Propuesta de seguridad de la arquitectura tecnológica en una red empresarial

SegArqTI

Carlos Felipe Bohórquez Rozo

ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO

DECANATURA DE INGENIERÍA DE SISTEMAS

PROYECTO DE GRADO

BOGOTÁ

2017

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

_____

FIRMA DEL DIRECTOR DEL PROYECTO

_____

FIRMA DEL ESTUDIANTE

Tabla de contenido

INTRODUCCIÓN

La implementación de tecnología y gestión de información está creciendo a gran escala y ha llevado a que toda empresa tenga la necesidad de tener equipos tecnológicos, aplicaciones que soporten los procesos de la empresa y herramientas software y hardware, teniendo esto como consecuencia un aumento de los ataques informáticos; Es por eso que es de vital importancia que toda empresa defina una buena arquitectura tecnológica, alternativas de seguridad eficientes y herramientas software y hardware que estén encaminadas a la estrategia de la empresa y mejoren la seguridad de sus sistemas para evitar ser víctimas de ataques informáticos.

Lo que se busca con esta propuesta de grado es brindar una alternativa de protección compuesta de mecanismos, aplicaciones, controles y procedimientos de seguridad de la información que suplan las necesidades de una arquitectura empresarial y tecnológica común; Para este estudio se realizó una búsqueda de todos los elementos que se utilizan en una arquitectura tecnológica y con estos se construyó una propuesta una con elementos necesarios y comunes, seguido de esta definición se realizó una evaluación de posibles amenazas y riesgos de la arquitectura, con la finalidad de poder definir políticas, herramientas y mecanismos que aseguren los equipos e información y mitiguen las amenazas encontradas.

Para apoyar esta alternativa se realizó una propuesta que promueva buenas prácticas del uso de la información, ya que no basta con tener una buena alternativa de seguridad, si las personas que manipulan e intervienen en los procesos de la empresa no se concientizan del buen uso que se le debe dar a la información, aplicaciones, equipos tecnológicos y las consecuencias que se pueden llegar a acarrear por el mal manejo de ellos.

En la primera parte de este documento se encuentra el marco teórico del proyecto, seguido a este encontraremos la definición de la arquitectura tecnológica, evaluación de amenazas y riesgos, la definición y evaluación de herramientas y por último la elaboración de la propuesta de seguridad con base en las herramientas evaluadas.

FORMULACIÓN DEL PROYECTO

Información general

NOMBRE	Propuesta de seguridad de la arquitectura tecnológica en una red empresarial
DIRECTOR	Claudia P Santiago
EQUIPO DE ESTUDIANTES	CARLOS FELIPE BOHORQUEZ ROZO
GRUPO DE INVESTIGACIÓN	Ciencia, Tecnología y Gestión - CTG-Informática
LÍNEA DE INVESTIGACIÓN	Infraestructura y seguridad de la información
PROYECTO DE INVESTIGACIÓN AL QUE PERTENECE	Grupo de investigación CTG-Informática
DURACIÓN (MESES)	9 MESES

Planteamiento del problema

El crecimiento empresarial del país ha aumentado en los últimos años considerablemente, motivo por el cual el tema de tecnología y gestión de información está en auge, y ha llevado así mismo a que los ataque cibernéticos aumenten y las pérdidas económicas y reputacionales de las empresas sean cada vez mayor, motivo por el cual se pretende ser un referente para que cualquier empresa que implemente tecnología la asegure a un costo razonable.

Justificación

Toda empresa que cuente hoy en día con una infraestructura tecnológica (equipos, servidores, aplicaciones nativas de la empresa y software que están soportando las mimas) puede llegar a ser víctima de ataques informáticos, lo que implicaría pérdidas financieras y/o reputacionales, es por eso que estas empresas necesitan herramientas que permitan que su infraestructura e información este protegida.

Objetivo general

Determinar los elementos comunes y necesarios de la plataforma de TI de una organización y a partir de ella realizar una definición y evaluación de herramientas, para generar una propuesta de integral de seguridad de la información.

Objetivos específicos de la propuesta

1. Identificar los elementos comunes y necesarios a nivel de arquitectura de TI de una organización.
2. Construir una propuesta de arquitectura tecnológica.
3. Hacer una evaluación de riesgos y amenazas generales de la arquitectura construida.
4. Realizar una búsqueda de alternativas de protección que mitiguen las posibles amenazas o riesgos identificados en la arquitectura definida.
5. Implementar y evaluar las herramientas de protección.
6. Construir una propuesta integral de seguridad para la arquitectura tecnológica de una organización.

Alcance

El proyecto buscara definir una propuesta de seguridad de información a partir de la definición de los elementos comunes de una arquitectura tecnológica y la definición de controles y herramientas de seguridad.

Con el fin de establecer esta propuesta se implementaran y calificarán las herramientas de protección de acuerdo a una matriz de evaluación definida previa a la instalación y se contemplara asegurar sistemas operativos Windows, Mac y Linux.

Herramientas software utilizadas

1. Project.
2. Office (Word y Excel).
3. Visio.
4. VMWare.
5. Herramientas de seguridad evaluadas.
6. Sistema operativo Linux mint.
7. Sistema operativo Linux Ubuntu.
8. Sistemas operativos Windows 7 y 8.1.
9. Sistema operativo MAC.

Criterios de terminación de trabajo

1. Entregada la propuesta de protección.
2. Entrega de documentos propios de proyecto de grado.
3. Evaluación final de jurados.

Evaluadores

1. Claudia Patricia Santiago.
2. Daniel Díaz.
3. Gerardo Ospina.

CRONOGRAMA

Proyecto de grado 1

Proyecto de grado 1			
Nombre de tarea	Duración	Comienzo	Fin
Entrega - Cronograma	5 días	mar 09/08/16	sáb 13/08/16
Recopilación de información - Arquitectura empresarial común	6 días	dom 14/08/16	vie 19/08/16
Entrega - Arquitectura empresarial final	4 días	vie 19/08/16	mié 24/08/16
Entrega- criterios calificación	1 día	vie 26/08/16	vie 26/08/16
Recopilación de información- Arquitectura de seguridad	4 días	sáb 27/08/16	mié 31/08/16
Entrega-Formulación de proyecto de grado	1 día	mar 06/09/16	mar 06/09/16
Entrega - Arquitectura de seguridad común	3 días	mié 31/08/16	vie 02/09/16
Recopilación de información y definición de riesgos	4 días	dom 04/09/16	mié 07/09/16
Recopilación de información-proveedores con opción de software libre	4 días	mié 07/09/16	lun 12/09/16
Análisis de riesgos	2 días	mar 13/09/16	mié 14/09/16
Recopilación de información-alternativas de seguridad	2 días	jue 15/09/16	vie 16/09/16
Entrega - Propuesta arquitectura de seguridad inicial	5 días	sáb 17/09/16	jue 22/09/16
Montaje- Bases de datos y posibles software libre	3 días	vie 23/09/16	mar 27/09/16
Montaje- Red LAN	3 días	mar 27/09/16	jue 29/09/16
Entrega - Esqueleto Artículo	1 día	sáb 01/10/16	sáb 01/10/16
Montaje - Protocolos Seguridad, Firewall	3 días	vie 30/09/16	mar 04/10/16
Pruebas funcionales	1 día	sáb 08/10/16	sáb 08/10/16
Montaje softwarelibre linux	3 días	mié 05/10/16	vie 07/10/16
Montaje- Firewall y alternativa de seguridad en máquina Linux	3 días	vie 23/09/16	mar 27/09/16
Inscripción vitrina académica	1 día	lun 31/10/16	lun 31/10/16
Pruebas funcionales	1 día	sáb 29/10/16	sáb 29/10/16
Entrega-Cartelera técnica	8 días	mar 06/12/16	jue 15/12/16
Entrega- Poster	2 días	vie 18/11/16	lun 21/11/16
Montaje-Vitrina académica	1 día	mié 23/11/16	mié 23/11/16
Vitrina académica	1 día	jue 24/11/16	jue 24/11/16
Entrega-Artículo primera edición	7 días	mar 06/12/16	mié 14/12/16
Actualizaciòn documentos finales	5 días	lun 16/01/17	vie 20/01/17

Proyecto de grado 2

Proyecto de grado 2			
Nombre de tarea	Duración	Comienzo	Fin
Definiciòn general de arquitectura tecnologica	6 días	sáb 21/01/17	vie 27/01/17
Instalaciòn y documentaciòn final Windows	15 días	sáb 28/01/17	jue 16/02/17
Instalaciòn y documentacion Linux	25 días	vie 17/02/17	jue 23/03/17
Instalaciòn y documentaciòn MAC	25 días	vie 24/03/17	jue 27/04/17
Recopilación de información-Arquitetura de seguridad orientada al capital humano	4 días	vie 28/04/17	mié 03/05/17
Vitrina academica	1 día	mié 04/05/16	mié 04/05/16
Entrega-Popuesta de seguridad orientada al capital humano	5 días	vie 05/05/17	jue 11/05/17
Entrega documentos finales para validaciòn	5 días	vie 12/05/17	jue 18/05/17
Sustentaciòn pares	1 días	vie 18/05/17	vie 19/05/17
Entrega-Artículo segunda edición	1 días	vie 19/05/17	jue 23/05/17

MARCO TEÓRICO

Arquitectura empresarial

Haciendo una recopilación de definiciones que se encuentran en la web, podemos decir que la Arquitectura tecnológica(AE) es una metodología, la cual incorpora y relaciona los recursos tecnológicos, procesos, datos, aplicaciones, infraestructura, recursos humanos, metodologías y los alinea con los objetivos estratégicos de la empresa.

Esta arquitectura empresarial está dividida en componentes (*Ilustración 1*), todos en función de la visión estratégica de la empresa, estos a su vez generan recursos valiosos que permiten tomar decisiones, descubrir necesidades, definir vías para cumplimiento de objetivos y definir brechas.

Ilustración 1 - Componentes de la arquitectura empresarial [1]

¿Por qué implementarla?

Muchas empresas invierten gran cantidad de recursos físicos y económicos en procesos e implementación de tecnologías las cuales no van alineados con los objetivos de la empresa, otras de éstas no tienen una comunicación efectiva ya que cada una de las áreas que la componen trabaja por su parte e invierten recursos y procesos que no están alineados con la estrategia de la empresa, otros aunque tienen una AE establecida no están aprovechando de manera eficiente los recursos de esta arquitectura. La AE permite que estas áreas se alineen y que cada uno de los recursos invertidos y procesos realizados estén orientados con la estrategia de la empresa, además de esto permite que la empresa aproveche las tecnologías de la mejor manera.

MARCOS DE REFERENCIA O FRAMEWORKS

La importancia de una arquitectura empresarial para cualquier empresa llevo al desarrollo de varias metodologías o marcos de referencia, los cuales proporcionan herramientas, mejores prácticas, pasos para definir o implementar una AE y como encaminar los recursos a la estrategia de la empresa.

A continuación vamos a citar algunas de las definición dadas por el estudiante Cristian Andrés Sánchez Rodríguez de algunos de los marcos de referencia existentes, estas definiciones fueron extraídas de su propuesta de arquitectura empresarial desarrollada como trabajo de grado para maestría de gestión de la información, la cual esta publicada en la página de la biblioteca de la Escuela Colombiana de Ingeniería Julio Garavito y sus repositorios; Se citarán estas definiciones ya que aunque existen muchas de ellas, inclusive las oficiales por cada autor de la referencia, se encuentra en las del estudiante una definición clara y en un lenguaje sencillo.

DoDaft (Department of Defense Architecture Framework)

DoDAF ha sido diseñado para satisfacer el negocio específico y las necesidades operacionales del Departamento de Defensa. Se define una forma de representar una arquitectura empresarial que permite a las partes interesadas concentrarse en áreas específicas de interés en la empresa, al tiempo que conserva la vista de la imagen grande. Para ayudar a los tomadores de decisiones, DoDAF proporciona los medios para abstraer información esencial de la complejidad subyacente y la presenta de manera que mantenga la coherencia y la consistencia. [2] [3]

Desafortunadamente por su naturaleza, DoDAF es deficiente en el momento de hacer un análisis de alternativas (de negocio, financiera, técnica) lo cual es indispensable en el sector privado para la toma de decisiones.

Zachman Enterprise Framework

El marco de referencia Zachman es una herramienta de pensamiento que nos permite organizar, clasificar y analizar los diferentes aspectos arquitecturales de una compañía (Modelo de estrategia, organigramas, modelos de procesos, modelos de datos, las reglas de negocio, etc.).

El propósito de este marco de referencia es proveer una estructura básica que soporte la organización, el acceso, la integración, la interpretación, el desarrollo, la administración y el cambio de un conjunto de representaciones arquitectónicas de los sistemas de información de la empresa, por lo que la implementación de este framework es bastante complicada. [2]

FEAF (Federal Enterprise architecture)

De acuerdo con [2] FEAF es una iniciativa de la Oficina de Administración y Presupuesto (OMB). Su propósito es proporcionar una metodología común para la compra de tecnologías de información; sin embargo, el alcance de FEAF se circunscribe al gobierno federal de los Estados Unidos de Norteamérica. Tres son los principios que le dan dirección estratégica

1. Guiada por el negocio,
2. Proactiva y colaborativa a lo largo del gobierno federal.
3. La arquitectura mejora la efectividad y eficiencia de los recursos de información del gobierno.

TOGAF (The Open Group Architecture Framework)

Según [2] y la información de [4] Es una metodología probada de arquitectura empresarial y el marco utilizado por grandes organizaciones en el mundo para mejorar la eficiencia del negocio. Es el más destacado y fiable estándar de arquitectura empresarial, asegurando estándares consistentes, los métodos y la comunicación entre los profesionales de la arquitectura empresarial, goza de mayor credibilidad de la industria, efectividad en el trabajo, y oportunidades de carrera. TOGAF utiliza los recursos de manera más eficiente y eficaz, y se evidencia un mayor retorno de la inversión.

Se puede concluir que es fundamental la definición de un modelo para el desarrollo de la arquitectura empresarial de una empresa, ya que facilita la definición general de la empresa, la capacidad de trabajo, la capacidad de activos físicos, capacidad de activos tecnológicos, interesados, aliados y métodos para cumplir la estrategia, permite también definir una buena arquitectura tecnológica, infraestructura tecnológica, modelo de aplicaciones y sistemas de seguridad física y de la información.

La finalidad del proyecto es seleccionar y definir los elementos comunes tecnológicos de una empresa, es por eso que no construirá toda una arquitectura empresarial, si no que se evaluaran algunos aspectos que nos permitieran llegar a la arquitectura tecnológica, este trabajo de grado se apoyó en algunas fases del modelo TOGAF.

Es por lo anterior que se propone este modelo como un modelo adecuado para el desarrollo de la arquitectura de cualquier empresa, pues es un modelo que permite llegar a una arquitectura empresarial y a la arquitectura de seguridad, a través de un lenguaje sencillo y estándar, razón por la cual vamos a hablar un poco de lo que es este modelo, lo que contempla y en que puede ayudar a definir una arquitectura tecnológica y la seguridad de la información.

TOGAF

TOGAF es una herramienta de *The Open group*, la cual permite desarrollar e implementar una arquitectura empresarial por medio del modelo iterativo de procesos, el cual puede ser adaptado a cualquier tipo de arquitectura empresarial, el secreto fundamental de TOGAF es el método de desarrollo de arquitectura (ADM).

TOGAF en la guía de bolsillo 9.1 tiene cuatro tipos relacionados de arquitectura, estos son: Arquitectura de negocio, arquitectura de datos, arquitectura de aplicación y en la que nos vamos a enfocar que es la arquitectura tecnológica, su descripción se encuentra en la siguiente ilustración:

Tipo de Arquitectura	Descripción
Arquitectura de Negocio	La estrategia de negocio, gobierno, organización y procesos clave de la organización.
Arquitectura de Datos[3]	La estructura de datos lógicos y físicos que posee una organización y sus recursos de gestión de datos.
Arquitectura de Aplicación	Un plano (blueprint en inglés) de las aplicaciones individuales a implementar, sus interacciones y sus relaciones con los procesos de negocio principales de la organización.
Arquitectura Tecnológica	Las capacidades de software y hardware que se requieren para apoyar la implementación de servicios de negocio, datos y aplicación. Esto incluye infraestructura de IT, capa de mediación (middleware en ingles), redes, comunicaciones, procesamiento y estándares.

Ilustración 2 - tipos de arquitectura definidos por TOGAF [5]

Método de desarrollo de la arquitectura (ADM)

Según Togaf en [6] el ADM es un método para obtener arquitecturas empresariales que son específicas para la organización, describe: un modo confiable y probado para desarrollar y utilizar una arquitectura empresarial, un método para desarrollar arquitecturas en diferentes niveles que permiten al arquitecto asegurar un conjunto complejo de requerimientos se aborden adecuadamente y un conjunto de guías y técnicas para el desarrollo de arquitectura.

A continuación se ilustra el ciclo del método ADM:

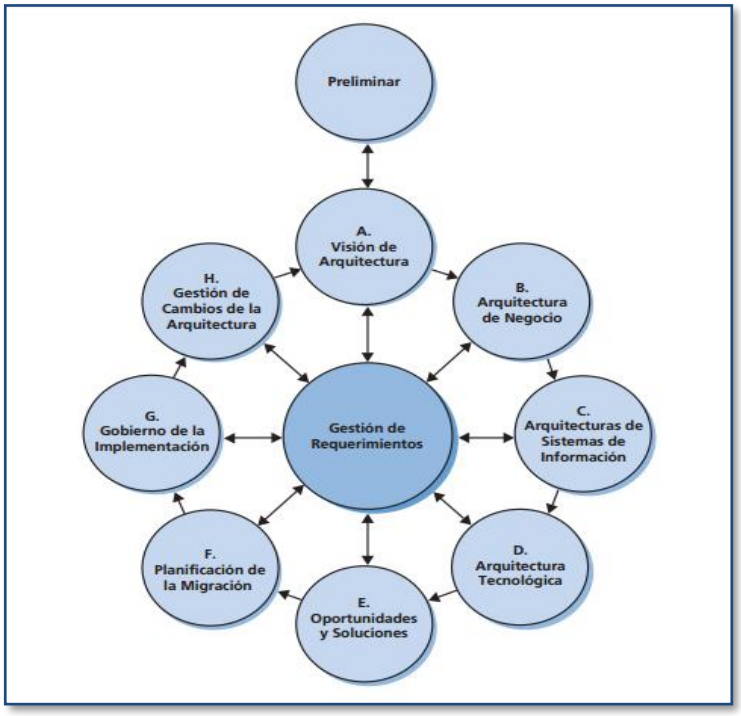


Ilustración 3 - Ciclo del método ADM [6]

Como el proyecto tiene como enfoque la arquitectura tecnológica se va ilustrar una breve descripción de las fases del ciclo de ADM y como la define la guía de TOGAF

Desarrolla arquitecturas en cuatro dominios:

1. Negocio
2. Sistemas de Información - Aplicaciones
3. Sistemas de Información - Datos
4. Tecnología

En cada caso, desarrolla la Arquitectura de la Línea de Base y de Destino y analiza las brechas entre ambas.

Ilustración 4 - Descripción fase B, C, D método ADM [6]

ARQUITECTURA TECNOLÓGICA

Esta arquitectura busca definir y diseñar a alto nivel los elementos tecnológicos físicos y lógicos que sean acordes a las necesidades de la empresa, es decir, software base, hardware, equipos e infraestructura tecnológica, lo anterior con el fin de apoyar el cumplimiento de los objetivos estratégicos de la empresa y generar confiabilidad e integridad de datos, para así asegurar la continuidad del negocio y generar valor agregado a los usuarios.

Esta arquitectura tiene la capacidad de ilustrarle a los interesados elementos como computadores, servidores, routers, switches, firewalls, impresoras, teléfonos, segmentación de la red, servicios, aplicaciones y bases de datos, es por eso que con base en esta arquitectura se puede hacer un análisis, definir políticas, hacer mejoras tecnológicas, de seguridad, de continuidad de negocio y definir soluciones a inconvenientes tecnológicos que se presenten en el negocio.

TOGAF en su guía de bolsillo 9.1 capitulo 12(Arquitectura tecnológica) define como objetivos los siguientes:

- Desarrollar la Arquitectura Tecnológica que permita el desarrollo lógico y físico, componentes de aplicaciones y datos, abordando la solicitud de arquitectura empresarial y preocupaciones de las partes interesadas.
- Identificar los componentes candidatos de la Hoja de Ruta de la Arquitectura basados en lagunas arquitecturas de tecnología de referencia y de destino.

También define elementos o documentos de entrada y salida de la arquitectura como:

Entradas	Salidas
Petición de Trabajo de Arquitectura Evaluación de Capacidades Plan de comunicaciones Modelo Organizacional de Arquitectura Empresarial Marco de Referencia de Arquitectura adaptado Principios de Tecnología Declaración de Trabajo de Arquitectura Visión de la Arquitectura Repositorio de Arquitectura Documento preliminar de Definición de Arquitectura, conteniendo: • Arquitectura de Negocio de la Línea de Base (detallada) • Arquitectura de Negocio de Destino (detallada) • Arquitectura de Datos de la Línea de Base (detallada) • Arquitectura de Datos de Destino (detallada) • Arquitectura de Aplicación de la Línea de Base (detallada) • Arquitectura de Aplicación de Destino (detallada) • Arquitectura Tecnológica de la Línea de Base (de alto nivel) • Arquitectura Tecnológica de Destino (de alto nivel)	Declaración de Trabajo de Arquitectura, actualizado si fuera necesario Principios de Tecnología validados o nuevos principios de Tecnología (si se generaron aquí) Versión preliminar del Documento de Definición de Arquitectura, conteniendo actualizaciones de contenido: • Arquitectura Tecnológica de la Línea de Base • Arquitectura Tecnológica de Destino • Vistas de Arquitectura Tecnológica correspondientes a Puntos de Vista que han sido seleccionados para responder a las preocupaciones clave de los interesados Especificación preliminar de los Requerimientos de Arquitectura, incluyendo actualizaciones de contenido: • Resultados del Análisis de Brechas • Requerimientos resultantes de las Fases B y C • Requerimientos de Tecnología actualizados

Ilustración 5 - Entradas y salidas de la línea base [7]

Es importante tener un orden para la definición de esta arquitectura tecnológica es por eso que una vez evaluadas varias propuestas y consejos se definió que es importante seguir los siguientes pasos:

1. Seleccionar el modelo de referencia, puntos de vista y herramienta.
2. Desarrollar la descripción de la arquitectura tecnológica de la línea de base.
3. Desarrollar la descripción de la arquitectura tecnológica de destino.
4. Realizar un análisis de brechas.
5. Definir los componentes candidatos del plan de itinerario.
6. Resolver los impactos del panorama de arquitectura.
7. Conducir una relación de los aliados estratégicos.
8. Finalizar la arquitectura tecnológica.
9. Crear el documento de definición de la arquitectura.

ARQUITECTURA DE SEGURIDAD SEGÚN TOGAF

Para esta sección nos apoyamos en el capítulo 21 de TOGAF [8] y en un proyecto de grado de la escuela Colombiana de ingeniería [9], estos hablan la arquitectura de seguridad y definen que esta arquitectura es una herramienta para describir el estado de una empresa basándose en los activos de información que posee, sistemas de información y funcionarios de la empresa, también ayuda a definir las actividades de un arquitecto de seguridad y acciones que debe seguir para determinar las políticas de seguridad y hacer una correcta gestión del riesgo.

Lo anterior con el fin de minimizar el riesgo al que está expuesta la información de una empresa y apoyarla a encontrar y definir las vulnerabilidades de dicha organización.

La guía de TOGAF define las siguientes áreas de interés con el fin que toda la información de la empresa está protegida, además de brindar un acompañamiento y aconsejando al usuario sobre temas que debe considerar para asegurar la información:

- Autenticación: identidad de una persona o entidad relacionada con la entrada o sistema.
- Autorización: Capacidades permitidas para una persona o entidad cuya identidad ha sido establecida.
- Auditoría: La capacidad de proporcionar datos forenses.
- Aseguramiento: La capacidad de probar y demostrar que la arquitectura de la empresa tiene la seguridad necesaria para mantener las políticas de seguridad establecidas.
- Habilidad: Capacidad de la empresa para funcionar sin interrupción o agotamiento del servicio a pesar de eventos anormales o maliciosos.
- Protección de activos: La protección de los activos de información de la pérdida o divulgación no deseada.
- Administración: La posibilidad de publicar anuncios.
- Gestión del riesgo: La actitud de la organización y la tolerancia al riesgo.

Esta sección menciona de donde surgen los requisitos de seguridad y define algunas fuentes.

- Una nueva ley o mandato reglamentario.
- Una nueva amenaza realizada o experimentada.
- Una nueva iniciativa de arquitectura de TI descubre nuevas partes interesadas y / o nuevos requisitos.

Es importante resaltar la tarea que hace TOGAF para el proyecto ya que no solo da una visión de donde se deben las empresas enfocar a nivel de seguridad, sino que también nos da información de cómo se asocia la arquitectura de seguridad con la arquitectura tecnológica, dando recomendaciones y especificaciones de esta asociación como por ejemplo.

- Evaluar y basar las tecnologías actuales específicas de la seguridad.
- Revisar los supuestos a los sistemas de conexión.
- Identificar métodos para controlar el consumo de recursos.
- Identificar los privilegios mínimos requeridos.
- Identificar las medidas de mitigación de la seguridad, cuando así lo justifique la evaluación de riesgos

Los documentos de seguridad que deben existir luego de realizar la arquitectura de seguridad basada en la arquitectura tecnológica, son:

- Lista básica de tecnologías de seguridad.
- Lista de sistemas interconectados validados.
- Lista de normas de seguridad seleccionadas.
- Plan de conservación de recursos.
- Métricas de seguridad y plan de monitoreo.
- Políticas de autorización del usuario.
- Plan de gestión de riesgos.
- Requisito de confianza del usuario (autorización).

SEGURIDAD DE LA INFORMACIÓN

La norma internacional ISO27001 define un SGSI (sistema de gestión de seguridad de la información) para garantizar la seguridad de la información, allí define un criterio estándar y primordial que es preservar la confidencialidad, integridad y disponibilidad de la información en cada ciclo de vida de la misma, lo que se busca es asegurar que la información esté disponible de acuerdo a las políticas de la empresa para las personas, entidades o procesos autorizados, que sea manipulada por el personal autorizado para que sea exacta y que no permita ser vista o no esté a disposición de personal no autorizado.

Para lograr que la información de la empresa cumpla con los estándares, es importante que toda organización determine políticas de autenticidad, privilegios de acceso, cifrados, aseguramientos de la red y cualquier alternativa de protección necesaria, sin embargo para poder definir qué medidas, procesos y software necesita la empresa, se debe realizar un previo análisis de amenazas y riesgos donde se identifiquen las falencias que puede tener a nivel de tecnología, infraestructura y recursos humanos, considerando riesgos o incidentes de seguridad causados desde el exterior e interior de la empresa y temas de daños naturales o físicos.

Todos y cada uno de los recursos invertidos para cumplir con la seguridad de una organización deben cumplir con los objetivos estratégicos de la empresa y debe también cumplir con documentos y medidas legales de cada país o lugar donde se implementen.

A continuación ilustraremos las actividades, procesos y causas que intervienen en la seguridad de la información.

Ilustración 6 - Modelo de relación de actividades de seguridad [10]

Es importante aclarar que en la seguridad de la información intervienen activos tecnológicos (físicos y lógicos) y activos humanos, teniendo como prioridad los activos humanos ya que son los más difíciles de controlar porque no se puede asumir cómo va a actuar, ni se puede asegurar que las

órdenes dadas sean cumplidas, es por eso que la mayoría de la seguridad está enfocada a preservar y proteger la información utilizada y que esté al alcance ser humano, sin dejar atrás los posibles riesgos tecnológicos y físicos que existan.

La seguridad de la información es muy importante y debe ser primordial para toda empresa ya que protege sus activos, asegura el cumplimiento de políticas y objeticos específicos de la empresa, evita perdidas reputacionales, económicas y por ultimo permite tener un manejo adecuado y un ciclo de vida correcto de la información.

NORMAS Y ESTÁNDARES INTERNACONALES

Estas normas nacen con la necesidad de tener un lenguaje sencillo, conceptos técnicos y de gestión unificadados, guías o manuales de operaciones y buenas prácticas para definir, analizar y evaluar la seguridad de la información de una empresa.

Dentro de estos estándares se encuentra un ente que define, rige y certifica el cumplimiento de las normas y ese es:

- ISO (International Organization for Standardization)

Este ente define y regula criterios estándares de muchas líneas de negocio dentro de ellas las de seguridad de la información empresarial, la cual puede ser estudiada y conocida por medio de las siguientes normas.

ISO 27000

Es una norma internacional emitida por ISO la cual proporciona un marco de tecnología de la información, técnicas de seguridad, sistemas de gestión de seguridad de la información e información general. [11]

ISO 27001

Aprobado como estándar internacional en octubre de 2005, es la norma principal de requisitos del sistema de gestión de seguridad de la información, especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI). [11]

Análisis y gestión de riesgos ISO27001

El modelo establecido para desarrollar la etapa de análisis y gestión de riesgo define unas sub-etapas o subprocesos que son los siguientes:

- Planificación de análisis y gestión de riesgos.
- Análisis de riesgos.
- Gestión de riesgos.
- Selección de salvaguarda.

A continuación ilustraremos una descripción de los objetivos de cada una de estas etapas.

Etapa 1: Planificación de análisis y gestión de riesgos

- Oportunidad de realización: se clarifica la oportunidad de realización.
- Definición del dominio y los objetivos: se especifica el dominio de los objetivos del proyecto.
- Planificación del proyecto: se planifican las entrevistas.
- Puesta en marcha del proyecto: seleccionar criterios de evaluación y técnicas para el proyecto, asignar los recursos necesarios.

Etapa 2: Análisis de riesgos

- Recogida de información: preparar la información.
- Identificación y agrupación de activos: identificar los grupos de activos y valorarlos.
- Identificación y evaluación de amenazas: identificar y agrupar las amenazas.
- Identificación y estimación de vulnerabilidades: identificar y estimar las vulnerabilidades.
- Identificación y valoración de impactos: identificar, tipificar y valorar los impactos.
- Evaluación del riesgo: evaluar y analizar el riesgo.

Etapa 3: Gestión de riesgos

- Interpretación del riesgo: interpretar los diferentes riesgos.
- Identificación y estimación de las funciones para proteger la información: identificar las funciones de protección.
- Seleccionar las mejores funciones de protección: aplicar parámetros de selección.
- Cumplir con los objetivos marcados: determinar el cumplimiento de los objetivos.

Etapa 4: Selección de medidas de protección

- Identificar mecanismos de protección de información: identificar, estudiar e incorporar restricciones.
- Selección de mecanismos de protección: identificar los diferentes mecanismos a implantar.
- Especificación de los mecanismos de implantación: especificar los mecanismos que implantar.
- Planificar la implementación: priorizar y evaluar los mecanismos.
- Integrar los resultados: integrar los resultados.

Ilustración 7 - Etapas de análisis de SGSI [12]

CONTROLES

En esta sección del documento se ilustra una serie de controles que fueron evidenciados como comunes en cualquier sistema de seguridad y que permiten asegurar cualquier arquitectura tecnológica o sistema de información de las empresas.

1. Registrar todos los intentos de entrada y salida de una red.
2. filtro de direcciones.
3. filtrado de protocolo.
4. Controlar el número de conexiones que se están produciendo desde un mismo punto.
5. Controlar las aplicaciones que pueden acceder a Internet.
6. Detección de puertos que están en escucha y en principio no deberían estarlo.
7. Copias de seguridad.
8. Verificación de cintas.
9. Recuperación de datos y reversión de cambios.
10. Administración de sistemas de antivirus.
11. Administración de usuarios y contraseñas.
12. Administración de acceso a los recursos.
13. Administración de acceso remoto.
14. Medición de desempeño.
15. Capacidad y disponibilidad de los recursos de TI.
16. Gestión de pistas de auditoria y sistemas de registro de información.
17. Aseguramiento de plataformas.
18. Adquisición, desarrollo y mantenimiento de equipos.

SITUACIÓN DE LA EMPRESAS Y TI

En la siguiente parte del documento se citan algunos fragmentos de artículos de diferentes entes las cuales hacen referencia a la situación que están viviendo las empresas con respecto a la adopción de tecnologías de la información (TI).

- Hasta un pequeño negocio como las tradicionales tienda de barrio pueden ampliar su base de proveedores y clientes, los canales de distribución, los campos de acción e incluso idear nuevos esquemas de protección. Con la tecnología todos están llamados a innovar, gracias a MiPyme vive digital, actualmente cerca Del 70% de las micro, pequeñas, y medianas compañías han aceptado el reto de utilizar tecnología en sus procesos. [13]

- Seguro que existen opciones para impulsar a las pequeñas y medianas empresas a que aumenten su nivel de adopción en tecnología; sin embargo, aún hace falta una integración de los prestadores de servicios de TI para lograr que esto suceda en un corto plazo. Por otra parte, es muy bueno que ya existan soluciones en el mercado que facilitan el acceso a aplicaciones de negocio y den la oportunidad a este tipo de empresas de contar con equipo de cómputo, comunicaciones e impresión, mediante esquemas de servicios integrales tales como SaaS (Software as a Service, por sus siglas en inglés), pero aun, se requiere de soluciones integrales basadas en una visión completa del negocio enfocadas en cada tipo de empresa, las cuales reúnan soluciones de diferentes proveedores mediante un punto de contacto, que permita a los empresarios liberarse de las actividades relacionadas con la administración de la tecnología para ocuparse de su negocio. Así, el gobierno de TI como primera etapa para impulsar la adopción de tecnología debería existir, pero en un esquema simplificado en el cual pudieran medir el valor que aporta la tecnología y exigir el cumplimiento de los niveles de servicio acordados, para incrementarlo en la medida en que el negocio crezca y la adopción de la tecnología aumente. [14]

Por lo anterior se puede llegar a la conclusión que hoy en día un valor agregado para una empresa en especial las es la implementación de tecnologías de la información, ya que no sólo la encamina al éxito de sus objetivos estratégicos, sino que las empresas también mejoran sus ganancias, generan más empleo, generan expansiones propias, elevan el nivel de competencia en el mercado, crean una mejor relación con sus clientes y proveedores y facilitan los procesos internos de la empresa.

También se puede decir que gracias a las labores de Mintic y a la creación de soluciones tecnológicas las empresas han perdido el temor a diferentes temas como invertir dinero en proyectos de tecnología, contratar personal para administrar el TI e implementar soluciones y formas de aseguramiento a la red.

También puede verse [15]

EDUCACIÓN DE TI EN COLOMBIA

A continuación se van a citar algunos fragmentos de artículos, documentos web y partes de noticias que nos dan una visión de cómo se encuentra la educación a nivel de TI.

El uso de medios de comunicación e información en las prácticas pedagógicas es un recurso indispensable para acercar el desarrollo de las competencias de los estudiantes a las dinámicas del mundo contemporáneo. La Revolución Educativa propone mejorar los aprendizajes fomentando el uso de los medios electrónicos, la televisión, la radio, el cine, el video y el impreso en el aula de clase. "Maestros y maestras son los ejes de este proceso para el tránsito de la enseñanza al aprendizaje" dijo Sonia Cristina Prieto, directora de Calidad Educativa de Preescolar, Básica y Media del Ministerio de Educación. [17]

Dice [18] el Ministerio de Educación Nacional ha llevado a cabo una política consistente para integrar las tecnologías de la información y de la comunicación (TIC) en su sistema educativo, dado que son un elemento eficaz para propiciar equidad, amplitud de oportunidades educativas y democratización del conocimiento. Al delinear el camino del uso pedagógico de las TIC, La publicación "Competencias TIC para el Desarrollo Profesional Docente" es el resultado de un trabajo liderado por la Oficina de Innovación Educativa del Ministerio de Educación, quienes se construyeron acuerdos conceptuales y lineamientos para orientar los procesos formativos en el uso pedagógico de las TIC.

Según la universidad ICESI [19] la misión del PNTI en**,** lograr un salto en la inclusión social y en la competitividad del país a través de la apropiación y el uso adecuado de las TIC, tanto en la vida cotidiana como productiva de los ciudadanos, las empresas, la academia y el Gobierno.

Estas y otras conclusiones que dicen las partes interesadas de los TICS, hacen pensar que en el enfoque de la educación en Colombia está la inclusión de los TIC en los jóvenes de nuestro país, como RELPE (red latinoamericana de portales educativos) que habla sobre enseñar el uso responsable de las TIC en la educación y es acá donde tanto en la educación como en la parte empresarial de nuestro país se deben generar nuevas y mejores campañas de concientización sobre el manejo adecuado de la información, el manejo que se le debe dar desde el punto de vista interno de cada empresa y el uso de las TIC en general.

Como se mencionó anteriormente concientizar el adecuado uso de la información por parte de las personas que la manipulan y las empresas que implementan el uso de tecnologías es muy importante ya que estas deben ser conscientes de los riesgos que existen, cómo los pueden afectar y cómo las herramientas que existen los puede apoyar a cubrir las brechas o huecos de seguridad.

Para lo anterior existen entes certificadores, capacitadores y generadores de buenas prácticas en Colombia y en el mundo, las cuales serán nombradas más adelante.

También puede verse [21]

DEFINICIÓN ARQUITECTURA EMPRESARIAL DEL NEGOCIO

Con la finalidad de que cualquier organización pueda implementar o le sirva de base esta propuesta de seguridad se debe definir claramente los alcances y la capacidad tecnológica, esto con el fin de tener la certeza que una empresa micro o una mediana empresa, con o sin altos recursos se verá beneficiada.

Ya que la arquitectura tecnológica (AT) hace parte de una arquitectura empresarial (AE) y para poder llegar a la AT debería existir una AE ya defina, motivo por el cual se pensó se debía crear una AE de ceros, sin embargo no se podía diseñar ya que es específica para un negocio y no se podría beneficiar si no a una parte de las empresas, por esta razón se evaluaron únicamente algunos aspectos de las AE, extrayendo de ellas los elementos comunes de las matrices DOFA, BPM, cadena de valor.

Lo anterior para poder conocer procesos, interesados, necesidades, equipos y del resultado de esta información se diseñaron las arquitecturas que podrían ser generales o comunes, arquitecturas que se evaluaran e ilustraran en el documento más adelante.

Se tomaron en cuenta las siguientes arquitecturas [2], [22], [23], [24].

SOLUCIONES SOFTWARE

Se realizó también un estudio de las áreas de la organización, procesos e información que cualquier empresa manipula, en este ejercicio se hizo una evaluación de soluciones software con el fin de evaluar que tantas aplicaciones podría tener una empresa, se tomaron aspectos de los beneficios que tiene, los costos que implica, las bases de datos se manejan, que servicios consumen y que soporte tiene.

Para esta tarea se realizó un análisis y se encontró que las aplicaciones que tiene una empresa para la operación son:

1. Facturas
2. Contabilidad, compras y ventas
3. Nomina
4. Inventario
5. Puntos de venta
6. CRM
7. Arqueo y cierres de cajas
8. Logística de transportes
9. Correo Electrónico
10. Comercio electrónico

Una vez evidenciadas las necesidades se realizó un estudio de cuáles podrían ser las opciones para que una empresa implemente sus ERP, para esto se van a ilustrar dos imágenes, la primera ilustra un Top de las mejores opciones de ERP que puede manejar la empresa las cuales tienen costo de licenciamiento y la segunda un Top por área de las aplicaciones que existen y tienen licenciamientos gratuitos.

Aplicaciones	Con licenciamiento	
Facturas	Alegra-SoftPymes	SAP Business one - SoftLand
Contabilidad	Alegra-SoftPymes	
Nomina	SoftPymes	
Inventario	OpenERP-SoftPymes	
Puntos de venta	Alegra	
CRM	Alegra	
Arqueo y cierres de caja		
Logistica de transporte		
Correo electrónico	Microsoft Outlook	
Comercio electrónico		

Ilustración 8 - ERP con costo de licenciamiento

Aplicaciones	Sin licenciamiento
Facturas	CoDeka - Hipergate - AhoraFreeware - Open Bravo - Dolibarr
Contabilidad	CoDeka - Hipergate-AhoraFreeware - Dolibarr - Open Bravo
Nomina	Orange HRM-AhoraFreeware - Dolibarr - Open Bravo
Inventario	OpenERP - Adempiere - Hipergate- AhoraFreeware - Dolibarr - Open Bravo
Puntos de venta	Lemon ubuntu - pos Colombia- Dolibarr
CRM	Open bravo - Adempiere- AhoraFreeware
Arqueo y cierres de caja	AhoraFreeware
Logistica de transporte	OpenBravo - AhoraFreeware - Dolibarr
Correo electrónico	Hipergate - Dolibarr - Opencrx
Comercio electrónico	Dolibarr

Ilustración 9 - ERP sin costo de licenciamiento

Con la finalidad que la empresa centralice sus actividades operacionales a costo razonable, la empresa puede trabajar con los ERP "Ahora freeware" y "Dolibarr" ya que no tienen costos de licenciamiento y brindan una opción de mantenimiento, asesoría, trabajan con un Motor de MS SQL, SQL server o MySQL lo que le beneficiaria a la organización para hacer más fácil la conexión entre la aplicación y la base de datos propuesta, además también tienen conexiones con Excel, esto implicaría que no necesariamente tienen que tener una persona que conozca de modelado de SQL para poder adoptar los ERP.

MODELO DE APLICACIONES

Una vez evidenciados los elementos y servicios comunes que toda empresa tiene se definió una arquitecta de aplicaciones que cumpliera con las necesidades de cualquier negocio partiendo de los servicios que podrían tener, la comunicación entre dichos servicios, el usuario y las aplicaciones, se decidió utilizar dos ERP, aplicaciones de seguridad, aplicaciones básicas como lo es office y el host de la página web; Se definió un bus de servicios empresariales con el fin que si la empresa lo necesita o ve importarte pueda tener comunicadas las aplicaciones y los servicios centralizados.

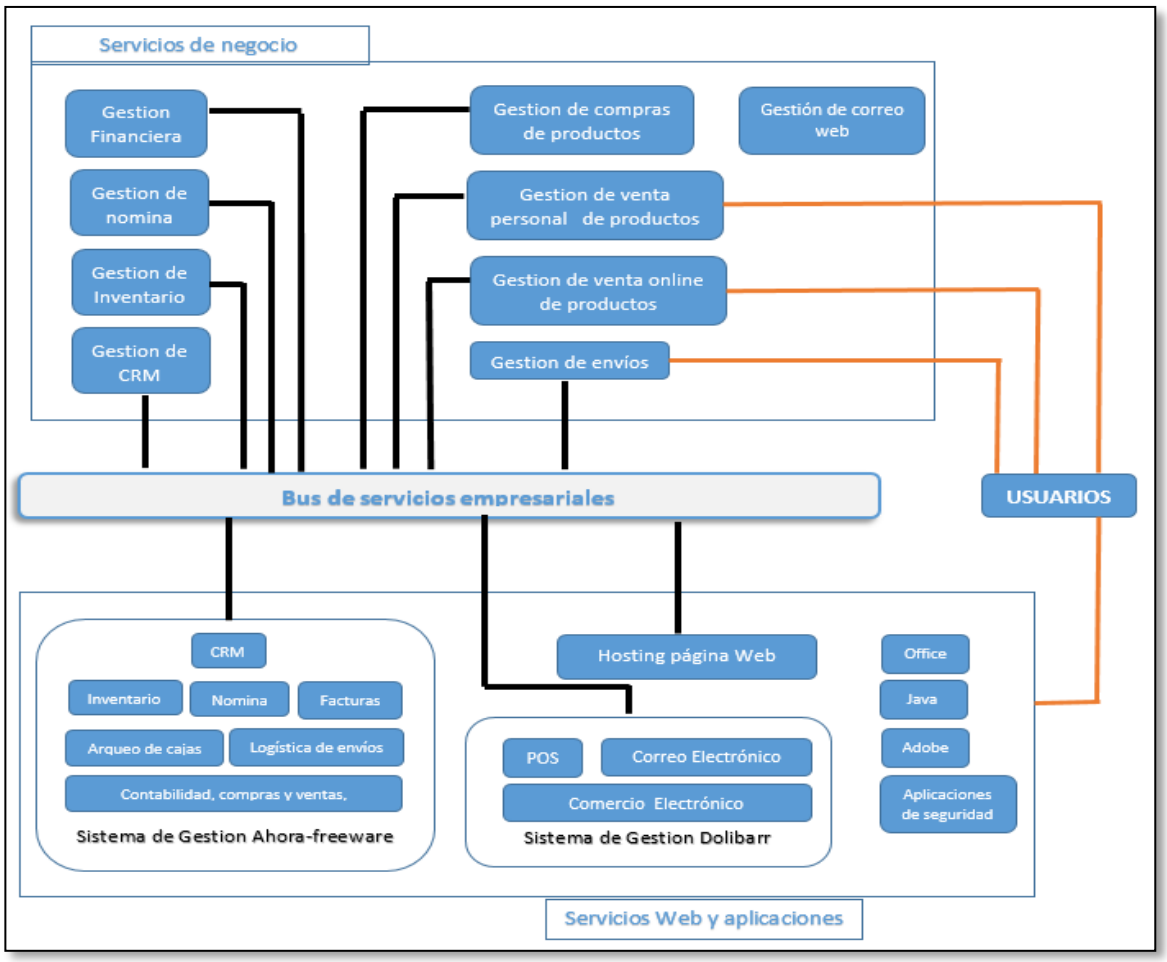


Ilustración 10 - Arquitectura de aplicaciones

ELEMENTOS DE UNA PLATAFORMA DE TI

Para poder identificar los elementos comunes de la plataforma de TI se realizó un estudio previo sobre los elementos físicos, lógicos y humanos con los que contaban la mayoría de plataformas, a continuación vamos a ilustrar una imagen de dichos elementos.

Estos elementos fueron encontrados en la mayoría las arquitecturas empresariales y tecnológicas publicadas en internet, en las siguientes citas se encuentran algunos documentos, artículos e imágenes que permitieron identificarlos [12], [13], [14], [15], [16], [17], [18], [19], [20], [21].

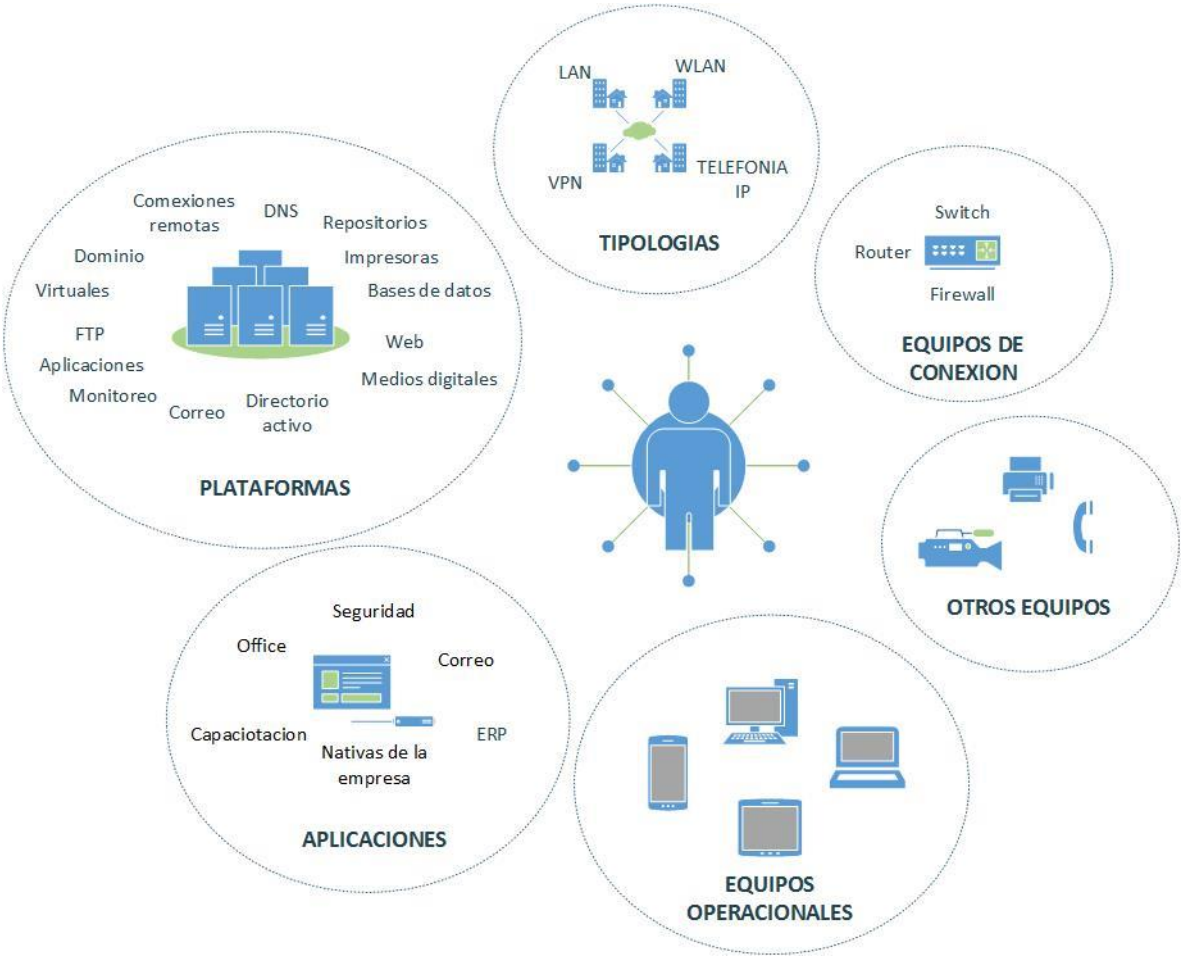


Ilustración 11 - Elementos de una arquitectura tecnológica

En esta imagen se evidencian los elementos que componen una arquitectura tecnológica y que son utilizados comúnmente por las organizaciones diferenciados en grupos, en las **plataformas** se pueden observar los servidores que soportan la operación, conexiones, información y equipos de la empresa, en el de **grupo de aplicaciones** se encuentran las aplicaciones de seguridad, las comunes como paquetes de office y adobe, las desarrolladas por la empresa para su proceso y los ERP(Enterprise Resource Planning – Planificación de Recursos Empresariales) que manejen; En el **grupo de topologías** se observan las redes que utilizan las empresas como lo son LAN, WLAN, VPN

y telefonía IP; En los **dispositivos de conexión** están los dispositivos hardware que permiten la conexión de los equipos a la red, estos pueden ser propios de la empresa o los que ofrece el ISP(Internet Service Provider**)**, en los **equipos operacionales** se ilustran los equipos de cómputo que pueden ser parte de la red como equipos de mesa, portátiles, celulares o tabletas y en el **grupo de otros equipos** se encuentran los equipos, máquinas o dispositivos como lo son telefonía por IP, cámaras, impresoras o scanner.

Una vez identificados todos los elementos comunes, se buscó un modelo que ayuda a definir los elementos que necesariamente debería tener una arquitectura tecnológica de una empresa para su funcionamiento, para esto nos apoyamos en el modelo de seguridad en profundidad o esquema de arquitectura de seguridad promovido por Microsoft, aunque es un modelo que propone acciones para asegurar capas, este modelo dio una idea de que elementos eran los que podrían existir en cada una de las capas, es decir, al existir una capa de datos se evaluó la opción de tener un servidor de base de datos y así con cada capa.

Este modelo no solo funciono para definir los elementos necesarios sino que también brindo una idea a futuro de cómo asegurar cada una de estas capas, es decir cómo asegurar cada uno de los elementos que se definieron.

A continuación vamos a ilustrar las capas del modelo de seguridad en profundidad y la definición de cada una de ellas.

CAPA	Finalidad
Datos	Manejar los datos de manera segura
Aplicaciones	Organización, centralización y controles para que las aplicaciones sean seguras
Host	Asegurar servidores y estaciones de trabajo
Internet	Asegurar trafico de la red y conexiones
Perimetral	Asegurar la red LAN y WAN de la organización
Seguridad Fisica	Asegurar los equipos fisicos y lugares fisicos
Politicas y procedimientos	Politicas de la empresa para asegurar la información

Ilustración 12 - Modelo de seguridad en profundidad

PROPUESTA ARQUITECTURA TECNOLÓGICA

Con base en los elementos comunes de las arquitecturas tecnológicas y con el apoyo de la arquitectura de datos, arquitectura de aplicaciones y el modelo de seguridad de Microsoft se diseñó la arquitectura tecnológica, vale la pena aclarar que estos elementos son una propuesta y la implementación de ellos depende de las necesidades tecnológicas de cada empresa, estas necesidades deben ser definidas por una persona que conozca de tecnología y del negocio. Lo anterior quiere decir que no necesariamente una empresa tiene que tener todos estos elementos propuestos para tener una buena arquitectura tecnológica, sin embargo si pueden servir como una guía empresarial de los elementos que existen y de cómo y para que los pueden utilizar en la organización.

A continuación se ilustran dichos elementos asociados al modelo de seguridad en profundidad.

	Equipos de control y servidores de control
Datos	Servidores de bases de datos, repositorios y información equipos
Aplicaciones	Servidor de aplicaciones
Host	Todos los servidores y equipos(Pc de mesa, portatiles, celulares, tablets, remotos)
Internet	Equipos de control y servidores de control
Perimetral	Servidores(Directorio activo, DNS, DHCP) y equipos(Pc de mesa, portatiles, celulares, tablets)
Seguridad Fisica	Todos los servidores y equipos(Pc de mesa, portatiles, celulares, tablets)
Politicas y procedimientos	Servidor DNS y directorio activo

Ilustración 13 - Elementos de la arquitectura necesarios

De los elementos que se pueden observar en la imagen anterior, se construyó y diseño una arquitectura tecnológica la cual se ilustra a continuación.

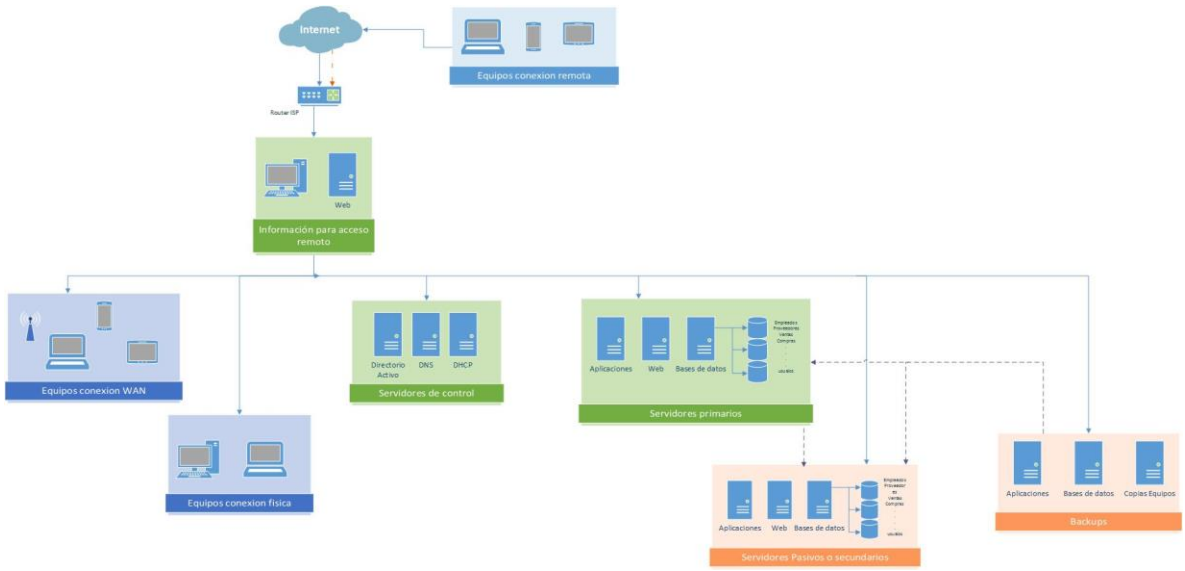


Ilustración 14 - Arquitectura tecnológica común

Se propone una arquitectura con diferentes segmentos de red o zonas, las cuales se ilustran con diferentes colores; Se puede observar la zona con los servidores y equipos donde estará la información de la empresa y que podrían ayudar al control de la red (**Verde**), los equipos que se pueden conectar a la red (**Azul**) y los servicios y elementos que permitirán darle continuidad al negocio (**Naranja**).

En la zona verde y con el fin de tener identificados las IP y los equipos, tener políticas de seguridad de los equipos de la red y poder crear zonas de autoridad si se requiere, se recomienda implementar un servidor DNS (sistema de nombres de dominio), también se recomienda tener un servidor de directorio activo para crear políticas de grupo, asignar políticas de contraseñas, identificar y autorizar los equipos, Se recomienda también implementar servicios o protocolos DHCP para distribuir y controlar las IP de la red.

- **Servidor de aplicaciones:** Se propone alojar las aplicaciones o ERP de la empresa para tenerlas controladas y actualizadas desde un servidor y no desde cada equipo cliente de la empresa, y como no se conoce una dimensión futura pero si se espera que tener una gran cantidad de equipos, es más fácil para tener las aplicaciones montadas en un servidor aplicaciones o en un host y desde allí darle el soporte o mantenimiento.

- **Servidores de bases de datos**: En estos servidores se encuentra la información de la operación de la empresa y datos que cada empresa considere tener ya sea en uno o varios servidores del mismo tipo.

- **Servidor web**: Allí se puede alojar la información, aplicaciones o página web.

Se propone tener en esta zona verde un segmento aislado para accesos remotos y allí alojar la información que va a ser autorizada para acceder por equipos desde el exterior de la red.

En la zona azul se contemplaron los equipos cliente que podrían conectarse a la red, se definieron los equipos de mesa, portátiles, celulares, tabletas u otros equipos de su línea y se propone ubicarlos de acuerdo a su conexión a la red en tres segmentos de red aislados, los que tienen conexión inalámbrica, los que se conectan físicamente por cable y los que accederán remotamente a la información, con el objetivo de tener diferenciadas las políticas, aseguramientos, mecanismos y cualquier tipo de control necesario.

Se sugiere para la continuidad del negocio tres tipos de soluciones, la primera es tener un esquema de alta disponibilidad, para este se propone tener conectividad a internet con un segundo ISP por si en algún momento hay fallas en la red del ISP principal, la empresa y sus operaciones se soporten con otro proveedor de internet, el segundo es tener un segmento de red aislado con servidores espejo, preferiblemente en una ubicación física distinta, por si los servidores primarios sufren algún daño provocado o natural, se tengan unos servidores que funcionen igual y no se vea afectada la operación y como tercer elemento se plantea contar con un segmento aislado de servidores donde se encuentren los backup o repositorios de la empresa.

EVALUACIÓN DE AMENAZAS Y RIESGOS

Una vez establecida la arquitectura tecnológica se procedió a realizar un análisis de amenazas y riesgos, este análisis se realizó con el apoyo de algunas de las características de la ISO27001 y su SGSI.

Para la etapa de **planificación de análisis y gestión de riesgos** se definieron los servicios básicos y una lista de activos que son comunes en todas las organizaciones, en la segunda etapa de **análisis de riesgos** se definieron los riesgos, vulnerabilidades y la posibilidad de materialización, en la etapa de **gestión de riesgos** se crearon las políticas y procesos de seguridad para mitigarlos y se asociaron a los activos o equipos que podría afectar y por último en la etapa de **selección de herramientas de control** se hizo un análisis previo de las herramientas que permitían cumplir los dos puntos anteriores.

De las etapas anteriores se definieron una serie de herramientas y mecanismos que aseguran la arquitectura y apoyan al cumplimiento de las políticas definidas.

Estos documentos se pueden observar en los archivos anexos.

ACTIVOS

Anexo 1: Análisis de riesgos y controles hoja Activos comunes.

RIESGOS

Anexo 1: Análisis de riesgos y controles hoja Riesgos o amenazas.

POLÍTICAS DE CONTROL

Anexo 1: Análisis de riesgos y controles hoja Políticas de activos.

HERRAMINETAS Y MECANISMOS DE SEGURIDAD

Anexo 1: Análisis de riesgos y controles hoja Herramientas de seguridad.

SOLUCIONES DE SEGURIDAD

Una vez se evidenciaron las herramientas y mecanismos de seguridad que hacían que se cumplieran las políticas y aseguraban la información de la empresa, se realizó una búsqueda de fabricantes de cada herramienta de preferencia que cubrieran los sistemas operativos Windows, Linux y Mac, lo anterior con la finalidad de poder asegurar cualquier arquitectura independiente al sistema operativo que utilicen sus equipos.

En el archivo anexo se podrá encontrar una lista de los fabricantes asociados a los sistemas operativos con los que puede operar.

Para definir estas soluciones nos apoyamos en los siguientes documentos [22], [23], [24], [25], [26], [27] y el resultado se puede observar en el archivo anexo.

En seguida se ilustra un listado de los fabricantes de las herramientas asociados a los sistemas operativos.

Fabricantes	Linux	Windows	Mac Os	Otro	Mobiles
Ipcop	x				
PfSense				x	
Zone alarm		x			
Comodo(LOCAL)	x	x	x		
MyDb -studio				x	
handy BuckUp				x	
ApexSQl				x	
Snort	x	x			
suricata	x	x			
Avira		x	x		x
AVG		x	x		x
Clamav	x		x		x
Avast	x	x	x		
Truecryp	x		x		
GNUPG		x	x		
fileVault			x		
OpenLDAP	x				
Active diretory		x			
OS X Server			x		
Nessus	x	x			
OSSEC(hids)	x	x	x		
Free radius	x	x			
EaseUS		x	x		
Time machine			x		
Server radius			x		
OpenVPN	x	x	x		
Hotspot Shield		x	x		
ES file manager					x
Easy Recovery		x			
Event log explorer		x			
Logalyze	x				
OSSIM	x	x	x		
Norton		x	x		x
TestDisk	x	x	x		

FABRICANTES

Anexo 1: Análisis de riesgos y controles hoja Fabricantes herramientas.

ARQUITECTURA TECNOLÓGICA CON ELEMENTOS DE SEGURIDAD

Ya identificados los elementos de la arquitectura tecnológica y las herramientas de seguridad diseñamos la siguiente propuesta de arquitectura tecnológica con elementos de seguridad, la cual hace parte de uno de los entregables principales del proyecto ya que en esta se plasman los primeros 4 objetivos específicos.

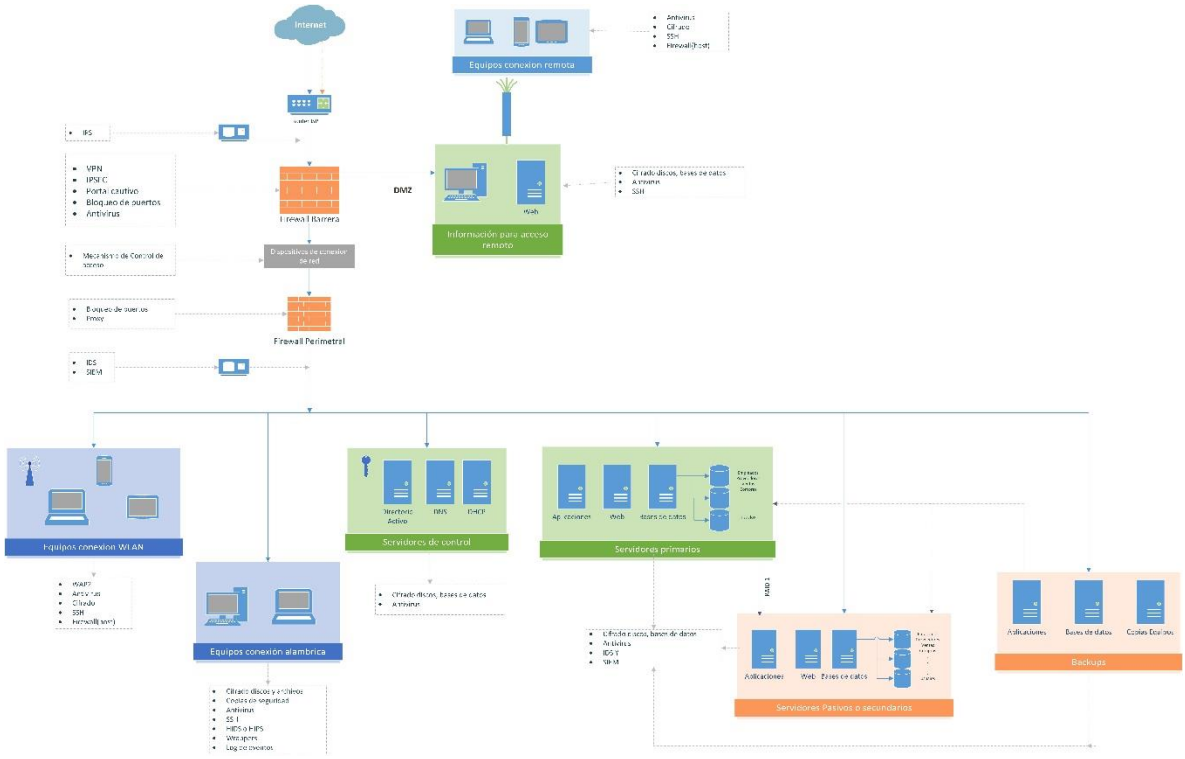
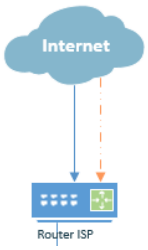
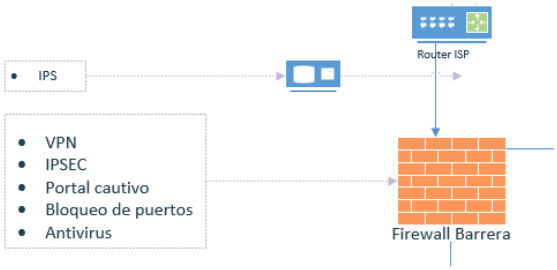


Ilustración 15 - Arquitectura tecnológica y herramientas de seguridad

En el capítulo de arquitectura tecnológica común se describe la razón de segmentar por zonas y por qué se eligieron cada uno de los servidores. En este nuevo capítulo se especifica porque se eligieron las soluciones de seguridad para cada área y las recomendaciones de los mismos.

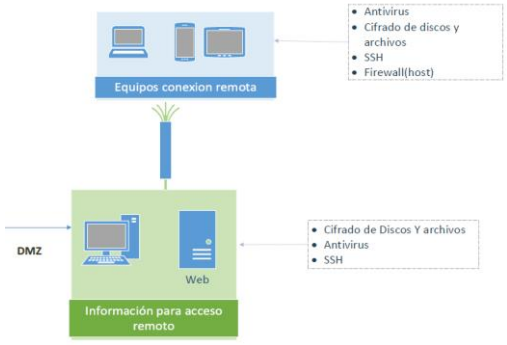


Con el fin de generar disponibilidad de los sistemas y continuidad al negocio, la empresa puede establecer una segunda conexión de internet por si la principal falla y no afectar las operaciones que necesiten conexión a internet.



Como se espera que existan aplicaciones que se conecten a internet y si la empresa autoriza conexión internet desde los equipos se propone tener herramientas de monitoreo y control en el borde de la red, para esto la empresa puede utilizar una solución IPS (sistema de prevención de intrusos) que permite monitorear el tráfico de la red, detectar cambios y ataques de la red e intentar detener o distraer dichos ataques.

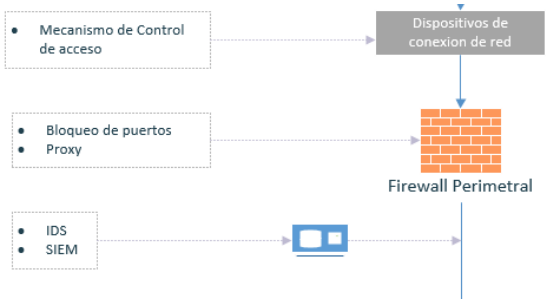
Seguida a esta solución se propone que la empresa implemente un firewall de borde preferiblemente de nueva generación con el fin de aprovechar la capacidad de análisis exacto de aplicaciones y no solo puerto/protocolo, mecanismos como VPN, portal cautivo, radius, filtrado de contenido, analizar dispositivos, bloqueo de puertos y demás controles que permita la herramienta, sin embargo si la empresa no lo ve necesario puede implementar un firewall tradicional que permita control de servicios, puertos, usuarios, excepciones, comportamientos, etc.



Hoy en día se necesita acceder a los recursos de la empresa desde el exterior de la misma es por eso que se espera que algunos equipos accedan remotamente, se propone tener un segmento en el borde de la red donde se ubiquen los servidores o equipos que tengan los recursos autorizados para ser accedidos desde el exterior de la empresa, con el fin de que los equipos que se conecten remotamente y no tengan que viajar hasta la LAN para acceder a la información; Se propone que la conexión remota se haga a través de una VPN(Virtual Prívate Network en español red privada virtual) y así poder tener una conexión segura, políticas de gestión de una red privada y una comunicación cifrada.

Con el fin de no utilizar tantas herramientas y equipos se puede implementar el servidor VPN en el firewall de borde.

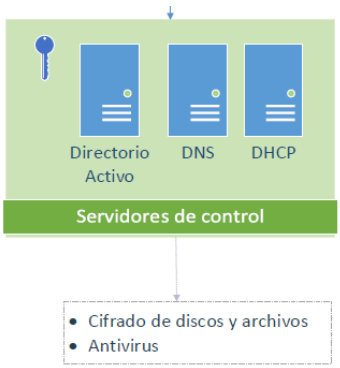
Se propone también instalar en todos los equipos que hagan parte de esta conexión mecanismo ssh (secure Shell o en español interprete de ordenes seguras), cifrado de alto nivel de los discos y de la información, certificados digitales SSL y antivirus tanto en los equipos remotos como en los servidores.



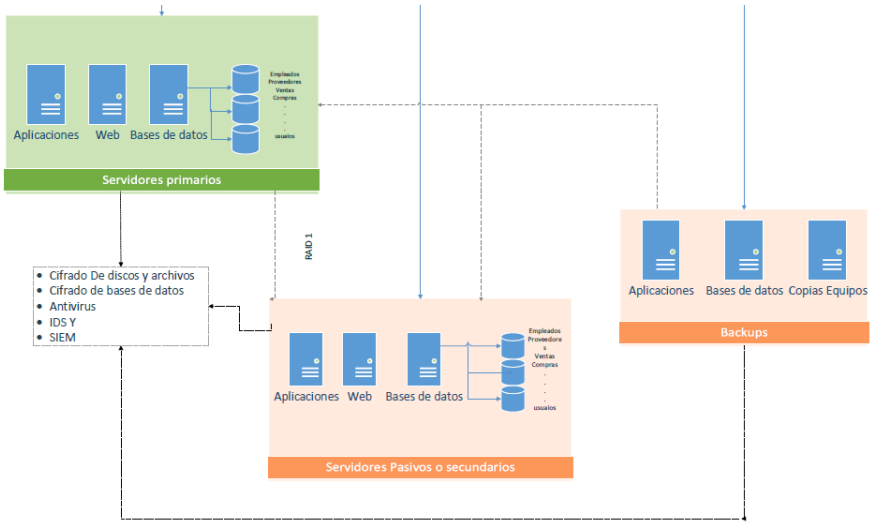
En este segmento de la red se evidencia el dispositivo de conexión que elija la empresa, ya sea un router o un switch, se propone que dicho mecanismo tenga implementado NAC(Network Access Control en español control de acceso a la red) con el fin de asegurar los puertos de conexión.

Seguido al este dispositivo se podría implementar un firewall perimetral para no recargar operativamente el firewall de borde, este no necesariamente tiene que ser de nueva generación ya que con este se busca realizar una configuración proxy, realizar filtrado de contenido, filtrado de equipos en la red interna y bloqueo de puertos.

Se sugiere tener monitoreada también la red interna con el fin de detectar posibles ataques o anomalías desde alguno de los dominios internos de la empresa, para esta gestión se puede utilizar un IDS (Sistema de detección de intrusos) y primordial implementar un centralizador de eventos como un SIEM (Información de seguridad y administración de eventos) ya que este SIEM no solo nos puede centralizar eventos si no también analizarlos, en algunos caso prevenirlos y realizar análisis de vulnerabilidades.



Se recomienda utilizar en estos servidores sistema de cifrado de discos y archivos, antivirus, cifrado de bases de datos, copias de seguridad de la información e implementar un IDS o HIDS para conocer y alertar los eventos de estas máquinas.



Se evidencio la necesidad de tener los servidores core de la organización en otro segmento de red con la finalidad que todos los accesos a la información o recursos que estén alojados en estos sean monitoreados y autorizados por cada uno de los controles, con eso aseguramos que las personas y equipos que accedan a los recursos se encuentren autorizada. Para tener disponibilidad y continuidad de los servicios de la empresa se recomienda tener servidores espejo los cuales se encuentren en otro segmento de red por si existe algún inconveniente con los principales se puedan direccionar los servicios de la empresa a los estos, de igual manera tener un backup de la información o equipos que se consideren importantes para la organización en otro segmento de red por si los servidores core o espejos son víctimas de ataques o daños existan unas copias de seguridad y no afecten la continuidad del negocio.

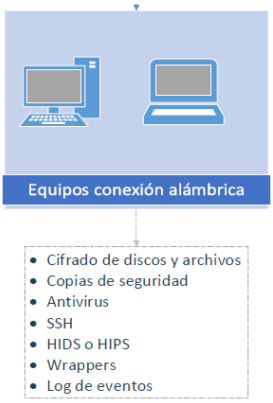
En estos equipos se pueden implementar mecanismos de cifrado, antivirus y de preferencia un sistema de detección de intrusos, apoyado con una herramienta SIEM para tener analizado la red e identificar cambio o posibles ataques a los servidores primarios.

Para el servidor de Bases de datos se encontraron herramientas como Cifrado centralizado de gestión de claves, cifrado de las claves de la red y bases de datos, Database security, MyDb -studio con el fin de crear controles técnicos, procedimientos, administración de equipos físicos, cifrados y copias de seguridad.

En otro segmento de la red encontramos los dispositivos que se conectan por WiFi, estos dispositivos se recomienda estén en un segmento diferente para tenerlos diferenciados de los que se conectan físicamente por cable y poder crear e implementar mecanismos de seguridad propios como método de autenticación WAP2, control de MAC, protocolos de autenticación como a través de portal cautivo o radius y así asegurar la correcta prestación de servicios los servicios por este canal y asegurarse que las personas que se conecten estén autorizadas a hacerlo.

Preferiblemente estos equipos deberían implementar mecanismo como SSH, cifrado de discos y de información, programas de monitoreo de ejecuciones de aplicaciones como wrappers, protocolos de autenticación WAP2 y antivirus.

Si estos equipos que se conectan una red WiFi diferente a la de la empresa debe tener todas las herramientas anteriores más un firewall de host, ya sea el nativo del sistema operativo o algún firewall que se pueda instalar en los equipos para poder asegurarse que no sufrirán ninguna afectación por estar conectados a otra red.



Por los motivos anteriores se recomienda tener en otro segmento de red los equipos que se conectan físicamente e implementar herramientas propias para estos como antivirus, cifrado de discos y archivos, wrappers para evitar ejecución de aplicaciones en segundos planos, protocolos ssh para conexiones seguras, HIDS para monitorear la red y por ultimo mecanismos de registro de las actividades de red del equipo los cuales estén centralizados en logs. Para asegurar la continuidad del negocio la organización podría implementar una herramienta para tener un backup o copia de seguridad de la información de cada equipo.

Con el fin de garantizar el correcto estado de la información, equipos y host se recomienda tener implementadas herramientas para monitorear vulnerabilidades de la red o de los host y análisis de virus.

MATRIZ DE EVALUACIÓN

Para integrar a la propuesta las herramientas de control más sobresalientes y que favorezcan más a asegurar la arquitectura tecnológica se realizó una comparación de los diferentes fabricantes de cada herramienta, para ello se instaló, configuró, probó y calificó de cada herramienta.

Para el proceso de calificación se construyó una matriz de evaluación la cual define criterios comunes para calificar una herramienta software como lo son usabilidad, eficiencia, fiabilidad, portabilidad, costos y características propias o características específicas de cada una de las herramientas por ejemplo para el caso de los antivirus saber si se caracteriza por tener heurística, HIDS, mecanismo de VPN, entre otros.

El método de calificación propuesto fue poner una serie de (x) en cada uno de los criterios que cumpla la herramienta y anotar las observaciones que se consideren importantes en la calificación.

A continuación se ilustra la matriz de evaluación, en esta matriz se evidencian los criterios comunes evaluados.

Perspectiva	Descripción	Criterio/herramienta
Funcionalidad	Capacidad para satisfacer las necesidades de la herramienta	Adecuación
	Capacidad de intercambiar información y utilizar información de otros sistemas	Interoperabilidad
Características	Características propias	Cumplimiento de característica
Fiabilidad	Realiza o es fácil hacer buckup de la información	Recuperabilidad
Eficiencia	Consumo de bajos recursos	Utilización de recursos
Portabilidad	Capacidad de operar frente a otros software	Coexistencia
	Pasos para la instalación del software o herramienta sencillos	Facilidad de instalación
	Facilidad de instalación de diferentes sistemas operativos	Adaptabilidad
Usabilidad	Facilidad para manipular o operar	Operatividad
	Tiempo corto para realizar configuración	productividad
Costo	sin costo de la adquisición del software	Costo
	sin costo por el soporte técnico de la herramienta	Soporte

COPIAS DE SEGURIDAD

Matriz de evaluación

Anexo 2: Matriz evaluación.

IMPLEMENTACIÓN

Se realizó la instalación de las herramientas en máquinas virtuales con el programa VMWare Workstation 12, en esta implementación se instalaron, configuraron y se probaron conexiones, funcionamiento básicos, para luego calificar cualitativamente cada una de las herramientas.

Se utilizaron los sistemas operativos Windows 7, Windows 8.1, Linux mint, Linux Ubuntu y Mac.

Como resultado de este proceso se definió un cuadro el cual ilustra los fabricantes sobresalientes a los demás, asociados a la herramienta de control y al sistema operativo, en algunos campos se evidencian dos herramientas, en este caso es porque ambas fueron las superiores y tuvieron el mismo puntaje.

	Herramientas superiores		
Herramientas	Windows	Linux/ Unix	Mac Osx
Firewall	Comodo	Ipcop, Pfsense	-
IPS y HIPS	Snort, Suricata	Snort, Suricata	-
Antivirus	Norton	Comodo	Avast, ClamAV
Cifrado discos y archivos	GnuPG	Truecrypt	GnuPG, Truecrypt
Sistemas de directorios activos	Windows server	OpenLDAP	Osx server
IDS y HIDS	OSSEC	OSSEC	OSSEC
Logs y recuperación	Event log explorer	Event log explorer	Norton antivirus, Clamav
Portal cautivo, Radius	FreeRadius	Pfsense	Server radius
VPN	OpenVPN	OpenVPN	
SIEM	OSSIM	OSSIM	OSSIM
Copias de seguridad y recuperación de archivos	EaseUS	Testdisck	EaseUS

Se realizó un video de cada una de las herramientas probadas, a continuación se ilustrara la evaluación de las herramientas escogidas como más adecuadas.

FIREWALL

Perspectiva	Descripción	Criterio/herramienta	IPCOP	PFSENSE	COMODO
			Linux	Unix	Windows
Funcionalidad	Capacidad para satisfacer las necesidades de la herramienta	Adecuación	x	x	x
	Capacidad de intercambiar información y utilizar información de otros sistemas	Interoperabilidad	x	x	
Características	Identificar aplicaciones y no solo puertos	Cumplimiento de característica			
	Balanceo de carga			x	
	NAC o NAT		x	x	
	Políticas de acceso		x	x	x
	Protección contra malware basada en red		x		x
	IDS o IPS		x		x
	VPN o IPSec		x	x	x
	Portal cautivo o radius			x	
	Configuraciones básicas		x	x	x
Fiabilidad	Realiza o es fácil hacer buckup de la información	Recuperabilidad	x	x	
Eficiencia	Consumo de bajos recursos	Utilización de recursos	x	x	x
Portabilidad	Capacidad de operar frente a otros software	Coexistencia			x
	Pasos para la instalación del software o herramienta sencillos	Facilidad de instalación	x	x	x
	Facilidad de instalación de diferentes sistemas operativos	Adaptabilidad			x
Usabilidad	Facilidad para manipular o operar	Operatividad	x	x	x
	Tiempo corto para realizar configuración	productividad	x	x	x
Costo	x : sin costo de la adquisición del software, - : tiene prueba gratis	Costo	x	x	x
	sin costo por el soporte técnico de la herramienta	Soporte	x	x	
			15	15	13

CIFRADO

Perspectiva	Descripción	Criterio	TrueKryp		GNUPG	
			Linux	MAC	MAC	Windows
Funcionalidad	Capacidad para satisfacer las necesidades de la herramienta	Adecuación	x	x	x	x
	Capacidad de intercambiar información y utilizar información de otros sistemas	Interoperabilidad				x
Características	Cifrado de datos y archivos	Cumplimiento de característica	x	x	x	x
	Cifrado de discos		x	x	x	x
	PGP					x
	Paralelización		x			
	firmas digitales			x	x	x
	Cantidad de algoritmos aceptados -:menos de 3 a 5 o x: mas de 5		x	x	x	x
Fiabilidad	Realiza o es fácil hacer buckup de la información	Recuperabilidad				
Eficiencia	Consumo de bajos recursos	Utilización de recursos	x	x	x	x
Portabilidad	Capacidad de operar frente a otros software	Coexistencia	x	x	x	x
	Pasos para la instalación del software o herramienta	Facilidad de instalación	x	x	x	x
	Facilidad de instalación de diferentes sistemas operativos	Adaptabilidad	x	x	x	x
Usabilidad	Facilidad para manipular o operar	Operatividad	x	x	x	x
	Tiempo para realizar configuración	productividad	x	x	x	x
Costo	sin costo de la adquisición del software	Costo	x	x	x	x
	sin costo por el soporte técnico de la herramienta	Soporte	x	x	x	x
			13	13	13	15

ANTIVIRUS

Perspectiva	Descripciòn	Criterio	Avast	Norton	Comodo	Clamav
			MAC	Windows	Linux	MAC
Funcionalidad	Capacidad para satisfacer las necesidades de la herramienta x:pasa pruebas -:no detecta pruebas	Adecuaciòn	x	x	-	x
	Capacidad de intercambiar informaciòn y utilizar informacon de otros sistemas	Inteoperabilidad				
Caracteristicas	Heuristica	Cumplimiento de caracteristica	x	x	x	
	Generaciòn log antivirus		x	x	x	x
	Generaciòn logs equipo					x
	Detección mínima de falsos positivos o falsos virus		x	x	x	x
	Integración con el correo electrónico		x	x	x	x
	Capacidad de recuperacionde discos y herramienta		x	x		
	HIDS O HIPS			x		
	VPN		x			x
	Servicios de proxy		x	x	x	x
	Analisis de archivos y discos		x	x	x	x
	Veracidad de eliminacion de virus		x	x	x	x
	Control remoto					
	Consola de control de mando		x		x	x
Fiabilidad	Realiza o es facil hacer buckup de la informaciòn	Recuperabilidad		x		
Eficiencia	Consumo de bajos recursos menos de 30 MB	Utilizaciòn de recursos	x		x	x
Portabilidad	Capacidad de operar frente a otros software	Coexistencia	x	x	x	x
	Pasos para la instalaciòn del software o herrmamienta	Faciliad de instalaciòn	x	x	x	x
	Facilidad de instalaciòn de diferentes sitemas operativos	Adaptabilidad	x	x	x	x
Usabilidad	Faciliad para manipular o operar	Operatividad	x	x	x	x
	Tiempo para realizar configuraciòn	productividad	x	x	x	x
Costo	sin costo de la adquisicion del software, - : tiene version gratuita, x : es totalmente gratis	Costo	-	-	x	x
	sin costo por el soporte tecnico de la herramienta	Soporte	x		x	x
			18	16	16	18

IPS

Perspectiva	Descripción	Criterio	snort
			Windows
Funcionalidad	Capacidad para satisfacer las necesidades de la herramienta alto	Adecuación	x
	Capacidad de intercambiar información y utilizar información de otros sistemas	Interoperabilidad	x
Características	Generación alertas y reglas	Cumplimiento de característica	x
	Capacidad de prevenir intrusos		x
	Detección de rootkids y virus		
	Análisis de log y archivos		x
	Scanner de vulnerabilidades		
	Capacidad de detener ataques		x
	Capacidad alta de análisis		x
Fiabilidad	Realiza o es fácil hacer backup de la información	Recuperabilidad	x
Eficiencia	Consumo de bajos recursos	Utilización de recursos	x
Portabilidad	Capacidad de operar frente a otros software	Coexistencia	x
	Pasos para la instalación del software o herramienta	Facilidad de instalación	-
	Facilidad de instalación de diferentes sistemas operativos	Adaptabilidad	x
Usabilidad	Facilidad para manipular o operar	Operatividad	-
	Tiempo para realizar configuración	productividad	-
Costo	sin costo de la adquisición del software	Costo	x
	sin costo por el soporte técnico de la herramienta	Soporte	x
			13

IDS

Perspectiva	Descripción	Criterio	OSSEC		
			Windows	Linux	MAC
Funcionalidad	Capacidad para satisfacer las necesidades de la herramienta alto	Adecuación	x	x	x
	Capacidad de intercambiar información y utilizar información de otros sistemas	Interoperabilidad	x	x	x
Características	Generación alertas y reglas	Cumplimiento de característica	x	x	x
	Capacidad de prevenir intrusos				
	Detección de rootkids y virus		x	x	x
	Análisis de log y archivos		x	x	x
	Scanner de vulnerabilidades				
	Capacidad de detener ataques				
	Capacidad alta de análisis		x	x	x
Fiabilidad	Realiza o es fácil hacer backup de la información	Recuperabilidad	x	x	x
Eficiencia	Consumo de bajos recursos	Utilización de recursos			
Portabilidad	Capacidad de operar frente a otros software	Coexistencia	x	x	x
	Pasos para la instalación del software o herramienta	Facilidad de instalación	x	x	x
	Facilidad de instalación de diferentes sistemas operativos	Adaptabilidad	x	x	x
Usabilidad	Facilidad para manipular o operar	Operatividad	x	x	x
	Tiempo para realizar configuración	productividad	x	x	x
Costo	sin costo de la adquisición del software	Costo	x	x	x
	sin costo por el soporte técnico de la herramienta	Soporte	x	x	x
			14	14	14

LOG

Perspectiva	Descripción	Criterio	Event log explorer
			Windows
Funcionalidad	Capacidad para satisfacer las necesidades de la herramienta	Adecuación	x
	Capacidad de intercambiar información y utilizar información de otros sistemas	Interoperabilidad	x
Características	Análisis de diferentes equipos en la red	Cumplimiento de característica	x
	Log de sistema		x
	Log de aplicaciones		x
	Análisis de eventos		x
	Capacidad alta de análisis		x
Fiabilidad	Realiza o es fácil hacer backup de la información	Recuperabilidad	
Eficiencia	Consumo de bajos recursos	Utilización de recursos	x
Portabilidad	Capacidad de operar frente a otros software	Coexistencia	x
	Pasos para la instalación del software o herramienta	Facilidad de instalación	x
	Facilidad de instalación de diferentes sistemas operativos	Adaptabilidad	x
Usabilidad	Facilidad para manipular o operar	Operatividad	x
	Tiempo para realizar configuración	productividad	x
Costo	sin costo de la adquisición del software	Costo	x
	sin costo por el soporte técnico de la herramienta	Soporte	
			14

PORTAL CAUTIVO

Perspectiva	Descripción	Criterio	Pfsense	Free radius
			FreeDBS- Unix	Windows
Funcionalidad	Capacidad para satisfacer las necesidades de la herramienta	Adecuación	x	x
	Capacidad de intercambiar información y utilizar información de otros sistemas	Interoperabilidad		x
Características	Conexión segura	Cumplimiento de característica	x	x
	Conexión Estable WAN		x	x
	Conexión Estable LAN		x	
	Asignación de velocidad		x	x
	Autenticación como servidor radius		x	x
	Portal cautivo		x	
	Control de conexiones		x	x
	Asistente de consola		x	
Fiabilidad	Realiza o es fácil hacer backup de la información	Recuperabilidad		
Eficiencia	Consumo de bajos recursos	Utilización de recursos	x	x
Portabilidad	Capacidad de operar frente a otros software	Coexistencia	x	x
	Pasos para la instalación del software o herramienta	Facilidad de instalación	x	x
	Facilidad de instalación de diferentes sistemas operativos	Adaptabilidad		x
Usabilidad	Facilidad para manipular o operar	Operatividad	x	x
	Tiempo para realizar configuración	productividad	x	x
Costo	sin costo de la adquisición del software	Costo	x	x
	sin costo por el soporte técnico de la herramienta	Soporte	x	x
			16	15

VPN

Perspectiva	Descripción	Criterio	OpenVPN	
			Windows	Linux
Funcionalidad	Capacidad para satisfacer las necesidades de la herramienta	Adecuación	x	
	Capacidad de intercambiar información y utilizar información de otros sistemas	Interoperabilidad	x	
Características	Generación de clientes	Cumplimiento de característica	x	x
	Generación de llaves		x	x
	Rapidez de conexión		x	x
Fiabilidad	Realiza o es fácil hacer backup de la información	Recuperabilidad		
Eficiencia	Consumo de bajos recursos	Utilización de recursos	x	x
Portabilidad	Capacidad de operar frente a otros software	Coexistencia	x	x
	Pasos para la instalación del software o herramienta	Facilidad de instalación	x	-
	Facilidad de instalación de diferentes sistemas operativos	Adaptabilidad	x	x
Usabilidad	Facilidad para manipular o operar	Operatividad	x	x
	Tiempo para realizar configuración	productividad	x	x
Costo	sin costo de la adquisición del software	Costo	x	x
	sin costo por el soporte técnico de la herramienta	Soporte	x	x
			13	10

SIEM

La herramienta que fue seleccionada se instaló probo y califico por la estudiante Alejandra NANA la cual está realizando el proyecto NANANA de grado para la escuela colombiana de ingeniería julio Garavito

Perspectiva	Descripción	Criterio	OSSIM		
			Windows	Linux	MAC
Funcionalidad	Capacidad para satisfacer las necesidades de la herramienta	Adecuación	x	x	x
	Capacidad de intercambiar información y utilizar información de otros sistemas	Interoperabilidad	x	x	x
Características	Análisis pormenorizado de log	Cumplimiento de característica	x	x	x
	Reportes de los y eventos		x	x	x
	Análisis de vulnerabilidades		x	x	x
	Correlación cruzada		x	x	x
	comparación con firmas de ataques conocidos o comportamientos sospechosos		x	x	x
	Interfaz grafica		x	x	x
	Informes		x	x	x
	Comunidad de inteligencia de amenaza o OTX		x	x	x
	Descubrimiento de activos		x	x	x
	Puertos espejo		x	x	x
	Capacidad de centralizar		x	x	x
Fiabilidad	Realiza o es fácil hacer backup de la información	Recuperabilidad	x	x	x
Eficiencia	Consumo bajo de recursos	Utilización de recursos			
Portabilidad	Capacidad de operar frente a otros software	Coexistencia	x	x	x
	Pasos para la instalación del software o herramienta	Facilidad de instalación	x	x	x
	Facilidad de instalación de diferentes sistemas operativos	Adaptabilidad	x	x	x
Usabilidad	Facilidad para manipular o operar	Operatividad	x	x	x
	Tiempo para realizar configuración	productividad	x	x	x
Costo	sin costo de la adquisición del software	Costo	x	x	x
	sin costo por el soporte técnico de la herramienta	Soporte			
			20	20	20

DOCUMENTOS SOPORTE

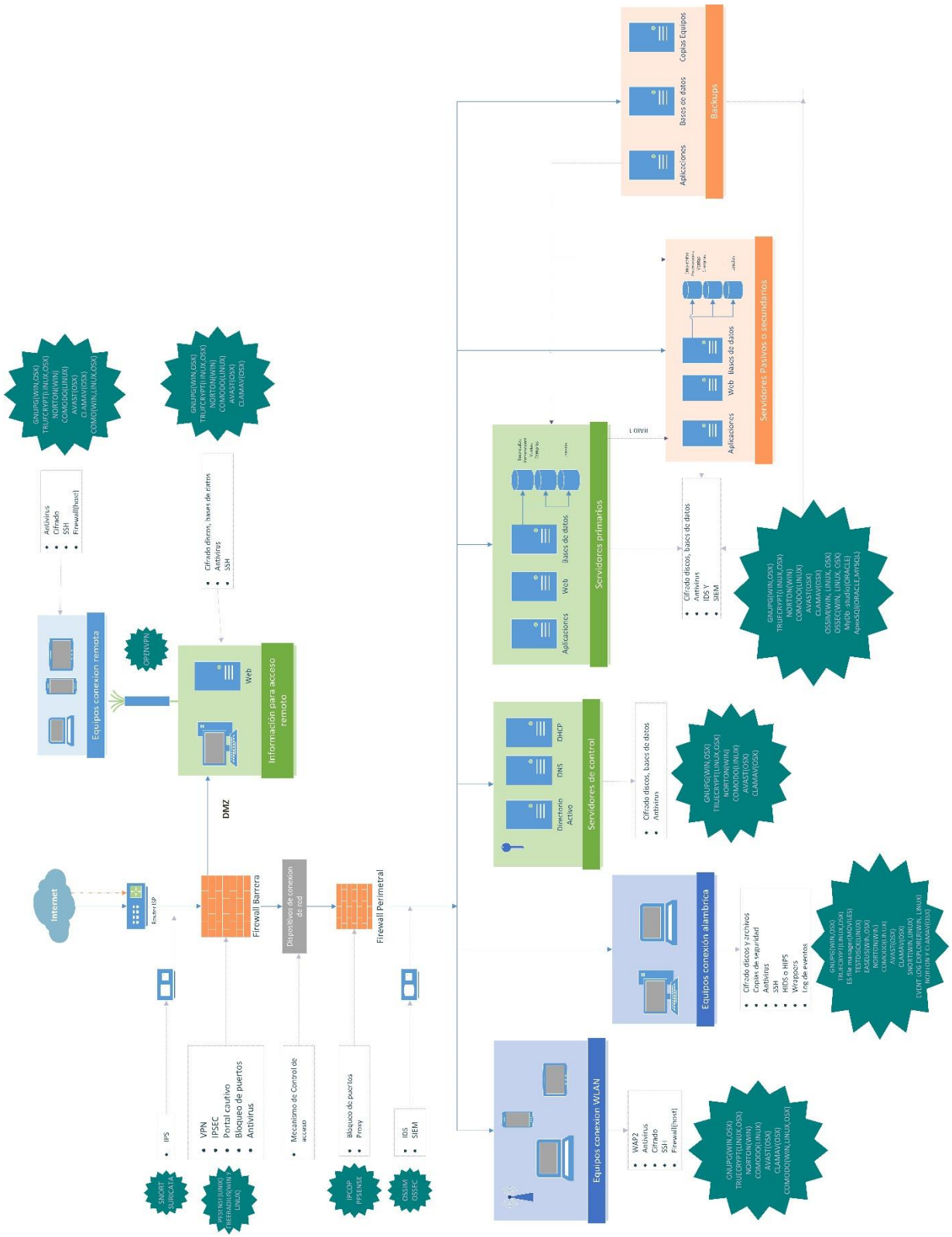
Anexo 3: Videos.
Anexo 4: Máquinas virtuales con herramientas instaladas.

PROPUESTA INTEGRAL DE PROTECCIÓN

En esta parte del documento se van a ilustrar los resultados obtenidos en la matriz, asociándolos a las soluciones que cumplieron con la mayor parte de criterios definidos, es importante resaltar que en este estudio se está trabajando con las versiones actuales de cada herramienta, y no se puede asegurar que a medida que pase el tiempo y cada fabricante produzca nuevas versiones, estas continúen siendo las que cumplen con más características o continúen cumpliendo las actuales.

Esta propuesta busca actuar como una guía o referente para que cualquier empresa que quiera empezar a asegurar la información pueda conocer que elementos tecnológicos puede implementar, como puede asegurar la infraestructura y que herramientas puede empezar a validar o implementar para cumplir con la estrategia de tecnología y de seguridad.

A continuación se ilustrara el modelo final de la arquitectura tecnológica.


Internet
Router/FW
Firewall Barrera
DMZ
Dispositivos de conexion de red
Firewall Perimetral
Equipos conexion remota
Antivirus
Cifrado
SSH
Firewall(host)
OPENVPN
Información para acceso remoto
Web
Cifrado discos, bases de datos
Antivirus
SSH
Servidores primarios
Aplicaciones
Web
Bases de datos
Servidores Pasivos o secundarios
Backups
Aplicaciones
Bases de datos
Copias Equipos
Servidores de control
Directorio Activo
DNS
DHCP
Cifrado discos, bases de datos
Antivirus
Equipos conexión alambrica
Cifrado discos y archivos
Copias de seguridad
Antivirus
SSH
HIDS o HIPS
Wrappers
Log de eventos
Equipos conexion WLAN
WAP2
Antivirus
Cifrado
SSH
Firewall(host)
IPS
VPN
IPSEC
Portal cautivo
Bloqueo de puertos
Antivirus
Mecanismo de Control de acceso
Bloqueo de puertos
Proxy
IDS
SIEM
SNORT SURICATA
IPCOP IPFIRE
OSSIM OSSEC

BUENAS PRÁCTICAS Y RECOMENDACIONES PARA GESTIONAR SEGURIDAD EN EL RECURSO HUMANO

Asegurar la arquitectura tecnológica es muy importante ya que con ella se es capaz de tener controlada la información y los procesos, sin embargo no todos los procesos y herramientas pueden garantizar que la información este segura y no sea vulnerada, ya que existe un recurso que es autónomo en sus decisiones y capaz de manipular la información que tiene en su poder a su antojo y este recurso es el ser humano quien manipula la información que tiene en su poder. Es importante para las empresas entender que la seguridad de la información no solo está en manos del área de seguridad de TI si no que toda la organización debe estar alineada y responsabilizada del tema, es por lo anterior se va a complementar la propuesta nombrando algunas de las políticas que debe tener una empresa para el manejo de los recursos humanos y se nombraran algunos de los entes que capacitan y certifican el cumplimiento de seguridad de la información.

Para asegurarse que las personas utilicen la información adecuadamente se realizó un estudio apoyado en algunas fuentes como [20], [21], [22], [23], [24] las cuales recomiendan lo siguiente:

- Seleccionar empleados idóneos para los cargos de la empresa.
- Verificar los antecedentes de acuerdo con las leyes y reglamentos para el proceso de contratación de empleados y cambios dentro de la organización, esta verificación se debe hacer de acuerdo a la clasificación de la información a la cual el empleado va a tener acceso
- Definir y asignar roles y responsabilidades.
- Asegurarse que todos los empleados comprenden las responsabilidades y son idóneos para los roles asignados, por medio de la creación de contratos o documentos de confidencialidad.
- Crear y notificar procesos disciplinarios para atender las violaciones de seguridad por parte de los usuarios.
- Formar, capacitar y concientizar a los empleados del buen uso de la información.
- Monitorear ingreso y actualización a los datos.
- Políticas de copias y divulgación de la información.
- Evitar el acceso no autorizado a sistemas y aplicaciones por medio de políticas de usuarios y contraseñas únicas, las cuales estén a cargo de un departamento de TI o gestión de usuarios.
- Restringir acceso a los códigos fuente de los programas.
- Asegurarse de que los empleados se hacen responsables de los activos de la información y físicos que estén autorizados a utilizar.
- Gestión de políticas de manuales convivencia de trabajo, como por ejemplo cuando un usuario esté ausente que no de información expuesta o libre de cuidado.
- Gestionar el proceso de los empleados que abandonan la organización.

Para apoyar la formación de los empleados, empresas y personas en general existen muchos entes que trabajan para mejorar este habito como el Mintic, que genera artículos como "¿y de seguridad de TI que hacen las entidades?", también curos y becas para seguridad las cuales son promovidas en su página web así "Mintic viene promoviendo la educación formal para promover el conocimiento e implementación de la mejor cultura en seguridad TI" [25], documentos como el modelo de seguridad de la información para la estrategia de gobierno en línea, donde nos cuenta cual es el plan para capacitar y sensibilizar a las personas y empresas sobre la seguridad de TI.

Por otra parte empresas como ESET quien genera y promueve guías de seguridad en su centro de amenazas, en estas trata temas cómo nuevas formas de gestionar seguridad, guía para responder a una infección de malware, guías de privacidad, guía del empleado seguro, entre muchas otras, estas guías son promovidas también por algunos otros sitios web como WELIVESECURITY, quien hace artículos sobre las guías y permiten dimensionar de lo que trata y lo que puede beneficiar.

Las empresas pueden también apoyarse en la ISO27001 la cual habla sobre la seguridad ligada a los recursos humanos y hace un énfasis en el capítulo 8.2.2: "Formación y capacitación en seguridad de la información".

A continuación vamos a listar algunas organizaciones que están interesadas en el tema y certifican, evalúan, crean programas de aprendizaje, documentos, videos, foros, cursos para que las empresas y las personas se concienticen de la importancia del tema.

Colombia	Otros países [26]
• SGS • Mintic • Cámara de comercio de Bogotá • E magíster • 2Secure • Global suites • Bureau veritas formación • Microsoft	• ENINSA: Agencia europea de seguridad de las redes y la información. • AGPD: Agencia española de protección de datos. • CNN-CERT: Centro Nacional Criptológico. • INTECO. • Information Security Encyclopedia. • ISQ. • LAMP Security training. • Microsoft. • NIST: National Institute os Ftandards and technology

También puede verse [29]

CONCLUSIONES

Es importante que las empresas que implementen tecnología estén enteradas de todos los riesgos que puede llegar a tener, sin embargo aún más importante que conocer estos riesgos, es saber cómo pueden ser mitigados y a costos razonables, es por eso que con esta propuesta queremos ser un referente para que todas estas empresas que se creen en el país y usen tecnología puedan asegurar su red y dispositivos.

En este proyecto se cumplió con lo siguiente:

- **Identificación de los elementos de la arquitectura:** Se logró identificar e ilustrar los posibles elementos que puede contemplar una arquitectura, para que cada empresa los utilice de acuerdo a su necesidad, una vez identificados todos los elementos se plasmaron en un imagen y separaron en grupos; De este producto se pudo determinar que todas las empresas utilizan los mismos elementos y herramientas, solo que varía la manera de ilustrarlos, segmentarlos y asegurarlos de acuerdo a la madurez de cada una de ellas.

- **Definición de una arquitectura tecnológica:** Se logró diseñar una arquitectura que está al alcance de cualquier empresa, que satisfaga la mayoría de necesidades tecnológicas, que dé continuidad al negocio y que permita asegurar la información, para esta definición se utilizaron los elementos comunes y el modelo de profundidad de Microsoft.

- **Definición de herramientas de seguridad**: Se puede concluir que una empresa puede utilizar herramientas de seguridad a costos mínimos, que pueden ser implementadas para diferentes sistemas operativos, que cumplen la función de la herramienta y que cumplen con muchas de las características funcionales propias.

- **Implementación y evaluación de herramientas:** Se pudo identificar que para el proceso de instalación y configuración existe una gran cantidad de documentación y videos tutoriales, lo que es una gran ventaja para que una empresa no dependa de todo un equipo tecnológico o empresa tercerizada para implementar estas herramientas; también se puede concluir que todas las herramientas definidas permiten ser instaladas en los diferentes sistemas operativos y que cumplen con la funcionalidad propia de la herramienta.

- **Propuesta de seguridad asociada a los recursos humanos:** En esta propuesta se puede evidenciar que la mayoría de documentación existente lleva a que no solo hay que enfocarse en las herramientas de seguridad, ya que es aún más importante elegir y formar correctamente a las personas que van a manipular la información de la empresa y que por más mecanismos de seguridad que existan si no se tiene una adecuada concientización y capacitación al recurso humano no se puede asegurar que la información este protegida al interior de la empresa.

Se puede concluir que es vital en la implementación de tecnología, la definición de una arquitectura tecnológica adecuada, ya que sobre ella se pueden evidenciar riesgos, hacer mejoras tecnológicas para la empresa, hacer una búsqueda de nuevas necesidades, solucionar inconvenientes e identificar las formas de mitigar riesgos.

Se puede tomar cómo un referente para la elección de una herramienta la matriz de evaluación definida en este proyecto ya que se calificaron y nombraron las características propias de cada una de ellas, además de solucionar un problema grande que es que muchas herramientas de la red no son lo que dicen ser si no que son soluciones maliciosas y en este trabajo se pudo identificar que las

herramientas elegidas cumplen con el objetivo y son seguras y para esto se grabó la funcionalidad de cada una de ellas.

Se observó a medida que paso el proyecto que hoy en día el tema de asegurar las plataformas está cogiendo más fuerza ya que la cantidad de ataques han aumentado a gran escala y las pérdidas económicas de las empresas han sido enormes, es por eso que muchas empresas han creado soluciones que apoyan la seguridad de la información.

TRABAJO FUTURO

En esta propuesta se realizó la comparación de 2 o 3 fabricantes de cada herramienta y se realizaron configuraciones y pruebas básicas de las mismas, por lo anterior posterior a este estudio se pude anexar un proyecto de ingeniería en el cual se haga en un estudio independiente cada una de las herramientas comunes que existen para asegurar una arquitectura tecnológica y así poder identificar costos exactos, capacitad hardware de la herramienta y dar un listado más amplio de herramientas u opciones para que las empresas puedan elegir, de este estudio se podría generar un producto como guía técnica de implementación y evaluación de herramientas software para controles de seguridad.

Se propone hacer un énfasis en tres herramientas SIEM, Firewall de nueva generación y sistemas de monitoreo y prevención de intrusos como los IDS e IPS, se propone que sean estas herramientas debido a que la empresa sería capaz de controlar, monitorear, definir políticas, protocolos, alertar y prevenir cualquier tipo de anomalía que exista en su red y los equipos de la misma, analizar vulnerabilidades y crear conexiones seguras.

BIBLIOGRAFÍA

[1] G. trainigcenter, «goIT,» 2016. [En línea]. Available: http://www.goit.com.mx. [Último acceso: 2017].

[2] C. A. Sanchez Rodriguez, «Escuela de Ingenieria Julio garavito - biblioteca,» Bogota, 2015.

[3] US Departament of defense, «US Departament of defense,» [En línea]. Available: http://dodcio.defense.gov. [Último acceso: 2016].

[4] TOGAF, «opengroup.org,» [En línea]. Available: http://www.opengroup.org. [Último acceso: 2016].

[5] TOGAF, «TOGAF Capitulo 1,» de *guia de bolsillo Vr9.1*, 9.1 ed.

[6] TOGAF, «Capitulo 2,» de *Guia de bolsillo Vr 9.1*.

[7] Jennygiraldo, «Arquitectura empresarial TOGAF. Fase D,» wordpress, 19 05 2015. [En línea]. Available: http://chae20151170101262.wordpress.com. [Último acceso: 2016].

[8] TOGAF, «Capitulo 21, 4.4 arquitectura de seguridad,» de *Guia de bolsillo vr 9.1* .

[9] F. D. Palacios, «Propuesta de integración arquitectura empresarial y arquitectura de seguridad metadata,» Repositorios biblioteca escuelaing.edu.co, Bogota, 2016.

[10] P. I. e. español, «ISO27000,» 2012. [En línea]. Available: eee.Iso27000.es. [Último acceso: 2016].

[11] UNAM, «UNAM,» Universidad Nacional Autonoma de Mexico, 2015. [En línea]. Available: http://redyseguridad.fi-p.unam.mx. [Último acceso: 2017].

[12] S. blog, «pmg-ssi,» 4 5 2015. [En línea]. Available: www.pmg-ssi.com. [Último acceso: 2017].

[13] MINTIC, «Ministerio de tecnologia y comunicación,» de *Mipyme digital*, Bogota, 2015.

[14] L. M. G. S. Ibarra, «Reunion informativa sobre la gobernabilidad de TI».

[15] M. Santos, «Enter.co Enterprise,» 6 11 2013. [En línea]. Available: http://www.enter.co/chips-bits/enterprise/las-pymes-que-adoptan-ti-crecen-mas-rapido-bcg/. [Último acceso: 2016].

[16] Camara de Comercio de Bogota, 2016. [En línea]. Available: www.ccb.org.cp. [Último acceso: 2016].

[17] Confecamaras, «En el 2016 aumento 15,8% la creaciòn de empresas en Colombia,» Confecamaras, Bogota, 2017.

[18] Cristina Prieto, directora de Calidad Educativa de Preescolar, Básica y Media del Ministerio de Educación, «Ministerio de eduación de Colombia,» 2016. [En línea]. Available: www.mineducacipn.gov.co. [Último acceso: 2016].

[19] M. F. Ocampo Saavedra, «Colombia aprende,» 2013. [En línea]. Available: www.colombiaaprende.edu.co. [Último acceso: 2016].

[20] Universidad ICESI, «Universidad ICESI,» 2008. [En línea]. Available: http:eduteka.icesi.edu.co. [Último acceso: 2016].

[21] E. C. Rios, «Concienciar para prevenir,» *Seguridad cultura de prevencion para TI.*

[22] AUDILACTEOS, «auditoriauc20102mivi,» 30 08 2010. [En línea]. Available: https://auditoriauc20102mivi.wikispaces.com/PETI. [Último acceso: 2016].

[23] forondarena, «forondarena,» [En línea]. Available: https://www.forondarena.net/pages/ejemplo-itil-y-soft-libre.html. [Último acceso: 2016].

[24] D. f. Ruiz sanchrez, «DISEÑO DE ARQUITECTURA EMPRESARIAL EN EL SECTOR EDUCATIVO,» UNIVERSIDAD CATÓLICA DE COLOMBIA, Bogotà, 2014.

[25] C. Osorio, «SCRIBD,» [En línea]. Available: https://es.scribd.com/doc/61411217/ARQUITECTURA-TECNOLOGICA. [Último acceso: 2016].

[26] Universidad Oberta de Cataluña, «UOC,» [En línea]. Available: http://www.uoc.edu/portal/es/tecnologia_uoc/arquitectura/index.html. [Último acceso: 2016].

[27] A. G. Valdez Menchaca, «SCRIBD,» [En línea]. Available: https://es.scribd.com/doc/35231457/Arquitectura-Tecnologica. [Último acceso: 2016].

[28] A. Barros, «Arquitecturas tecnològicas empresariales,» 2007.

[29] PhoneCallCenter, «PhoneCallCenter,» [En línea]. Available: http://www.phonecallcenter.es/empresa.html. [Último acceso: 2016].

[30] Revista espacios, [En línea]. Available: http://www.revistaespacios.com/a15v36n10/153610E2.html. [Último acceso: 2016].

[31] J. Norbei zamudio , «hstech-electronica.blogspot,» 23 08 2011. [En línea]. Available: http://hstech-electronica.blogspot.com.co/2011_08_01_archive.html. [Último acceso: 2016].

[32] R. Dimas y J. Maestre, «geocities,» Universidad Yacambú, Maestría de Gerencia de las Finanzas y de los Negocios Redes y Telecomunicaciones, [En línea]. Available: http://www.geocities.ws/jemaestre/fase2/t9.html. [Último acceso: 2016].

[33] Themostwanted-actividades- Redes Sociales, «http://themostwanted-actividades.blogspot.com.,» 17 02 2010. [En línea]. Available: http://themostwanted-actividades.blogspot.com.co/2010_02_01_archive.html. [Último acceso: 2016].

[34] Google, *Imagenes Arquitecturas empresariales,* 2016.

[35] Open Source Foru, «Open Source Foru,» 6 2 2014. [En línea]. Available: http://opensourceforu.com/2014/02/top-10-open-source-security-tools/. [Último acceso: 2016].

[36] insecure, «insecure,» [En línea]. Available: http://insecure.org/tools/tools-es.html. [Último acceso: 2017].

[37] IBM, «IBM,» [En línea]. Available: http://www-03.ibm.com/software/products/es/qradar-siem. [Último acceso: 2017].

[38] Weblog sobre seguridad informatica, 13 3 2008. [En línea]. Available: https://kahit.wordpress.com/2008/03/13/sistemas-de-deteccion-de-intrusos-ids/. [Último acceso: 2017].

[39] Palo Alto Networks, «Resumen firewall de nueva generaciòn,» 2011.

[40] S. Northcutt, «Linkedin,» 26 02 2016. [En línea]. Available: https://www.linkedin.com/pulse/open-source-siem-stephen-northcutt. [Último acceso: 2017].

[41] MINTIC, «Seguridad y privacidad de la información,» [En línea]. Available: www.mintic.gov.co/gestionti. [Último acceso: 2017].

[42] RHM Grupo de comunicaciones, «RRHH agazine,» 25 09 2003. [En línea]. Available: www.rrhhmagazine.com/articulos. [Último acceso: 2017].

[43] ICETEX, «ICETEX,» 2014.

[44] WebliveSecurity, «WebliveSecurity,» 2012. [En línea]. Available: www.weblivesecurity.com/la-es/. [Último acceso: 2017].

[45] ESET, «Guias de seguridad- centro de Amenzas,» 2017.

[46] MINTIC, «MINTIC.GOV,» 2016. [En línea]. Available: eee.mintic.gov.co/gestion/615/w3-article-7083.html. [Último acceso: 2016].

[47] ISO27000 en español, «ISO27000 en español,» 2012. [En línea]. Available: www.iso27000.es/iso27002_7.html. [Último acceso: 2017].

[48] C. Villamizar, «magazcitum, El magazine para los profesionales de seguridad de TI,» 30 08 2013. [En línea]. Available: http://www.magazcitum.com.mx/?p=2361#.WRvEa-s1_IV. [Último acceso: 2016].

GLOSARIO

1. **TI:** Tecnologías de información
2. **AE:** Arquitectura empresarial
3. **AT:** Arquitectura tecnológica
4. **DoDaft:** Department of Defense Architecture Framework en Español Departamento de Defensa Marco de Arquitectura
5. **FEAF:** Federal Enterprise architecture en Español arquitectura empresarial federal
6. **TOGAF:** The Open Group Architecture Framework
7. **ADM:** The Architecture Development Method **,** Método de desarrollo de la arquitectura
8. **CCB:** Cámara de comercio de Bogotá
9. **IDS:** Intrusion Detection System, en español sistema de detección de intrusos
10. **IPS:** Intrusion Prevention System, en español Sistema de Prevención de Intrusos
11. **SIEM:** Security Information and Event Management, en español Información de seguridad y administración de eventos.
12. **DNS:** Domain Name System, en español sistema de nombre de dominio.
13. **DHCP:** Dynamic Host Configuration Protocol, en español protocolo de configuración dinámica de host.
14. **DMZ:** Demilitarized zone, en español Zona desmilitarizada.
15. **SHH:** Secure Shell, en español: intérprete de órdenes seguro.
16. **VPN:** Virtual Private Network, en español red privada virtual.
17. **SEGMENTO AISLADO:** Segmento que se encuentra diferenciado de otro ya sea con otro segmento de red IP o es otra ubicación.

LISTAS ESPECIALES

CONTRIBUCIONES Y AGRADECIMIENTOS ESPECIALES

Quiero agradecer al grupo de proyecto…… y a la estudiante Alejandra…… las cual está realizando su proyecto de grado en herramientas de monitoreo y gestión de eventos y nos apoyó en la calificación de las herramientas OSSIM y OSSEC y la Escuela Colombiana de Ingeniería Julio Garavito y la decanatura de ingeniería de sistemas quienes crearon el programa de proyecto de grado y brinda una formación y preparación para temas en el ámbito laboral.

También quiero dar un agradecimiento a los ingenieros Daniel Díaz y Gerardo Ospina quienes evaluaron el proyecto y dieron elementos y consejos que permitieron cumplir con los objetivos establecidos del proyecto.

Por último y más importante quiero agradecer a la Ingeniera Claudia Patricia Santiago quien estuvo pendiente del cumplimiento de los resultados del proyecto y me apoyo durante todo proceso de estudio e implementación del mismo, ayudándome a obtener un aprendizaje en diferentes aspectos, los cuales me permitieron conocer cómo funciona en la actualidad los elementos tecnológicos y el tema de seguridad para las empresas, adquirir conocimiento de nuevos términos, adquirir capacidades de análisis, de implementación y de generación de productos de alto nivel que favorezcan la sociedad, especialmente a las empresas que quieran asegurar su red y no sepan cómo comenzar.

ANEXOS

Anexo 1- Análisis de riesgos y controles hoja Activos comunes.

Anexo 2- Matriz evaluación.

Anexo 3- Videos.

Anexo 4- Máquinas virtuales con herramientas instaladas.