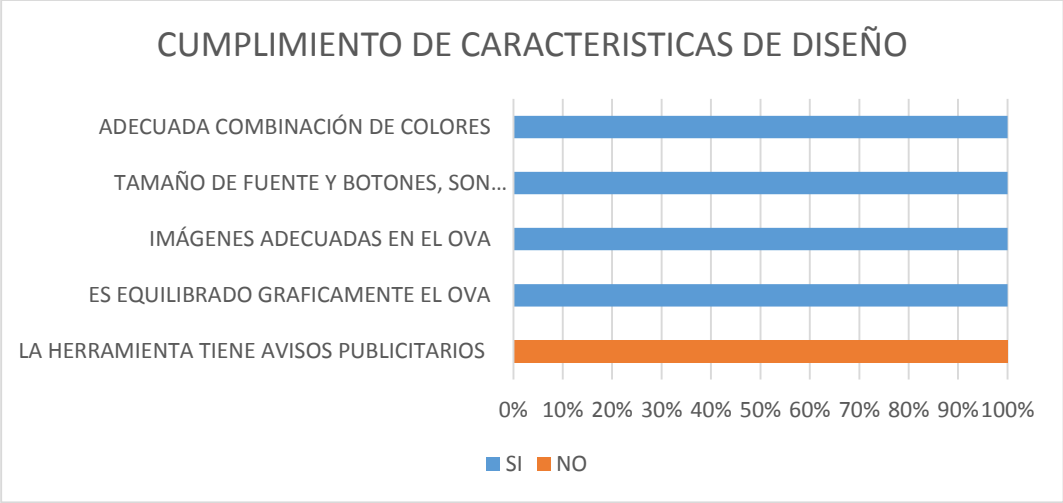
Gráfica 9. Cumplimiento de la característica de usabilidad en el OVA. (Fuente: encuestados)

A partir de la gráfica presentada anteriormente y en el marco de las preguntas correspondientes a la característica de usabilidad, podemos evidenciar que el OVA, no resultó confuso para los usuarios finales, favoreciendo de esta forma al NO. Pero con relación a la implementación de conocimientos profundos sobre herramientas tecnológicas, una pequeña parte de la muestra tomada, considero necesarios conocimientos adicionales para la utilización del objeto virtual de aprendizaje.



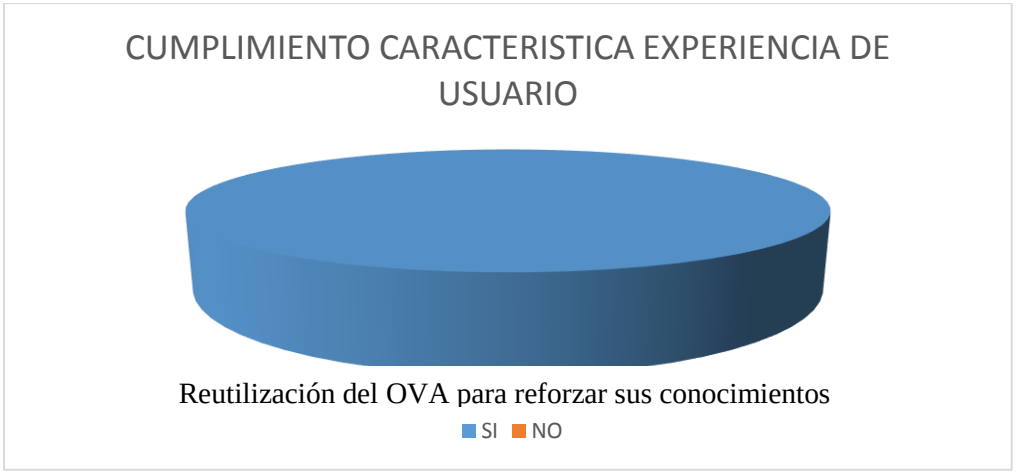
Gráfica 10. Cumplimiento de la característica de navegabilidad en el OVA. (Fuente: encuestados)

La grafica anterior revela el fácil acceso al OVA y a sus contenidos multimediales, además queda en evidencia la existencia de elementos de referencia que permiten ubicar al usuario a la hora de hacer uso de la herramienta. No obstante, queda evidenciado la buena navegabilidad en el OVA, al tener un SI rotundo por parte de las personas seleccionadas en la empresa para el proceso de evaluación.



Gráfica 11. Cumplimiento de la característica de diseño del OVA. (Fuente: encuestados)

Dentro de la característica de diseño, y conforme a los resultados obtenidos en las pruebas, podemos notar que se cumplieron con las expectativas previas a la etapa de evaluación, debido a que los usuarios finales, consideraron en términos generales que el OVA cuenta con la normatividad a nivel de diseño, para ser empleado al interior de la empresa. Por otro lado, se obtuvo un NO como respuesta positiva a la pregunta de ¿El OVA tiene banners o avisos publicitarios?, dicha respuesta brinda tranquilidad y confiabilidad al usuario final al momento de hacer uso del objeto virtual de aprendizaje.



Gráfica 12. Cumplimiento de la característica de experiencia de usuario. (Fuente: encuestados)

Como última característica encontramos la experiencia de usuario, la cual reúne las anteriores, y nos permite saber si en realidad el usuario final quedo satisfecho con la solución desarrollada por parte de los investigadores del proyecto, a través de esta última característica se busca conocer si

el usurario haría uso nuevamente del OVA, con el fin de reforzar sus conocimientos concernientes a las políticas de seguridad de BIOFILM S.A. Por lo anterior, y teniendo en cuenta el grafico presentado previamente, se puede evidenciar que todos los empleados designados para la prueba, utilizarían nuevamente el OVA para fortalecer sus conocimientos, debido a que les pareció una herramienta sencilla y de fácil uso.

Teniendo en cuenta los resultados presentados en cada una de las gráficas anteriores, podemos concluir en términos generales lo siguiente:

- Considerando las expectativas y metas trazadas en el inicio del desarrollo del objeto virtual de aprendizaje y basándonos en los resultados obtenidos por parte de los empleados de BIOFILM S.A, se concluye que el desarrollo del OVA fue todo un éxito, puesto que para todos los usuarios el OVA cumple con las especificaciones técnicas exigidas por la empresa, además proporciona un fácil manejo por ser una herramienta sencilla y de fácil uso. Más sim embargo se hicieron pequeñas observaciones con el fin de fortalecer a futuro el OVA y hacer de este una herramienta escalable.
- Al momento de realizar las pruebas con el OVA, se encontró con un inconveniente. Este se debía a que el objeto virtual de aprendizaje no corría correctamente en todos los navegadores, principalmente en Google Chrome y Mozilla Firefox, mientras que en Internet Explorer no todas sus versiones lo ejecutaban como era debido. En respuesta a este percance se optó por utilizar el navegador Microsoft Edge, el cual reunía los complementos necesarios en sus diferentes versiones, permitiendo así usar el OVA de la forma correcta.
- De acuerdo a los resultados, se puede afirmar que el OVA es una buena herramienta a la hora de fortalecer los conocimientos con relación a las políticas de seguridad de la información en BIOFILM S.A., cumpliendo de esta forma con las expectativas a nivel de aprendizaje.
- Con base a las pruebas, los empleados declararon que el OVA posee un alto grado de usabilidad, debido a que es sencillo y no amerita conocimientos avanzados de tecnología. Además, también expresaron que el diseño estético es ideal, agradable a la vista y posee contenido gráfico apropiado para la temática tratada.

- Del mismo modo los empleados de BIOFILM S.A afirmaron que al emplear el OVA, este no es confuso, debido a que cuenta con los colores corporativos, además tiene el logotipo de la empresa, e imágenes claras que permiten saber la temática tratada. Adicional a eso existen referencias en las distintas ventanas del OVA que permiten ubicar al usuario final y evitar que pueda confundirse o dificultar la navegabilidad en el objeto virtual de aprendizaje.

10.5.5. ETAPA DE IMPLANTACIÓN

Para llevar a cabo esta etapa en el desarrollo del OVA, se le entrego a BIOFILM S.A un archivo HTML correspondiente al OVA, en el cual estaban contenidos los diferentes componentes que permiten la interacción entre el usuario y los contenidos temáticos otorgados para la adquisición de conocimientos.

Atendiendo a las circunstancias ajenas al desarrollo del proyecto, se modificó la puesta en producción del OVA, que inicialmente se había estipulado en los requisitos, entregar e implantar en la plataforma LMS, pasando a un formato de HTML alojado en un Servidor de Archivos propio.

Una vez obtenido el archivo HTML mediante la herramienta de creación de OVA's, se realizaron una serie de configuraciones para lograr la puesta en producción de la herramienta de aprendizaje.

10.5.5.1. CONFIGURACIONES DE PRODUCCIÓN

Atendiendo a las necesidades de la empresa, se optó por alojar el OVA en un Servidor de Archivos propio de BIOFILM S.A, esto teniendo en cuenta que no era conveniente anexar el OVA al LMS empresarial, debido a que era incierto con el tiempo la utilización de dicha plataforma en la empresa, puesto que esta se encontraba en un proceso transitorio a nivel de los distintos departamentos administrativos. Razón por la cual se solicitó a los investigadores generar el OVA a un formato HTML, y que este pudiera ser ejecutado con facilidad por los empleados.

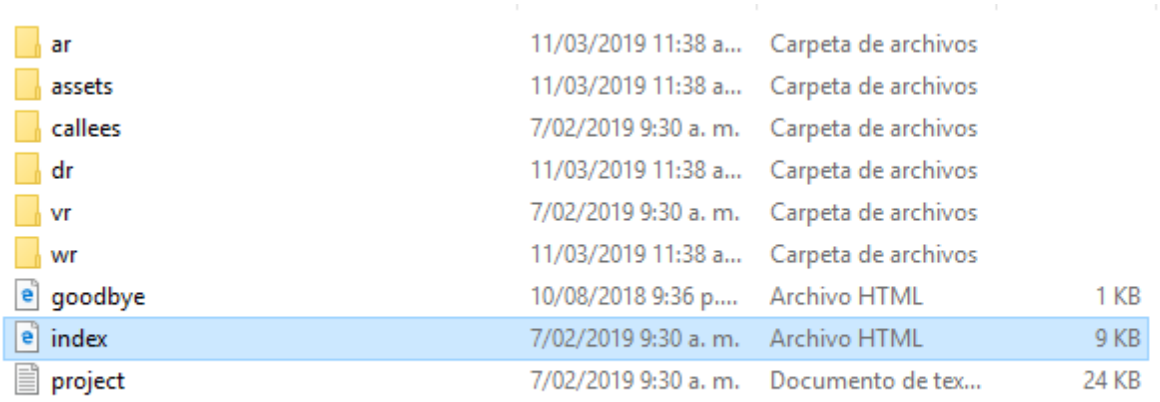


Figura 86. Carpeta contenedora del OVA. (Fuente: Investigadores)

En la imagen anterior se puede apreciar el OVA bajo el formato de HTML, junto a sus diferentes componentes que permiten ejecutarlo de forma correcta. Para ejecutar el OVA, se debe ingresar al archivo **índex,** el cual nos llevara directamente al menú inicial del objeto virtual de aprendizaje, sin requerir de alguna configuración o complemento adicional.

10.6. APLICATIVO WEB PARA LA ADMINISTRACIÓN DE LA APLICACIÓN MÓVIL

Uno de los requisitos planteados dentro del desarrollo del aplicativo móvil (RF4), se basa en la creación de una plataforma que sirva como administración y alimentación de las funciones de la APP. Para la realización de este requisito, se creó un aplicativo web basado en las tecnologías de Angular para el desarrollo de la parte visual y la interacción del usuario, MySQL como gestor de bases de datos y almacenamiento de información, y Node.js para la disponibilidad de la información y el manejo de datos entre las interfaces de usuario y la base de datos. La separación de este requisito radicó en la facilidad de uso que tiene un aplicativo web con respecto a uno móvil, en el manejo y llenado de los formularios que el administrador del aplicativo móvil debe diligenciar para el mantenimiento del mismo.

El desarrollo de la aplicación web se realizó bajo tres parámetros que permitieron la segmentación del proyecto: 1) Modelo de negocio; 2) Modelo de diseño; 3) Modelo de implementación.

En el marco del modelo de negocio, se empleó el modelo de dominio para representar la forma en que el administrador designado por la división de recursos humanos, realiza las tareas concernientes con la gestión de los procesos operacionales que buscan la adquisición de conocimientos sobre las políticas de seguridad que la empresa posee. En el modelo, se establecen las operaciones, acciones y entes reales que en la empresa existen, relacionados con la gestión de las políticas de seguridad.

Como método didáctico de adquisición de conocimientos sobre las políticas de seguridad, la empresa BIOFILM S.A. en compañía de dos estudiantes de la Universidad de Cartagena, desarrollaron un aplicativo móvil como medio de aprendizaje de las normatividades. Dicho aplicativo es utilizado por los empleados de la empresa, y la gestión del mismo queda a disposición del administrador asignado por la división de Recursos Humanos. Con la administración del aplicativo móvil utilizado por los empleados de la empresa, para evaluar las políticas de seguridad, se promueve la continuidad del negocio para beneficio de la empresa. Bajo los anteriores supuestos, se desarrolló el modelo de dominio en cuestión.

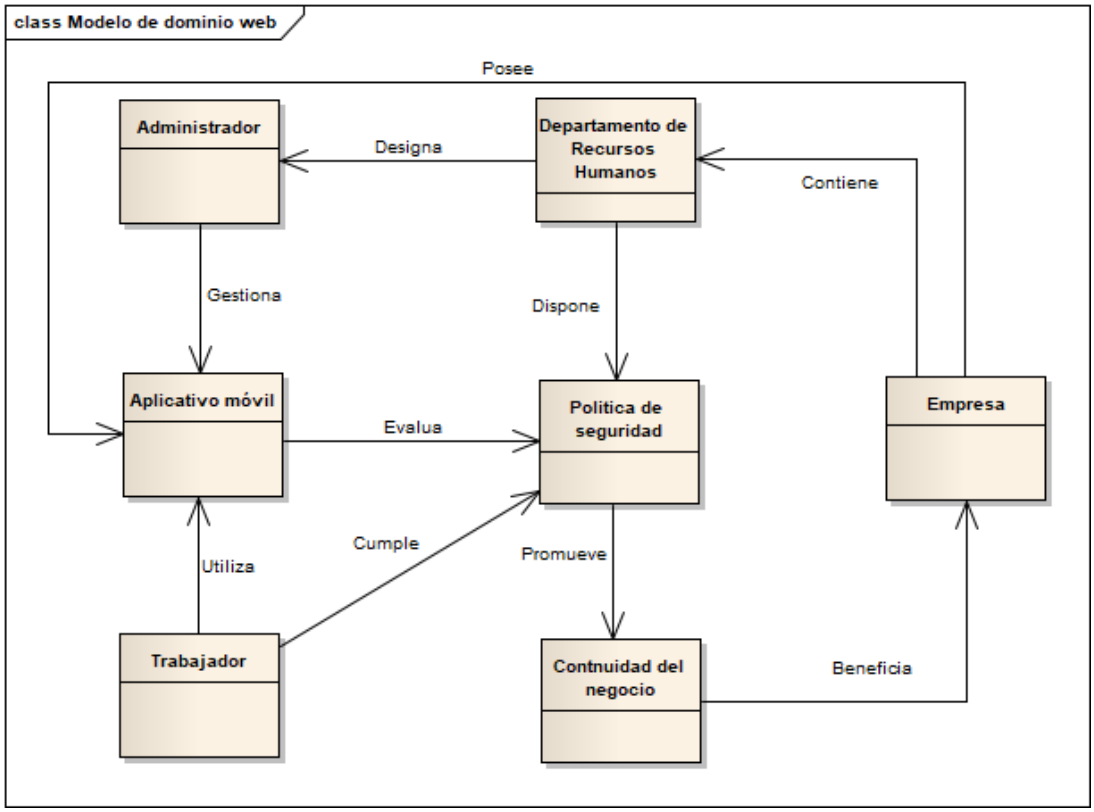


Figura 87. Modelo de dominio del aplicativo web. (Creado por los investigadores).

Del mismo modo, enmarcado en el modelo de negocio y basándose en lo anterior, se desarrolló el diagrama de casos de uso del mundo real. En este diagrama se reflejan los procesos, funciones y/o consecuencias (casos de uso) que desarrolla el administrador para la gestión de los deberes concernientes con la seguridad de la información.

El administrador es el actor principal, debido a que él se encarga, desde la división de Recursos Humanos, de crear estrategias para la divulgación, aprendizaje y evaluación de las políticas de seguridad.

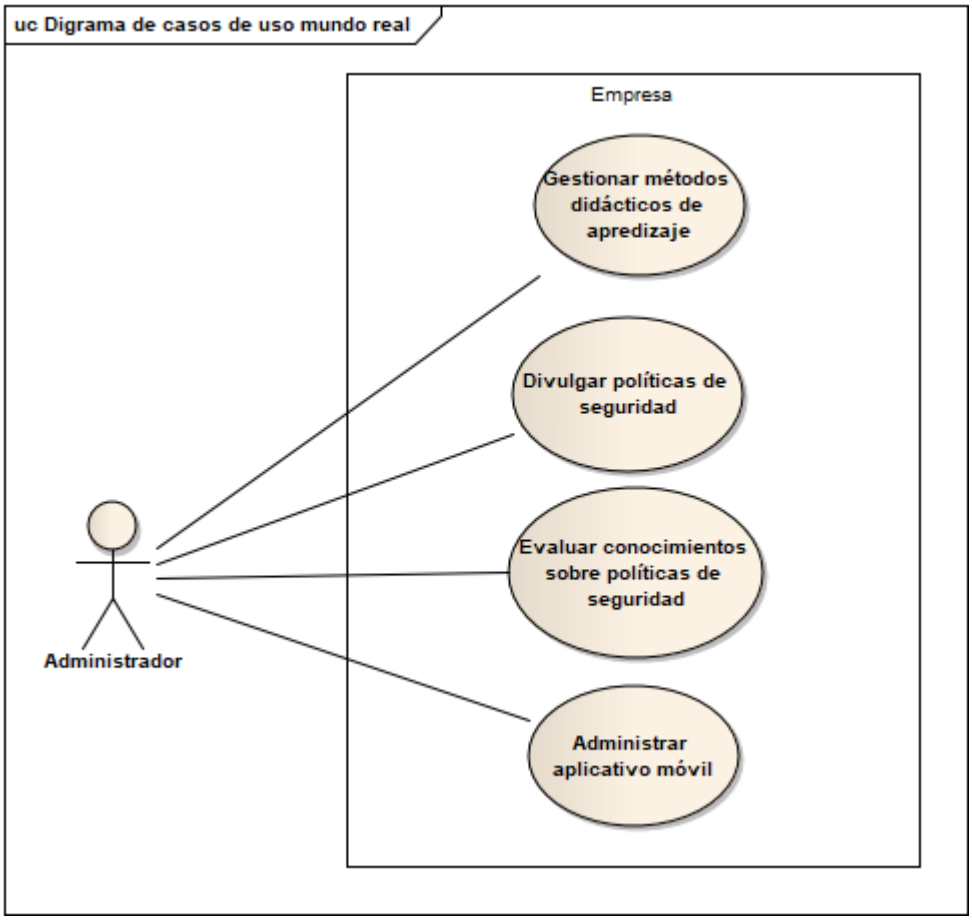


Figura 88. Diagrama de casos de uso del mundo real del aplicativo web. (Creado por los investigadores).

Como segunda etapa del desarrollo, en la creación del modelo de diseño se implementaron los diagramas que demuestran la solución desde el punto de vista técnico. Estos diagramas son: Diagrama de componentes, diagrama de clases, diagrama general de casos de uso, y diagrama de entidad relación.

Para la creación del diagrama de componentes, se utilizó el patrón arquitectónico de capas, que permite generar segmentaciones y paquetes que representan la solución, agrupados cada uno en su capa correspondiente. Este diagrama muestra las características fundamentales con las que cuenta el aplicativo web para la gestión de la aplicación móvil. La agrupación de los componentes que se presentan, conforma en su totalidad, la aplicación web.

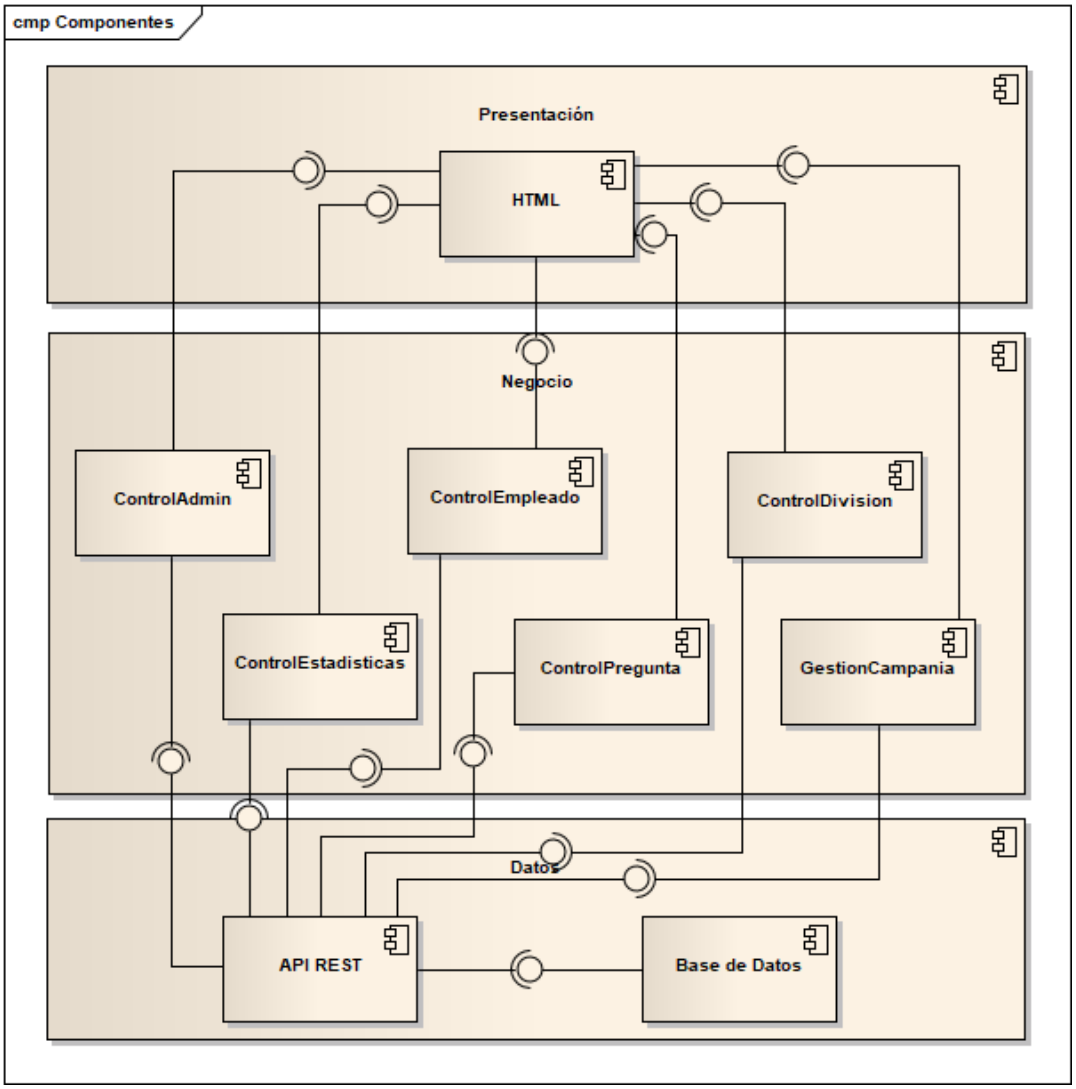


Figura 89. Diagrama de componentes del aplicativo web. (Creado por los investigadores).

El patrón arquitectónico utilizado, propone tres capas fundamentales para agrupar los componentes. En la capa de presentación se desarrollan los componentes visuales y de interacción del usuario final con los componentes internos. Aquí se define HTML como el componente principal que dispone la tecnología Angular para la creación de las interfaces y vistas que el usuario utiliza.

La capa de negocio recoge las acciones y peticiones realizadas por el usuario, brindando respuesta mediante un mecanismo basado en la búsqueda de información y utilización de los servicios dispuestos por la API REST presente en la capa de datos. Los componentes establecidos en la capa de negocio, tienen la finalidad de ejercer control sobre las campañas, los

usuarios, las estadísticas, las preguntas y grupos de preguntas, y las divisiones, es decir, atienden la lógica para la gestión adecuada de ambos aplicativos.

Del mismo modo, el patrón arquitectónico de capas permitió la realización del diagrama de clases en el cual se detallan los componentes de cada capa, planteados en el diagrama de componentes. También, se ilustra la forma de interacción entre cada capa, las dependencias y funcionalidades presentes, observadas desde la perspectiva de la programación.

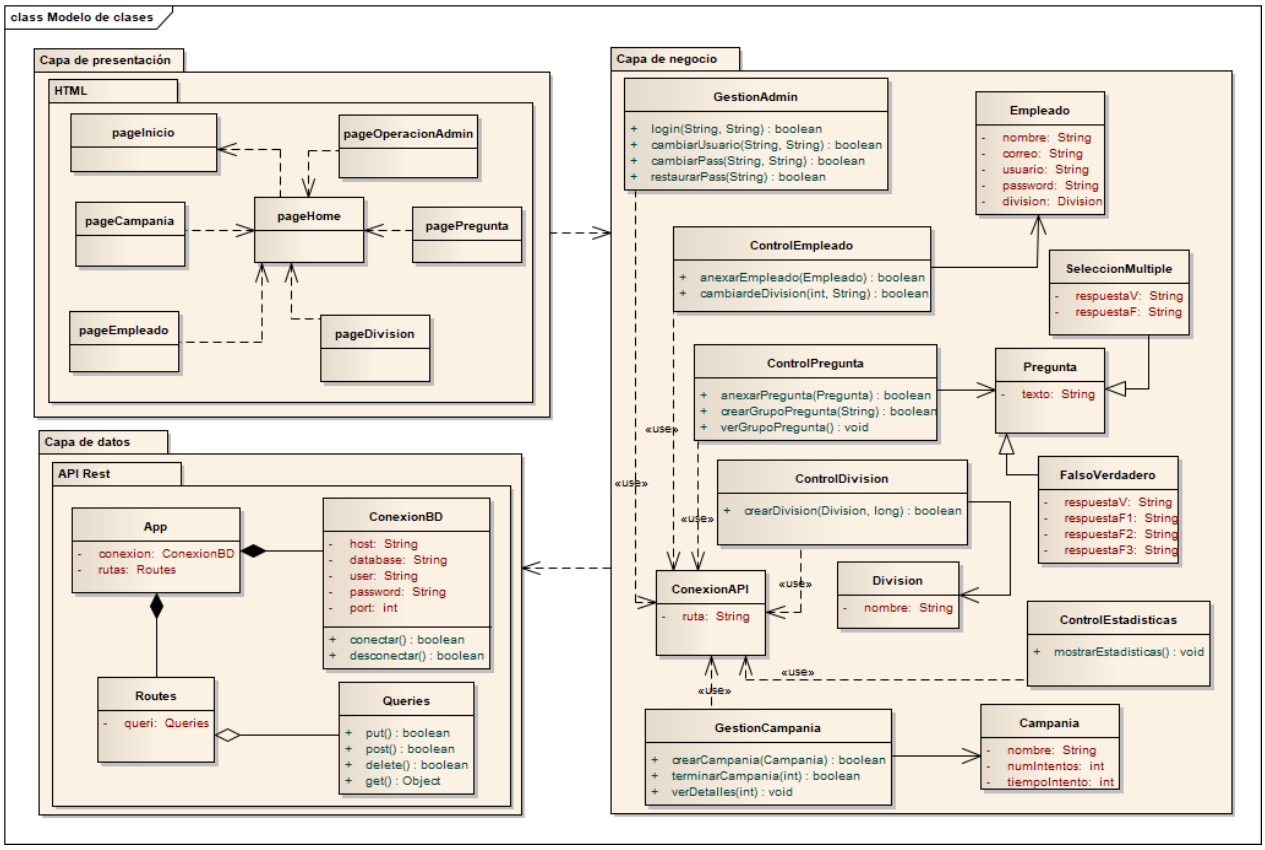


Figura 90. Diagrama de Clases de la aplicación web. (Creado por los Investigadores).

En la capa de presentación, están definidas las páginas que sirven para representar la información y la interacción del usuario. Mediante estas páginas, el administrador realiza acciones que la capa de negocio recoge para brindar la respectiva respuesta. Cada una de estas acciones o peticiones, tienen un efecto sobre los datos alojados en la base de datos, por tanto, la capa de negocio tiene acceso a la capa de datos para hacer el manejo de la información correspondiente.

Por otro lado, el diagrama general de casos de uso muestra de manera general las operaciones y acciones necesarias que el administrador realiza para la gestión adecuada del aplicativo móvil. Estos casos de uso, tienen relación directa con las funcionalidades que presenta la APP móvil.

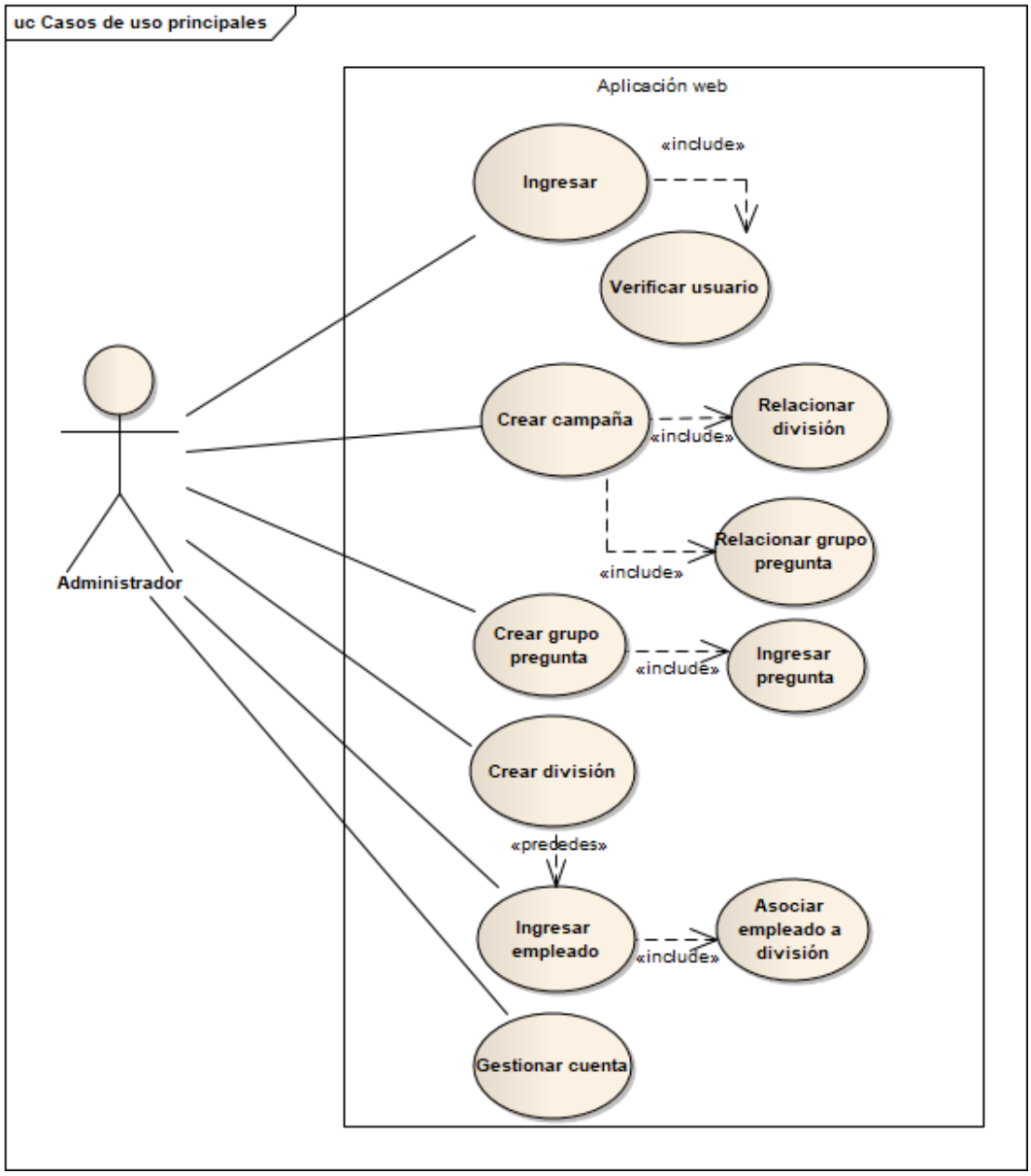


Figura 91.Diagrama general de casos de uso de la aplicación web. (Creado por los Investigadores).

Para el correcto almacenamiento de la información resultante de las operaciones y acciones realizadas por el administrador al usar el aplicativo web, se necesita una base de datos que recopile y almacene todas las características fundamentales de las dos aplicaciones, web y móvil.

Con la finalidad de cumplir lo anterior, se creó una base de datos soportada en el diagrama de entidad relación de la siguiente figura:

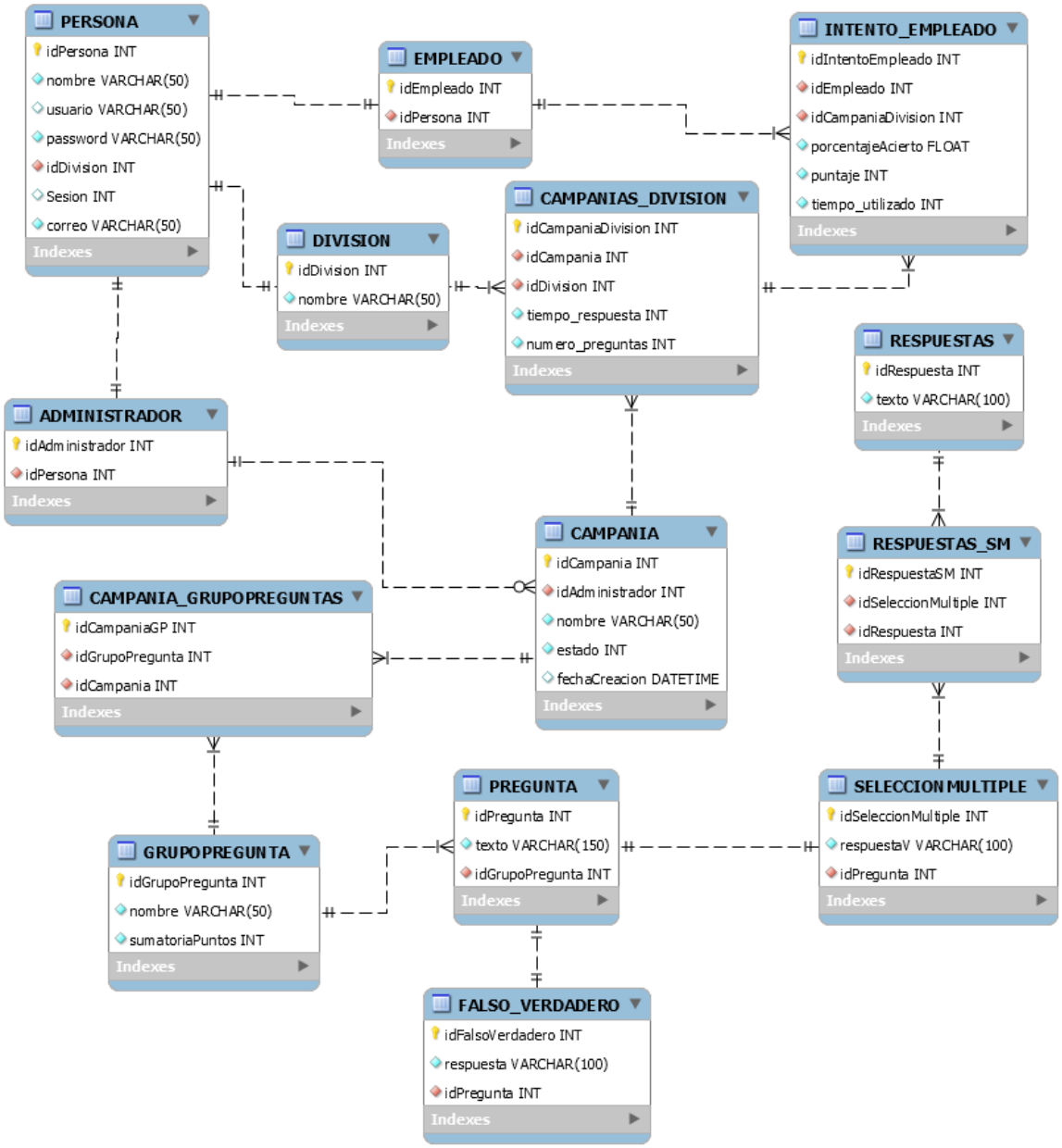


Figura 92. Diagrama de entidad relación del aplicativo web. (Creado por los investigadores).

Como último procedimiento en la etapa de producción del aplicativo web, se diseñó el modelo de implementación a partir de la vista de desarrollo en forma de diagrama de paquetes, y la vista de despliegue representada mediante un diagrama de despliegue.

El diagrama de paquetes se creó basándose en el patrón arquitectónico por capas. Este diagrama agrupa y muestra las segmentaciones lógicas que se realizaron para desarrollar el aplicativo web. Cada uno de los paquetes mostrados en las capas, se desarrollaron independientemente para agilizar el proceso de producción. Las flechas que relacionan cada capa, indican la forma en que se hizo la integración de los distintos paquetes para conformar la totalidad de la aplicación.

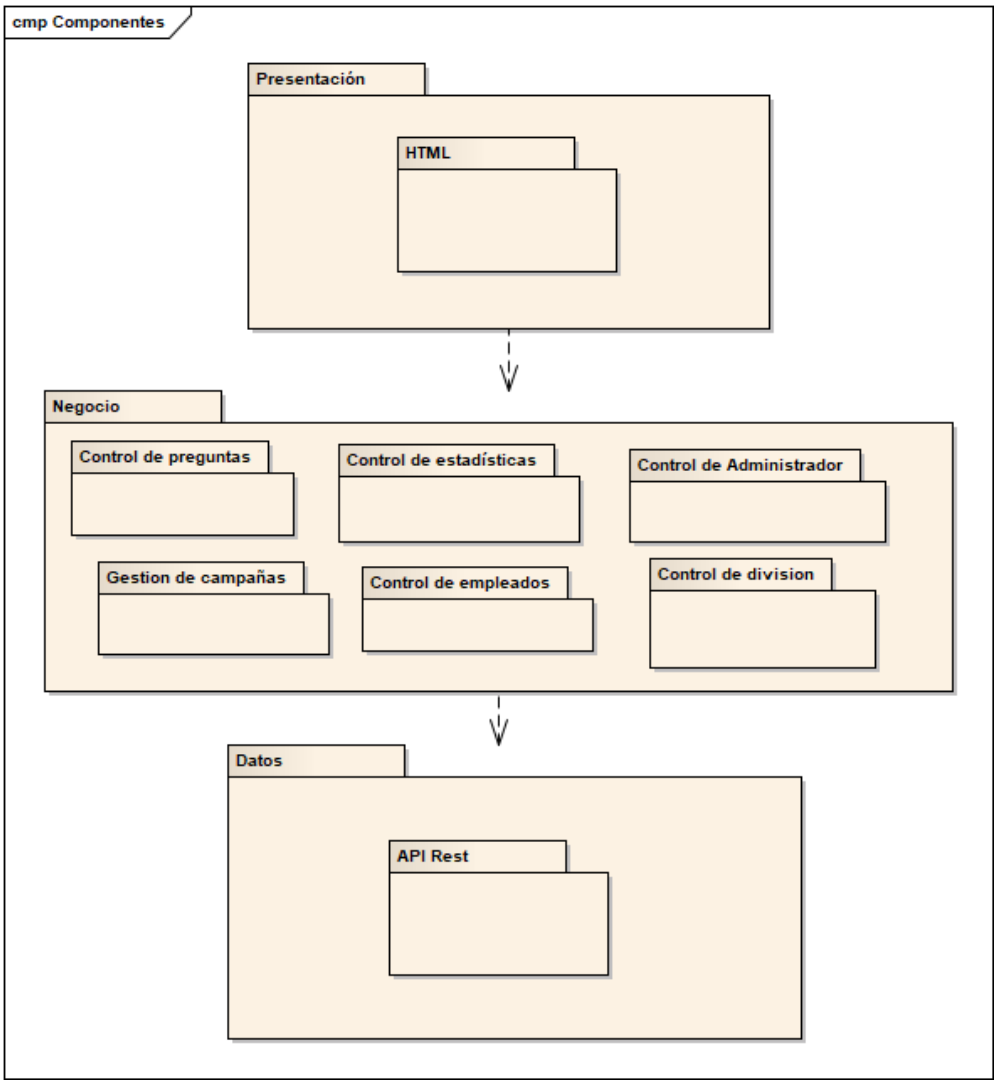


Figura 93. Modelo de implementación del aplicativo web representado a partir de un Diagrama de paquetes. (Creado por los Investigadores).

En la vista de despliegue, se muestra la distribución física que tienen los procesos y componentes del aplicativo web en el ambiente de producción, representados como nodos. El nodo WEB,

contiene la ejecución de la aplicación que consume los servicios de la base de datos alojada en un servidor virtual de Microsoft Azure, el cual representa el nodo WEB Server.

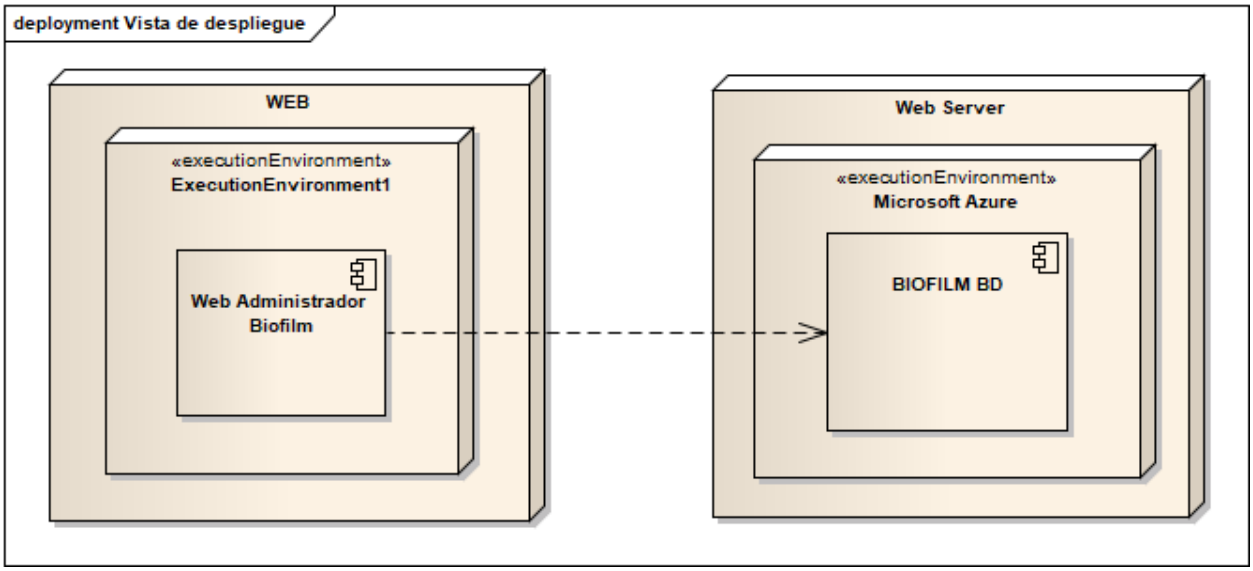


Figura 94. Vista de despliegue de la aplicación web, representada por un Diagrama de despliegue. (Creado por los Investigadores).

11. CONCLUSIONES

Como resultado de la realización de este proyecto, se logró la ejecución de todos los objetivos planteados, materializados en dos controles como mecanismos para mejorar los procesos desarrollados por los dominios de RRHH y Telecomunicaciones de la empresa BIOFILM S.A., concernientes con la seguridad de la información. Estos controles radicaron en la implantación de una herramienta SIEM en la infraestructura de red, y en la creación de una estrategia para la enseñanza/aprendizaje/evaluación de las políticas de SdI que la empresa maneja, basada en la creación de un aplicativo móvil y la creación de un Objeto Virtual de Aprendizaje (OVA).

A partir de lo anterior, se pueden mencionar las siguientes conclusiones sobre la elaboración del proyecto:

- La metodología mixta utilizada para la elaboración del proyecto, permitió la adquisición adecuada de las herramientas y recursos pertinentes para la realización y cumplimiento de los objetivos propuestos que aprobaron efectuar la finalidad del proyecto. Esta metodología se basó en el desarrollo por objetivos, dentro de los cuales, para cumplir con ellos se hizo necesario la adopción de una investigación aplicada bajo documentos, reuniones, entrevistas y pruebas, y además de la utilización de otros tipos de metodologías puntuales para los objetivos de desarrollo software.
- En el proceso de implantación y configuración de la herramienta SIEM, se destacó un aspecto que generó cambios drásticos al momento de desarrollar tareas para la realización de este objetivo. Este aspecto radicó en los cambios a nivel administrativo y gerencial que sufrió la empresa al momento de ser adquirida por nuevos dueños, debido a que esto trajo consigo la reestructuración lógica de la infraestructura de red de la empresa para la realización del empalme con los nuevos clientes y socios, procesos que impedían la utilización por parte de terceros del Switch Core, el Servidor de Archivos, y el Directorio Activo. Por lo cual, los investigadores de este proyecto no pudieron acceder a dichos dispositivos para continuar con las configuraciones pertinentes.

  Dentro de las configuraciones que no se pudieron realizar, estuvieron los eventos a auditar por la herramienta SIEM establecidos en el acta de recolección de requisitos

presente en el *anexo 6*. Debido a que estos procesos se debían controlar y administrar desde el servidor OSSIM a partir de la configuración del Directorio Activo y sus eventos enviados al servidor.

- En el objetivo de implantación de la SIEM no se utilizaron encuestas o valores cuantitativos para la evaluación de la funcionalidad de la herramienta, por lo cual no se puede analizar en función de estos datos. Los parámetros que se pueden analizar son: el método de configuración, el funcionamiento con la activación de los diferentes plugins, y los resultados proporcionados por los informes que genera OSSIM en producción.
- La implantación de la herramienta SIEM en la infraestructura de red, le brindó al dominio de RRHH un mecanismo para el fortalecimiento de las operaciones realizadas en cuestión de seguridad de la información, con la cual se le otorga seguridad a todas las operaciones, transacciones, servicios y peticiones que se realizan mediante la red de la empresa y sus canales de acceso hacia la Internet, para permitir que los datos e información utilizada, conserve su integridad, seguridad, disponibilidad y confidencialidad. Del mismo modo, permite disminuir la exposición y daños sobre la información sensible e importante de la empresa, almacenada en las bases de datos y servidores que la misma utiliza.
- La estrategia creada para la enseñanza/aprendizaje/evaluación de las políticas de seguridad de la información, permite que el dominio de RRHH tenga dos instrumentos complementarios que brindan facilidad para orientar y capacitar a los empleados de la empresa, sobre la importancia de las políticas y su puesta en marcha. El OVA desarrollado es utilizado para la enseñanza y el aprendizaje de las políticas, y el aplicativo móvil se emplea para la evaluación de las mismas.
- El aplicativo móvil, que inicialmente se había concebido para ser simplemente informativo, en el desarrollo de los objetivos del proyecto cambió su intención principal. Por petición de la empresa éste pasó a ser evaluativo, el cual es empleado como un juego de preguntas que sirve para, por medio de las preguntas, identificar las fortalezas de los conocimientos adquiridos por parte de los trabajadores, sobre las políticas de SdI.

- Del mismo modo, el OVA cambió su razón con relación al objetivo 5 establecido en el trabajo, debido a que se había estipulado para ser una herramienta de divulgación y evaluación de los conocimientos sobre las políticas de la SdI, la cual fue cambiada por petición de la empresa, a ser una herramienta solo para la divulgación y de impartición de conocimientos de dichas políticas, es decir, la parte evaluativa sería delegada al aplicativo móvil.
- El aplicativo móvil con el cumplimiento de las características de identidad, contenido, usabilidad, navegabilidad, diseño y experiencia de usuario, logra ser una herramienta adecuada para que, por medio de la evaluación de los conocimientos adquiridos durante el uso del OVA, los empleados de la empresa potencialicen y fortalezcan el aprendizaje y el conocimiento previo, debido a que pone a disposición una herramienta visual y didáctica, basada en la correcta distribución de contenidos, diseño y dinamicidad. Lo anterior, complementado con la existencia del aplicativo web para la gestión y administración adecuada de los contenidos mostrados, le otorga al dominio de RRHH una herramienta qué, además de evaluar los conocimientos de los empleados en cuestión de seguridad de la información, permite retroalimentar la forma en que se suministra la información y los contenidos para impulsar el aprendizaje y conocimiento de las políticas en los empleados de la empresa.
- Dentro de los requisitos estipulados en el desarrollo del aplicativo móvil, se debía realizar la creación de un perfil de administrador, el cual no necesariamente debía se móvil. Para el cumplimiento de este objetivo, los investigadores de este proyecto decidieron crear un aplicativo web, debido a que brinda mayor facilidad y comodidad para el usuario administrador, al momento de llenar los formularios, y exportar e importar los archivos pertinentes para la gestión del aplicativo móvil. El desarrollo de este aplicativo web, ameritó la creación de un nuevo objetivo para este trabajo, enumerado como el sexto objetivo, y presente en la etapa de resultados.
- La elección de las tecnologías para la elaboración de cada uno de los controles, fue un punto importante dentro del desarrollo del proyecto, dado que esta escogencia permitió la adquisición de nuevos conocimientos, basados en los previos que los investigadores poseían. Lo anterior permitió la disminución en el tiempo de creación del aplicativo móvil, el aplicativo web, y el OVA.

- Con la elección de IONIC como tecnología para la elaboración del aplicativo móvil, se obtuvo un resultado anexo no contemplado en los requisitos del aplicativo, ni en los objetivos específicos del proyecto. Este resultado hace referencia a la creación del aplicativo móvil también para la plataforma IOS, distinta a la estipulada en los requisitos, la cual fue Android. La aplicación orientada hacia esa plataforma, también fue entregada a la empresa para que disponga de ella.
- La interacción constante con los empleados que la empresa designó para ayudar y orientar en las distintas tareas realizadas a lo largo del desarrollo del proyecto, permitió que se hicieran revisiones parciales que ayudaron a fortalecer los procesos pertinentes y la obtención de los resultados esperados. Del mismo modo, sirvieron de apoyo y acompañamiento en las estrategias adoptadas, y para el cumplimiento de la metodología y los objetivos propuestos.
- La realización de este proyecto fortaleció la relación entre la Universidad de Cartagena y BIOFILM S.A., para la realización de trabajos e investigaciones conjuntas entre ambas instituciones, que ayuden a potencializar el conocimiento de los investigadores de los proyectos, además del intercambio de conocimientos que permiten aumentar el nivel académico de la Universidad y generan beneficios para la empresa. De igual modo, las documentaciones y los resultados formales del trabajo realizado, contribuyen a la parte científica de la Universidad y la impulsan como academia.

12. RECOMENDACIONES

Se deben tener en cuenta las siguientes recomendaciones para la adecuada utilización de los controles desarrollados en este proyecto:

- Cada vez que se necesite colocar en funcionamiento el aplicativo móvil, el administrador deberá encender el servidor donde se encuentra la base de datos y la API creada para suministrar la información pertinente a los aplicativos.
- En el aplicativo móvil, el administrador al momento de finalizar una campaña, debe ingresar al aplicativo web y seleccionar la campaña a finalizar. Luego, debe decidir la cantidad de ganadores pertenecientes a la campaña y notificarles a los usuarios pertinentes.
- Para la utilización de los aplicativos en la segunda planta de la empresa, ubicada en Altamira, México, solo deben crear las divisiones que allá existen, y en caso de ya existir la división en la base de datos, se debe anexar un distintivo para distinguir la división correspondiente de la planta de Cartagena, con la de Altamira.
- Si el administrador de red de la empresa desea crear cambios o anexos en la configuración de la herramienta SIEM implantada, se recomienda crear un backup del estado de la herramienta, y seguir la documentación suministrada por AlienVault OSSIM, pertinente con el cambio a realizar.
- Para la correcta utilización del OVA, es recomendable emplear Microsoft Edge o Internet Explorer 11.6 en adelante, dado que estos navegadores reúnen los complementos necesarios para el correcto funcionamiento del objeto virtual de aprendizaje.

13. REFERENCIAS BIBLIOGRÁFICAS.

AG, P. (2018). Monitoreo de redes con PRTG Network Monitor. Retrieved February 16, 2018, from https://www.es.paessler.com/network_monitoring?utm_source=google&utm_medium=cpc&utm_campaign=PRTG-Spanish-Search&utm_adgroup=Network-Monitoring&utm_adnum=002&utm_campaignid=18657746&utm_adgroupid=1237691186&utm_targetid=kwd-21387283946&gclid=CILa3uD-rssCF

Alam, M., Ihsan, A., & Khan, M. A. (2016). Optimizing SIEM throughput on the cloud using parallelization. *PLoS ONE*, *11*(11), 171581. https://doi.org/10.1371/journal.pone.0162746

Amaya Balaguera, Y. D. (2013). Metodologías ágiles en el desarrollo de aplicaciones para dispositivos móviles. *Revista de Tecnología | Journal Technology*, *12 número*, 111–124.

Amaya Guzmán, E. H., & Quiroga Martínez, L. V. (2012). *Integración y evaluación del piloto de la herramienta de monitoreo alienvault en la plataforma tecnológica de telefónica Telecom*. San Buenaventura Colombia.

Avella Coronado, J. D., Calderón Barrios, L. F., & Mateus Díaz, C. A. (2015). *Guía metodológica para la gestión centralizada de registros de seguridad a través de un SIEM*. UNIVERSIDAD CATÓLICA DE COLOMBIA. Retrieved from http://hdl.handle.net/10983/2847

Ayala Guanina, F. P., & Segovia Bedón, P. del P. (2016). *Implementación de una aplicación móvil, empleando la metodología mobil-d, para la geolocalización de centros de atención médica junto a sus profesionales requeridos, en las parroquias urbanas del cantón Latacunga en el periodo 2015*. Universidad Técnica de Cotopaxi. Retrieved from http://repositorio.utc.edu.ec/handle/27000/2051

Balarezo Chávez, A. F., & Poveda Pilatasig, D. X. (2015). *Propuesta de mejoramiento de la herramienta OSSIM siem (Open Source), para obtener los niveles óptimos de gestión en la administración de la seguridad, en una red implementada en cloud computing*. *Tesis*. Retrieved from http://dspace.ups.edu.ec/bitstream/123456789/5081/1/UPS-CYT00109.pdf

Barrios Valencia, N. D., Ferrer Garcia, R. C., Tovar Garrido, L. C., & Pupo Marrugo, S. (2016). *Desarrollo de objetos virtuales de aprendizaje como apoyo al estudio de la endodoncia en la Facultad de Odontología de la Universidad de Cartagena*. Universidad de Cartagena. Retrieved from http://190.242.62.234:8080/jspui/handle/11227/2940

Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network Security*, *2016*(9), 5–9. https://doi.org/10.1016/S1353-4858(16)30086-1

Bryant, B. D. (2016). *Hacking SIEMs to Catch Hackers: Decreasing the Mean Time to Respond to Network Security Events with a Novel Threat Ontology in SIEM Software*. University of Kansas. Retrieved from http://hdl.handle.net/1808/21973

Bryant, B. D., & Saiedian, H. (2017). A novel kill-chain framework for remote security log analysis with SIEM software. *Computers and Security*, *67*, 198–210. https://doi.org/10.1016/j.cose.2017.03.003

Camilo, C., & López, U. (2016). Framework for malware analysis in Android. *Scientific Information System*, *14*, 45–56. https://doi.org/10.18046/syt.v14i37.2241

Casola, V., De Benedictis, A., Rak, M., & Villano, U. (2017). *Monitoring Data Security in the Cloud: A Security SLA-Based APProach*. *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks* (1st ed.). Elsevier Inc. https://doi.org/10.1016/B978-0-12-811373-8.00011-2

Delgado Mendieta, L. J., & Suárez Asencio, J. H. (2015). *ANÁLISIS DE LA HERRAMIENTA OSSIM ALIENVAULT DE CORRELACIÓN DE EVENTOS PARA LA SEGURIDAD DE LA RED*. Universidad de Guayaquil. Retrieved from http://repositorio.ug.edu.ec/handle/redug/11799

Escamilla Pardo, T. (2017). *Sistema de autenticidad para aplicaciones de análisis de eventos para seguridad.* Universidad Politécnica de Valencia España. Retrieved from http://hdl.handle.net/10251/88583

Fernando, M., & Amaya, F. (2014). Valoración de la plataforma ASEF como base para detección de malware en aplicaciones Android Assessment of ASEF platform as a basic tool for detecting malware in Android APPs, *8*, 11–23. https://doi.org/https://doi.org/10.21774/ing.v8i21.439

Fonseca Escudero, D., Redondo Domínguez, E., Sánchez Riera, A., & Navarro Delgado, I. (2017). Educating Urban Designers using Augmented Reality and Mobile Learning Technologies / Formación de Urbanistas usando Realidad Aumentada y Tecnologías de Aprendizaje Móvil. *RIED. Revista Iberoamericana de Educación a Distancia*, *20*(2), 141. https://doi.org/10.5944/ried.20.2.17675

Garavito Robles, H. L. (2015). *Análisis y gestión del riesgo de la información en los sistemas de información misionales de una entidad del estado, enfocado en un sistema de seguridad de la información*. UNIVERSIDAD ABIERTA Y A DISTANCIA. Retrieved from http://hdl.handle.net/10596/3423

Graylog Inc. (2015). Graylog 1.0 Eliminates Cost Barriers to Unlocking Big Data. *Bussness Wire*.

Icinga. (2017). Icinga – Open Source Monitoring. Retrieved February 16, 2018, from https://www.icinga.com/

Iturralde, M., & Moreano Jurado, P. J. (2015). *Técnicas de detección de ataques en un sistema SIEM*. Universidad San Francisco de Quito.

João Pedro G. Alves. (2015). *Gestão de eventos de segurança de informação - SIEM*. Instituto Politécnico do Porto. Retrieved from http://www2.estgf.ipp.pt/~apinto/students/jalves_undergrad_2015.pdf

Ladino A., M. I., Villa S., P. A., & María, A. L. E. (2011). Fundamentos de iso 27001 y su aplicación en las empresas. *Scientia et Technica*, *1*(47), 334–339. Retrieved from http://revistas.utp.edu.co/index.php/revistaciencia/article/view/1177

LOGRHYTHM. (2016). Security Information and Event Management (SIEM). Retrieved from https://es.logrhythm.com/products/siem/

Londoño, S., Urcuqui, C. C., Fuentes Amaya, M., Gómez, J., & Navarro Cadavid, A. (2015). SafeCandy: System for security, analysis and validation in Android. *Sistemas Y Telemática*, *13*(35), 89. https://doi.org/10.18046/syt.v13i35.2154

Lorduy Salas, I. J., Peña Esquivel, Á. E., & Puello Marrugo, P. (2014). *Desarrollo de una plataforma para la gestión de objetos virtuales de aprendizaje para la Facultad de Odontología en la Universidad de Cartagena*. Universidad de Cartagena. Retrieved from http://190.242.62.234:8080/jspui/handle/11227/421

Lozano Ortiz, I., Vicent Safont, L., & Luque Hernández, A. (2013). Motivar y aprender con el móvil creando una aplicación para Android, mediante una metodología lúdica, constructivista y social. (Spanish). *Revista de Educación a Distancia*, (36), 1–23. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=fua&AN=89983910&lang=es&site=eds-live

Mario, J., Plata, O., Georgina, M., & Zermeño, G. (2013). Estrategias innovadoras en el aula : implementación de un objeto virtual de aprendizaje. *Revista Educación Y Humanismo*, *16*(26), 58–72. https://doi.org/https://doi.org/10.17081/eduhum.16.26.2347

Marrugo Marrugo, Y. J., Nuñez Barcos, R., & Martelo Gómez, R. J. (Director). (2012). *Sistema software de apoyo al proceso de creación y registro de políticas de seguridad informática en organizaciones*. UNIVERSIDAD DE CARTAGENA. Retrieved from http://190.242.62.234:8080/jspui/handle/11227/392

Matteis, L., & Ardenghi, J. R. (2011). Evaluación de PreludeIDS como herramienta de gestión de información y eventos relativos a seguridad. In *XIII Workshop de Investigadores en Ciencias de la Computación*. Retrieved from http://hdl.handle.net/10915/20438

Mineducación. (2017). OVA, Objetos Virtuales de Aprendizaje. Retrieved August 28, 2017, from http://www.mineducacion.gov.co/cvn/1665/article-131080.html

Mintic. Guía para la Implementación de Seguridad de la Información en una MIPYME (2016). Retrieved from http://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

Morán, J. G., García, J. C. R., Martínez, D. D. A., Baraza, J. C., & Gil, P. J. (2014). Formación on-line para profesionales en el campo de la Seguridad y la Inocuidad Informática a través de Competencias y Aprendizaje Basado en el Trabajo. *Formación on-Line Para Profesionales En El Campo de La Seguridad Y La Inocuidad Informática a Través de Competencias Y Aprendizaje Basado En El Trabajo*, *7*(3), 143–154.

Morelo Madariaga, J., & Betancur López, D. (2013). *Análisis forense al sistema Android afectado por el malware Fakelookout y su solución*. UNIVERSIDAD DE SAN BUENAVENTURA. Retrieved from http://hdl.handle.net/10819/1554

Nagios Enterprises. (2017). Nagios - El estándar de la industria en la supervisión de la infraestructura de TI. Retrieved February 12, 2018, from https://www.nagios.org/

Nicolett, M., & Kavanagh, K. M. (2011). Gartner research: Magic quadrant for security information and event management evaluation criteria definitions, (May), 1–32.

Nobles Perez, J. C., & Ruiz Garcia, P. M. (2014). *Construcción de un objeto virtual de aprendizaje para la capacitación en análisis forense de teléfonos móviles*. Universidad de Cartagena. Retrieved from http://190.242.62.234:8080/jspui/handle/11227/740

Nogueira de Góes, F. dos S., Monti Fonseca, L. M., Carvalho Furtado, M. C., Moraes Leite, A., & Silvan Scochi, C. G. (2011). Evaluación del objeto virtual de aprendizaje "Raciocinio diagnóstico en enfermería aplicado al prematuro." *Revista Latino-Americana de Enfermagem*, *19*(4), 8. Retrieved from www.eerp.usp.br/rlae

PandoraFMS Enterprises. (2009). Pandora FMS: el software de monitorización flexible. Retrieved February 15, 2018, from https://pandorafms.com/es/

Pascuas, Y., Jaramillo, C. & Verástegui, F. (2015). Desarrollo de objetos virtuales de aprendizaje como estrategia para fomentar la permanencia estudiantil en la educación superior. *Revista EAN*, (79), 116–129. Retrieved from http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-81602015000200008&lng=en&nrm=iso&tlng=es

Payares Guzmán, Á., & Ortega García, B. (2015). *Construcción De Un Aplicativo Cliente Servidor Para La Detección De Vulnerabilidades De Red En Smartphones Android Utilizando Una Herramienta De Escaneo*. Universidad de Cartagena. Retrieved from

http://190.242.62.234:8080/jspui/bitstream/11227/2945/1/TESIS.pdf

Perdomo, G. (2009). ¿Por qué, cómo y para qué estudiar los Sistemas Nacionales de Innovación y Estilos de Innovación en Colombia? *Pensamiento Y Gestión*, (27), 132–161. Retrieved from http://rcientificas.uninorte.edu.co/index.php/pensamiento/article/viewFile/849/494

Pereira Diéguez, M. (2015). *Entorno de gestión abierto para un laboratorio de redes de comunicaciones basado en software de monitorización NAGIOS y herramientas SNMP*. UNIVERSIDAD DE CANTABRIA. Retrieved from https://repositorio.unican.es/xmlui/bitstream/handle/10902/7733/379706.pdf?sequence=1

Pico Barrera, F. M. (2016). *Siem bajo software libre para la seguridad operacional en las pymes de la ciudad de Pelileo*. UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES. Retrieved from http://dspace.uniandes.edu.ec/handle/123456789/4691

Pomares Agamez, A. E., Betín Díaz, J. E., Puello Marrugo, P., & Insignares Órdoñez, S. (2013). *Desarrollo De Objetos Virtuales De Aprendizaje Para La Anatomía De Las Estructuras De Soporte De Los Órganos Dentarios En La Facultad De Odontología De La Universidad De Cartagena*. Universidad de Cartagena. Retrieved from http://190.242.62.234:8080/jspui/handle/11227/292

Rincón Flórez, Á. A., & Pájaro Arnedo, B. E. (2017). *APLICACIÓN MOVIL PARA GUIA DIAGNÓSTICA DE DESÓRDENES POTENCIALMENTE MALIGNOS Y PREVENCIÓN DE CANCER ORAL: UNA HERRAMIENTA EDUCATIVA DIDÁCTICA*. Universidad de Cartagena. Retrieved from http://190.242.62.234:8080/jspui/handle/11227/4560

Robledo, S., Osorio, G. A., & López, C. (2014). Networking en pequeña empresa: una revisión bibliográfica utilizando la teoria de grafos. *Revista Vínculos*, *11*(2), 6–16. https://doi.org/https://doi.org/10.14483/issn.2322-939X

Sapegin, A., Jaeger, D., Cheng, F., & Meinel, C. (2017). Towards a system for complex analysis of security events in large-scale networks. *Computers & Security*, *67*, 16–34. https://doi.org/10.1016/j.cose.2017.02.001

SIEM Alien Vault Enterprises. (2009). SIEM Software and Log Management | AlienVault. Retrieved February 2, 2018, from https://www.alienvault.com/solutions/siem-log-management

Silva Quinceno, M., & Sosa Chica, P. (2016). Diseño y desarrollo de un objeto virtual de aprendizaje para un curso de electrónica. *Inge Cuc*, *12*(1), 9–20. https://doi.org/10.17981/ingecuc.12.1.2016.01

SolarWinds. (2014). Network Tools, IT Management Software & Monitoring Tools | SolarWinds. Retrieved February 16, 2018, from http://www.solarwinds.com/

Suarez-Tangil, G., Palomar, E., Ribagorda, A., & Sanz, I. (2015). Providing SIEM systems with self-adaptation. *Information Fusion*, *21*(1), 145–158. https://doi.org/10.1016/j.inffus.2013.04.009

Thakur, K., Kopecky, S., Nuseir, M., Copeland, A., Saxena, N., & Bivins, D. (2016). An Analysis of Information Security Event Managers and the Data Extracted for Detecting Hidden Threats, (May 2014), 1–10. Retrieved from http://csis.pace.edu/~ctAPPert/srd2016/2016PDF/d5.pdf

Tibaquira Cortes, Y. A. (2015). *Metodología de gestión de incidentes de seguridad de la información y gestión de riesgos para la plataforma SIEM de una entidad financiera basada en la Norma ISO/IEC 27035 e ISO/IEC 27005*. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Retrieved from http://hdl.handle.net/10596/3634

Tovar, L. C., Bohórquez, J. A., & Puello, P. (2014). Propuesta Metodológica Para La Construcción De Objetos Virtuales De Aprendizaje Basados En Realidad Aumentada. *Formación Universitaria*, *7*(2),

11–20. https://doi.org/10.4067/S0718-50062014000200003

Vanegas, C. A. (2013). Desarrollo De Aplicaciones Sobre Android. *Vínculos*, *9*(2), 129–145.

Vega, C., & Chica, J. (2010). Diseño y validación de un objeto virtual de aprendizaje que permita el aprendizaje de heurísticas y metaheurísticas. *Revista Avances En Sistemas E Información*, *7*(3). Retrieved from http://www.redalyc.org/articulo.oa?id=133117498012

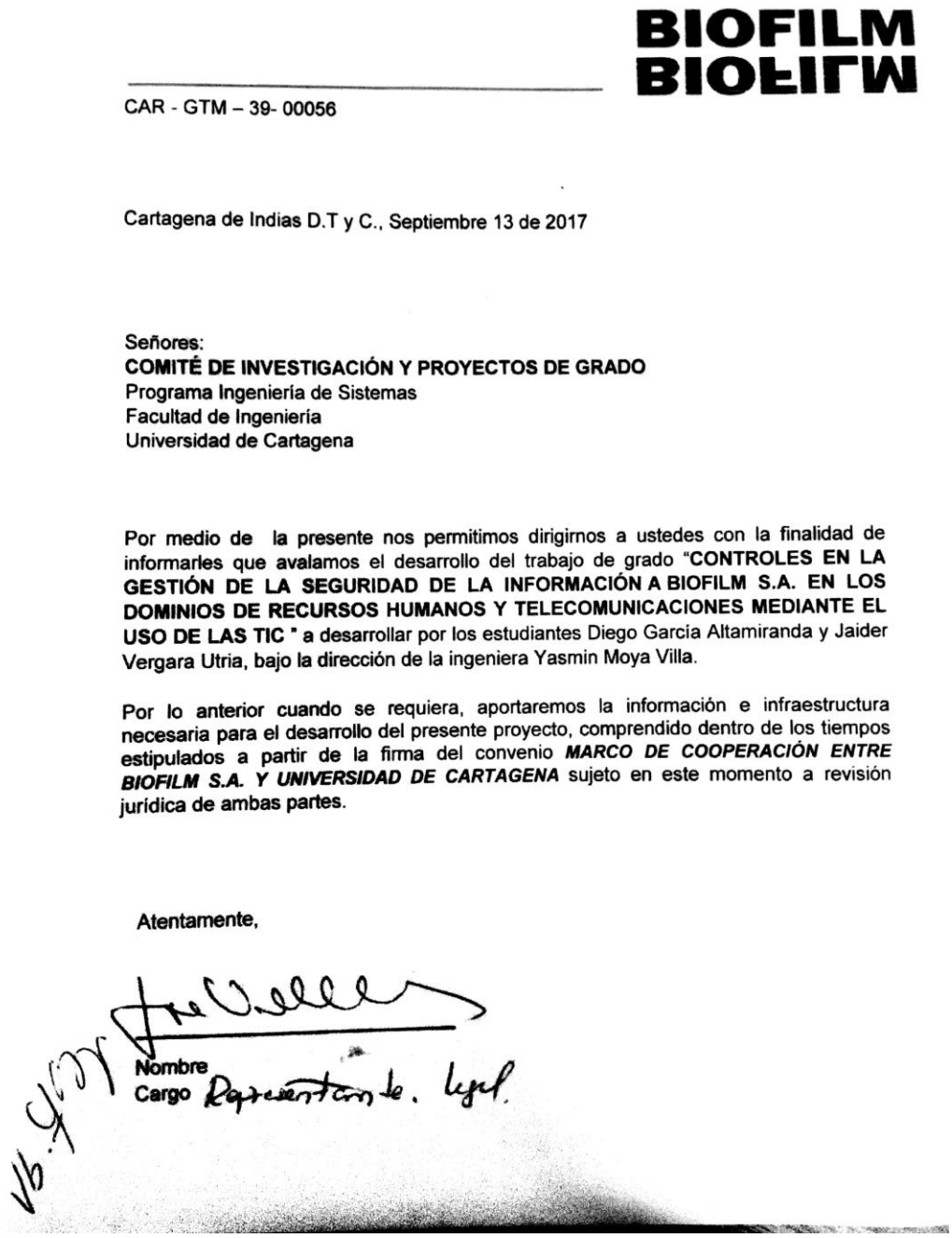
Villafuerte Quiroz, A. L., & Bravo Bravo, A. H. (2015). *IMPLANTACIÓN DE UNA HERRAMIENTA OSSIM PARA EL MONITOREO Y GESTIÓN DE LA SEGURIDAD DE LA RED Y PLATAFORMAS WINDOWS Y LINUX APLICADO A EMPRESAS MEDIANAS*. ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL. Retrieved from http://www.dspace.espol.edu.ec/xmlui/handle/123456789/30702

Zabbix Enterprise. (2005). Zabbix : The Enterprise-Class Open Source Network Monitoring Solution. Retrieved February 17, 2018, from http://www.zabbix.com/download

Zuleta Londoño, M. Á. (2013). *Actualización de nagios herramienta de monitoreo de la empresa une – telefónica de Pereira en el 2013*. Universidad Católica de Pereira. Retrieved from http://hdl.handle.net/10785/2000

14. ANEXOS

Anexo 1. Carta de aval de la empresa BIOFILM S.A. para la realización del proyecto.



BIOFILM

CAR - GTM – 39- 00056

Cartagena de Indias D.T y C., Septiembre 13 de 2017

Señores:
COMITÉ DE INVESTIGACIÓN Y PROYECTOS DE GRADO
Programa Ingeniería de Sistemas
Facultad de Ingeniería
Universidad de Cartagena

Por medio de la presente nos permitimos dirigirnos a ustedes con la finalidad de informarles que avalamos el desarrollo del trabajo de grado "**CONTROLES EN LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RECURSOS HUMANOS Y TELECOMUNICACIONES MEDIANTE EL USO DE LAS TIC** " a desarrollar por los estudiantes Diego García Altamiranda y Jaider Vergara Utria, bajo la dirección de la ingeniera Yasmin Moya Villa.

Por lo anterior cuando se requiera, aportaremos la información e infraestructura necesaria para el desarrollo del presente proyecto, comprendido dentro de los tiempos estipulados a partir de la firma del convenio ***MARCO DE COOPERACIÓN ENTRE BIOFILM S.A. Y UNIVERSIDAD DE CARTAGENA*** sujeto en este momento a revisión jurídica de ambas partes.

Atentamente,

Nombre
Cargo Representante. Legal.

Es de resaltar que el nombre del proyecto registrado en la carta de aval, no corresponde con el nombre final del mismo, debido a que se acataron las correcciones que los evaluadores realizaron en la presentación del anteproyecto.

Anexo 2. Acta de levantamiento de requisitos de las políticas a respetar en la realización y puesta en marcha de los controles.

Proyecto:	CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC		
Acta N° 1	**Fecha:** Febrero 23 de 2018	**Hora:** 10:00	**Lugar:** BIOFILM S.A.

REUNIÓN CONVOCADA POR	Investigadores
TIPO DE REUNIÓN	Levantamiento de requisitos.
ASISTENTES	Diego Armando García Altamiranda, Jaider Vergara Utria, Yenis Álvarez Jiménez.

Temas del orden del día:

- Leer documento general de las políticas.
- Resaltar las políticas afines con el proyecto.

[Tiempo asignado]	**[Entrevistador]**
2 horas	Diego Armando García Altamiranda

Discusión	Determinar las políticas de seguridad que se deben respetar a lo largo del desarrollo y puesta en marcha de los controles (solución del proyecto).
Conclusiones	Se realizó un nuevo documento con las políticas establecidas y este ha sido enviado al correo del entrevistador.

Información de los asistentes			
Firma		**Firma**	
Nombre	Yenis Alvarez J	**Nombre**	Jaider Vergara Utria
C.C.	45651164	**C.C.**	1050969127
Firma	Diego Garcia A.	**Firma**	
Nombre	Diego Garcia A.	**Nombre**	
C.C.	1104873074	**C.C.**	

Anexo 3. Acta de levantamiento de requisitos para la implantación de la herramienta SIEM en la empresa.

Proyecto:	CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC		
Acta N° 3	**Fecha:** Marzo 15 de 2018	**Hora:** 16:00	**Lugar:** BIOFILM S.A.

REUNIÓN CONVOCADA POR	Investigadores
TIPO DE REUNIÓN	Levantamiento de requisitos
ASISTENTES	Yenis Álvarez Jiménez, Pedro Torres, Diego García Altamiranda, Jaider Vergara Ltria.

Temas del orden del día:
Determinar el procedimiento de la implantación

[Tiempo asignado] 1 hora	**[Entrevistador]** Diego García Altamiranda.

Discusión	
Conclusiones	• Inventario de dispositivos de la planta de Cartagena • Determinar los eventos claves para la seguridad en Windows server, Fortinet, Cisco (buscar Security Windows 2010, 2016 moniting y demás) • Procedimientos de monitoreo de los equipos de la red • Creación de un entorno para pruebas dentro de BIOFILM • Cronograma de actividades

Información de los asistentes			
Firma	Jaider V	**Firma**	Diego G.
Nombre	Jaider Vergara U.	**Nombre**	Diego García A.
C.C.	1050969127	**C.C.**	1104873074
Firma	Pedro Torres	**Firma**	Ye-
Nombre	Pedro Torres	**Nombre**	Yenis Alvarez.
C.C.	9103671	**C.C.**	49691164.

Anexo 4. Acta de levantamiento de requerimientos para el aplicativo móvil y el OVA.

Proyecto:	CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC		
Acta N° 2	**Fecha:** Marzo 15 de 2018	**Hora:** 15:00	**Lugar:** BIOFILM S.A.

REUNIÓN CONVOCADA POR	Investigadores
TIPO DE REUNIÓN	Levantamiento de requisitos
ASISTENTES	Yenis Álvarez Jiménez, Laura Milena Alvis Gómez, Angelica Rodgers Guzmán, Diego Garcia Altamiranda, Jaider Vergara Utria.

Temas del orden del día:

- Discusión de estética de la aplicación y del OVA

[Tiempo asignado]	**[Entrevistador]**
50 minutos	Diego García Altamiranda

Discusión	Levantamiento de requisitos sobre aplicativo móvil y OVA
Conclusiones	OVA • Vídeo didáctico para reproducción en los televisores sobre las políticas de la seguridad de la información. • Colores institucionales • Sin sonido • Globos de idea (si se necesita) Aplicativo móvil • Juego de preguntas dentro del aplicativo para incentivar. • Conexión con base de datos de usuarios con información • Banco de preguntas.

Información de los asistentes

Firma	Angelica Rodgers G.	**Firma**	Diego G.
Nombre	Angelica Rodgers G.	**Nombre**	Diego García A.
C.C.	1.047.388.663.	**C.C.**	
Firma	Laura Alvis Gómez	**Firma**	
Nombre	Laura M. Alvis Gómez	**Nombre**	Yenis Alvarez J
C.C.	1047424696	**C.C.**	45691164.

Anexo 5. Acta definitiva y de profundización de levantamiento de requisitos de la APP móvil.

Proyecto:	CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC		
Acta N° 4	**Fecha:** Marzo 15 de 2018	**Hora:** 16:00	**Lugar:** BIOFILM S.A.

REUNIÓN CONVOCADA POR	Investigadores
TIPO DE REUNIÓN	Levantamiento de requisitos
ASISTENTES	Angélica Rodgers, Yenis Álvarez Jiménez, Diego García Altamiranda, Jaider Vergara Utria

Temas del orden del día:

- Funcionalidades del aplicativo móvil.
- Conclusión de las funcionalidades en forma de requisitos.

[Tiempo asignado]	**[Entrevistador]**
50 minutos	Diego García Altamiranda

Discusión	Levantamiento de requisitos sobre el aplicativo móvil.
Conclusiones	• Aplicativo móvil en forma de juegos de preguntas. • Los empleados deben acceder con un usuario y una contraseña. Sólo existirá un usuario por empleado. • El juego debe almacenar el puntaje de todos los jugadores. • Debe existir un perfil administrador para alimentar el juego. Este perfil no necesariamente debe ser móvil. • El juego debe generar campañas que son interpuestas por el administrador. • Los colores del aplicativo son basados en los colores institucionales. (Rojo y Blanco). • Las preguntas son de tipo selección múltiple con única respuesta, y de falso y verdadero. Cada una de ellas estará asociada a un grupo de pregunta. Una pregunta no debe aparecer en varios grupos de preguntas. • El número de ganadores por cada campaña, lo decide el administrador. • Toda esta información debe estar almacenada en una base de datos, de la cual se descargarán lo necesario para el funcionamiento del juego. • El administrador definirá el tiempo de duración de cada intento para contestar la cantidad de preguntas definidas también por el administrador. • El jugador podrá hacer cualquier cantidad de intentos. • Los ganadores saldrán de los mejores promedios.

Información de los asistentes			
Firma		**Firma**	
Nombre	Yenis Alvarez J.	**Nombre**	Angelica Rodgers6.
C.C.	45.091.164	**C.C.**	1047388663 C/gena.
Firma		**Firma**	
Nombre	Diego A. Garcia Hernandez	**Nombre**	Jaider Vegara Utria
C.C.	1104873074	**C.C.**	1050969127

Anexo 6. Acta de determinación del alcance de la herramienta SIEM.

Proyecto:	CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC		
Acta N° 5	**Fecha:** Mayo 9 de 2018	**Hora:** 9:00	**Lugar:** BIOFILM S.A.

REUNIÓN CONVOCADA POR	Investigadores
TIPO DE REUNIÓN	Acta de levantamiento de requisitos
ASISTENTES	Yenis Álvarez, Elkin de Castro, Diego García, Jaider Vergara

Temas del orden del día:

- Discusión sobre los eventos de seguridad más comunes.
- Determinación de las actividades claves en el proceso de vida de la herramienta.
- Determinación de los eventos de seguridad a auditar por la herramienta.

[Tiempo asignado]	**[Entrevistador]**
2 horas	Diego García Altamiranda – Jaider Vergara Utria
Discusión	Levantamiento de requisitos de la herramienta SIEM.
Conclusiones	Se decidió que en el proceso de implantación de la herramienta se deben desarrollar: • El alcance inicial de la herramienta, se limita al monitoreo del servidor que maneja el directorio activo, el cuál es Windows server 2012; al switch core Cisco 3750 G; al firewall Fortinet 90 C; y al servidor de archivos de Windows 2012 (opcional). • Instalación de la herramienta. • Realización del inventario de equipos de la red. • Extracción de los logs de todos los equipos de la red, en específico a los mencionados en el primer punto. • Revisión de eventos a auditar: 1) Escaneo de puertos; 2) Bloqueos de usuarios; 3) Autenticaciones fallidas; 4) Creaciones de usuarios; 5) Umbrales. • Alertas de los eventos anteriores. • Cuadros de mando. • Creación de informes.

Información de los asistentes			
Firma		**Firma**	
Nombre	Yenis Alvarez J.	**Nombre**	Diego García Altamiranda
C.C.		**C.C.**	1104873074.
Firma		**Firma**	
Nombre	Jaider Vergara U.	**Nombre**	Elkin De Castro
C.C.	1050969127	**C.C.**	79 625 554

Anexo 7. Acta de reunión para pruebas del aplicativo móvil.

ACTA DE REUNIÓN PARA PRUEBAS DE LOS CONTROLES

Proyecto	CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC		
Acta N° 6	**Fecha:** Septiembre 28 de 2018	**Hora Inicio:** **Hora final:**	**Lugar:** Biofilm S.A.
Objetivo de la reunión	Realizar las pruebas de usuario al aplicativo móvil SIG		
Responsable	Diego García Altamiranda – Jaider Vergara Utria		

ASISTENTES

Nombre y Apellido	Cargo/Dependencia
Luz Helena Florez G.	Analista Calidad
Alicia Correa Triana	Responsable SIG
Jose G. Castillo Ortega.	Coord. de Operaciones.
Jenis Alvarez Jiménez	Tecnología de Información.
Diego García Altamiranda	Investigadores.
Jaider Vergara Utria	Investigadores.

Agenda

- Introduccion del objetivo de la reunion.
- Instalar el aplicativo en los celulares.
- Usar el aplicativo. – Hacer diligenciamiento de formatos.

Desarrollo de la agenda

A los citados, se les instaló el aplicativo en los celulares y ellos hicieron uso del mismo, luego diligenciaron los formatos entregados.

Anotaciones relevantes

Información de los asistentes

Firma		Firma	
Nombre	Luz M. Florez G.	Nombre	Yenis Alvarez J.
C.C.	45.756.995	C.C.	45.691.164
Firma		Firma	
Nombre	ALCIRA GARCIA T.	Nombre	
C.C.	1.140.816.161	C.C.	
Firma		Firma	
Nombre	~~1047366366~~ Jose G Carrillo O.	Nombre	
C.C.	1047366366.	C.C.	
Firma		Firma	
Nombre		Nombre	
C.C.		C.C.	
Firma		Firma	
Nombre		Nombre	
C.C.		C.C.	
Firma		Firma	
Nombre		Nombre	
C.C.		C.C.	

Anexo 8. Formato de evaluación del aplicativo móvil.

FORMATO DE EVALUACIÓN DEL APLICATIVO MÓVIL SIG

1. Objetivo

Realizar la evaluación del aplicativo móvil SIG, desarrollado en el marco del proyecto de grado "CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC", para resaltar el cumplimiento de las características de identidad, usabilidad, navegabilidad, diseño y experiencia de usuario.

2. Descripción del sistema

El aplicativo móvil SIG, se utiliza como método para la evaluación de los conocimientos que los empleados de la empresa BIOFILM S.A., tienen en cuestiones de las políticas de seguridad de la información. El aplicativo móvil fue creado a manera de juego de preguntas, en el que se muestran aleatoriamente preguntas sobre temáticas puntuales, concernientes a las políticas de seguridad de la información.

3. Metodología para la aplicación de la prueba

La metodología a utilizar para la realización de las pruebas, se basa la citación de un grupo de empleados, quienes harán la instalación del aplicativo móvil en sus celulares, la creación de cuenta, y la realización de varios intentos sobre una campaña creada previamente. De esta manera, los empleados citados tendrán la facultad para diligenciar este formato, con la intención de evaluar el aplicativo móvil.

4. Formulario de evaluación

Las preguntas que aparecen a continuación, tienen como finalidad el cumplimiento de las características de identidad, usabilidad, navegabilidad, diseño y experiencia de usuario, que propone SIG. La respuesta, la debe seleccionar marcando una X en la casilla correspondiente.

Pregunta	**Si**	**No**
Preguntas de identidad		
1. *¿Con la información que se ofrece en pantalla, es posible saber a qué institución o empresa corresponde el aplicativo?*		
2. *¿Hay algún elemento gráfico o de texto que le haya ayudado a entender más claramente a que institución o empresa pertenece el aplicativo?*		
3. *¿Relaciona los colores predominantes en el aplicativo móvil con la institución?*		
4. *¿Distingue alguna imagen o logotipo que represente a la institución?*		
5. *¿Considera usted que este aplicativo móvil, está orientado hacia los trabajadores de la empresa?*		
Preguntas de contenido		
6. *¿Al momento de leer las diapositivas introductorias, pudo entender la dinámica del aplicativo?*		
7. *¿Los contenidos mostrados en cada ventana, corresponden con la opción seleccionada previamente?*		
8. *¿Las preguntas realizadas, son acordes con las políticas de seguridad de la información de la empresa?*		
9. *¿La metodología de preguntas aleatorias utilizada en el aplicativo, ayuda a la evaluación de los conocimientos de la temática en cuestión?*		
Preguntas de usabilidad		
10. *¿Para poder usar el aplicativo móvil, debió implementar conocimientos profundos sobre herramientas tecnológicas?*		

11. ¿Considera que es confuso el uso del aplicativo?		
Preguntas de navegabilidad		
12. ¿El aplicativo, permite el fácil acceso a los contenidos que provee?		
13. ¿Existen elementos en las páginas o ventanas, que le permitan identificar dónde está?		
14. ¿Hay alguna forma de regresar a la ventana principal o home, estando en cualquier parte del aplicativo?		
Preguntas de diseño		
15. ¿Es adecuada la combinación de colores?		
16. ¿El tamaño de la fuente y de los botones, es correcto?		
17. ¿Le pareció adecuada la forma en que se muestran las imágenes en el aplicativo?		
18. ¿Considera que gráficamente, el aplicativo es equilibrado?		
19. ¿El aplicativo tiene banners o avisos publicitarios?		
Pregunta de experiencia de usuario		
20. ¿Volvería a utilizar el aplicativo, para evaluar los conocimientos que posee usted, referente a las políticas de seguridad de la información?		

Nombre del empleado

Cargo

CC

Anexo 9. Formato de evaluación del OVA

FORMATO DE EVALUACIÓN DEL OVA

1. Objetivo

Realizar la evaluación del OVA, desarrollado en el marco del proyecto de grado "CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC", para resaltar el cumplimiento de las características de identidad, usabilidad, navegabilidad, diseño y experiencia de usuario.

2. Descripción del sistema

El OVA, se utiliza como método para la enseñanza de los conocimientos que los empleados de la empresa BIOFILM S.A., deben poseer en cuestiones de las políticas de seguridad de la información. El OVA fue creado de manera sencilla, haciendo un despliegue informativo en temáticas puntuales, concernientes a las políticas de seguridad de la información.

3. Metodología para la aplicación de la prueba

La metodología a utilizar para la realización de las pruebas, se basa la citación de un grupo de empleados, quienes harán uso del OVA. De esta manera, los empleados citados tendrán la facultad para diligenciar este formato, con la intención de evaluar el OVA.

4. Formulario de evaluación

Las preguntas que aparecen a continuación, tienen como finalidad el cumplimiento de las características de identidad, usabilidad, navegabilidad, diseño y experiencia de usuario, que propone el OVA. La respuesta, la debe seleccionar marcando una X en la casilla correspondiente.

Pregunta	**Si**	**No**
Preguntas de identidad		
1. *¿Con la información que se ofrece en pantalla, es posible saber a qué institución o empresa corresponde el OVA?*		
2. *¿Hay algún elemento gráfico o de texto que le haya ayudado a entender más claramente a que institución o empresa pertenece el aplicativo?*		
3. *¿Relaciona los colores predominantes en el aplicativo móvil con la institución?*		
4. *¿Distingue alguna imagen o logotipo que represente a la institución?*		
5. *¿Considera usted que el OVA, está orientado hacia los trabajadores de la empresa?*		
Preguntas de contenido		
6. *¿S le hizo fácil acceder a los contenidos presentes en el OVA?*		
7. *¿Los contenidos mostrados en cada ventana, corresponden con la opción seleccionada previamente?*		
8. *¿El contenido visualizado, es acorde con las políticas de seguridad de la información de la empresa?*		
9. *¿Considera que el contenido presentado en el OVA es entendible con relación a la política que se está tratando?*		

Preguntas de usabilidad		
10. ¿Para poder usar el OVA, debió implementar conocimientos profundos sobre herramientas tecnológicas?		
11. ¿Considera que es confuso el uso del aplicativo?		
Preguntas de navegabilidad		
12. ¿El OVA, permite el fácil acceso a los contenidos que provee?		
13. ¿Existen títulos o elementos en las ventanas, que le permitan identificar dónde está?		
14. ¿Hay alguna forma de regresar a la ventana principal o home, estando en cualquier parte del OVA?		
Preguntas de diseño		
15. ¿Es adecuada la combinación de colores?		
16. ¿El tamaño de la fuente y de los botones, es correcto?		
17. ¿Le parecieron adecuadas las imágenes que se muestran en el OVA?		
18. ¿Considera que gráficamente, el OVA es equilibrado?		
19. ¿El OVA tiene banners o avisos publicitarios?		
Pregunta de experiencia de usuario		
20. ¿Volvería a utilizar el OVA, para afianzar sus conocimientos con relación a las políticas de seguridad de la información?		

Nombre del empleado

Cargo

CC

Anexo 10. Acta de entrega de la herramienta SIEM.

ACTA DE ENTREGA

PROYECTO: CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC

SUBPROYECTO: SIEM

FECHA: marzo 08 de 2019

Diego García Altamiranda

Jaider Vergara Utria

Universidad de Cartagena

PRESENTE

Con referencia a la realización del proyecto de grado CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC, por este medio se hace entrega a la empresa BIOFILM S.A., de la herramienta SIEM para la gestión de las redes correspondiente con el objetivo 3 estipulado en el proyecto de grado y en los requerimientos plasmados por la empresa en las actas de levantamiento de requisitos.

Dicha herramienta SIEM será entregada a la empresa para la utilización de acuerdo a sus criterios de negocio y/o políticas.

Cliente	BIOFILM S.A.
Entrega de	Herramienta SIEM de gestión de redes
Fecha	marzo 08 de 2019
	Entrega **FINAL**

Elementos entregados
• Herramienta SIEM instalada en la red principal de la empresa, y configurada con los dispositivos declarados en el alcance del objetivo en cuestión.

El Cliente certifica que la totalidad de los suministros o servicios reseñados en la presente acta de recepción han sido entregados/terminados con las siguientes OBSERVACIONES

Certifican la entrega por el cliente	
Nombre: Jorge E. Rivera	Nombre: Yans Alvarez
Firma:	Firma:
C.C: 73'006.834 Cgena	C.C: 45691164
Cargo: Admon. Red infraestruc	Cargo: Jefe de TI

Certifican la entrega por el grupo de investigación	
Nombre: Diego A. García A	Nombre: Jaiber Vergara Ustra
Firma:	Firma:
C.C: 1104893074	C.C: 1050969127
Cargo: Estudiante	Cargo: Estudiante

Anexo 11. Acta de entrega y recibido del aplicativo móvil SIG.

ACTA DE ENTREGA

PROYECTO: CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC

SUBPROYECTO: APLICACIÓN MÓVIL SIG

FECHA: marzo 08 de 2019

Diego García Altamiranda

Jaider Vergara Utria

Universidad de Cartagena

PRESENTE

Con referencia a la realización del proyecto de grado CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC, por este medio se hace entrega a la empresa BIOFILM S.A., del aplicativo móvil SIG correspondiente con el objetivo 4 estipulado en el proyecto de grado y en los requerimientos plasmados por la empresa en las actas de levantamiento de requisitos.

Dicho software será puesto a disposición de los empleados de la empresa, para la evaluación de los conocimientos que los mismos poseen con respecto a las políticas de seguridad de la información.

Cliente	BIOFILM S.A.
Entrega de	Aplicación móvil SIG
Fecha	marzo 08 de 2019
	Entrega **FINAL**

Elementos entregados
• Archivo app que representa el instalador del aplicativo móvil SIG. • Aplicativo web para la administración del aplicativo móvil SIG, representado en las carpetas con el código fuente necesario para su puesta en producción. • Manuales de usuario de los dos aplicativos.

El Cliente certifica que la totalidad de los suministros o servicios reseñados en la presente acta de recepción han sido entregados/terminados con las siguientes OBSERVACIONES

Certifican la entrega por el cliente	
Nombre: Jairo Alvarez	Nombre:
Firma:	Firma:
C.C: 4569164	C.C:
Cargo: Jefe de TI	Cargo:

Certifican la entrega por el grupo de investigación	
Nombre: Diego A. García A.	Nombre: Jaider Vergara U.
Firma:	Firma:
C.C: 1104673074	C.C: 1050969121
Cargo: Estudiante	Cargo: Estudiante.

Anexo 12. Acta de entrega del Objeto Virtual de Aprendizaje (OVA).

ACTA DE ENTREGA

PROYECTO: CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC

SUBPROYECTO: OBJETO VIRTUAL DE APRENDIZAJE

FECHA: marzo 08 de 2019

Diego García Altamiranda

Jaider Vergara Utria

Universidad de Cartagena

PRESENTE

Con referencia a la realización del proyecto de grado CONTROLES EN LA SEGURIDAD DE LA INFORMACIÓN A BIOFILM S.A. EN LOS DOMINIOS DE RRHH Y TELECOMUNICACIONES EMPLEANDO LAS TIC, por este medio se hace entrega a la empresa BIOFILM S.A., del Objeto Virtual de Aprendizaje (OVA) correspondiente con el objetivo 5 estipulado en el proyecto de grado y en los requerimientos plasmados por la empresa en las actas de levantamiento de requisitos.

Dicho OVA será entregado a la empresa para la utilización de acuerdo a sus criterios de negocio y/o políticas.

Cliente	BIOFILM S.A.
Entrega de	Objeto Virtual de Aprendizaje (OVA)
Fecha	marzo 08 de 2019
	Entrega **FINAL**

Elementos entregados
• Archivo de formato HTML correspondiente al OVA. • Documento de preguntas frecuentes.

El Cliente certifica que la totalidad de los suministros o servicios reseñados en la presente acta de recepción han sido entregados/terminados con las siguientes OBSERVACIONES

Certifican la entrega por el cliente	
Nombre: Jesus Alvarez	Nombre:
Firma:	Firma:
C.C: 4569164	C.C:
Cargo: Jefe de TI.	Cargo:

Certifican la entrega por el grupo de investigación	
Nombre: Diego Garcia Hernandez	Nombre: Jaider Vergara Uria
Firma:	Firma:
C.C: 1104873074	C.C: 1050969167
Cargo: Estudiante	Cargo: Estudiante