



FACULTAD DE CIENCIAS EMPRESARIALES
CARRERA PROFESIONAL DE INGENIERÍA DE
SISTEMAS DE INFORMACIÓN Y GESTIÓN

“IMPACTO DE LA IMPLEMENTACIÓN DE SEGURIDAD DE LA
INFORMACIÓN MEDIANTE AMAZON WEB SERVICES EN EL
SISTEMA DE RECURSOS HUMANOS DE FRACTAL SAC LIMA -
2020”

Trabajo de investigación para optar el grado académico de:
Bachiller en Ingeniería de Sistemas de Información y Gestión

Presentado por:

Eduardo Ilizarbe Tito (0000-0002-5292-944X)

Ester Alarcón Ayquipa (0000-0001-5357-8859)

Luis Angel Apaza Quispe (0000-0002-3650-066X)

Lima - Perú

2020

FACULTAD DE CIENCIAS EMPRESARIALES
ANEXO 6
ACTA DE APROBACIÓN DEL TRABAJO DE BACHILLER POR JURADO

Fecha: 06/01/2021

El Jurado del trabajo de investigación de Bachiller:

Mg. Jose Luis Albites Sanabria

Luego de evaluar el trabajo de investigación de Bachiller titulado:

IMPACTO DE LA IMPLEMENTACIÓN DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE AMAZON WEB SERVICES EN EL SISTEMA DE RECURSOS HUMANOS DE FRACTAL SAC LIMA - 2020

Presentada por la estudiante:

| CÓDIGO | ALUMNO |
|-----------|-------------------------|
| 100037084 | Luis Angel Apaza Quispe |
| 100038770 | Ester Alarcón Ayquiipa |
| 100037967 | Eduardo Ilizarbe Tito |

Para optar al grado de Bachiller en: Ingeniería de Sistemas de Información y Gestión, en la carrera de Ingeniería de Sistemas de Información y Gestión, de la Facultad de Ciencias Empresariales.

Luego de haber evaluado el informe final del trabajo de investigación de Bachiller, concluye en calificar a:

| CÓDIGO | ALUMNO | CALIFICACION |
|-----------|-------------------------|---------------|
| 100037084 | Luis Angel Apaza Quispe | Aprobado (16) |
| 100038770 | Ester Alarcón Ayquiipa | Aprobado (16) |
| 100037967 | Eduardo Ilizarbe Tito | Aprobado (16) |

El jurado firma en señal de conformidad.



Mg. Jose Luis Albites Sanabria

ÍNDICE DE CONTENIDO

| | |
|--|-----------|
| Índice de figuras | 4 |
| Índice de Tablas | 5 |
| INTRODUCCIÓN | 6 |
| CAPÍTULO I: DESCRIPCIÓN DEL PROBLEMA | 7 |
| 1.1. Descripción de la realidad problemática..... | 7 |
| 1.2. Objetivos del proyecto | 12 |
| 1.2.1. Objetivo general | 12 |
| 1.2.2. Objetivos específicos | 12 |
| 1.3. Justificación del proyecto | 12 |
| 2. CAPÍTULO II: MARCO TEÓRICO | 13 |
| 2.1. Antecedentes | 13 |
| 2.2. Bases teóricas | 16 |
| 2.3. Definiciones conceptuales | 21 |
| 3. CAPÍTULO III: DESARROLLO DEL PROYECTO | 23 |
| 3.1. Arquitectura empresarial | 23 |
| 3.1.1. Arquitectura de Información (Datos) | 23 |
| 3.1.2. Arquitectura de Negocios (Procesos) | 25 |
| 3.1.3. Arquitectura de Aplicación..... | 26 |
| 3.1.4. Arquitectura Tecnológica..... | 29 |
| 4. CAPITULO IV: RECURSOS Y CRONOGRAMA | 34 |
| 4.1. Recursos | 34 |
| 4.2. Cronograma de ejecución..... | 35 |
| 5. CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES | 36 |
| 5.1. Conclusiones | 36 |
| 5.2. Recomendaciones | 37 |
| 6. CAPÍTULO VI: FUENTES DE INFORMACIÓN | 38 |
| 6.1. Referencias electrónicas..... | 38 |

Índice de figuras

| | |
|---|----|
| Figura 1: Listado de formatos de cargas masivas..... | 9 |
| Figura 2: Evolución de Servicios Cloud..... | 11 |
| Figura 3: Flujo del proceso al acceso de la aplicación | 24 |
| Figura 4: Macroproceso de la empresa Fractal..... | 25 |
| Figura 5: Proceso con la implementación con Amazon Web Services | 26 |
| Figura 6: Desarrollo de capa presentación | 27 |
| Figura 7: Desarrollo capa lógica de negocio | 27 |
| Figura 8: Desarrollo de capa datos. | 28 |
| Figura 9: Arquitectura del Sistema de Recursos Humanos de Fractal. | 29 |
| Figura 10: Arquitectura tecnológica de la empresa Fractal..... | 30 |
| Figura 11: Flujo de conexión del usuario con Amazon Web Services..... | 32 |

Índice de Tablas

| | |
|---|----|
| Tabla 1: Cuadro comparativo de envío de correos semestral..... | 8 |
| Tabla 2: Descripción de servidores de la empresa Fractal. | 31 |
| Tabla 3: Características de la implementación del servicio Amazon Web Services..... | 31 |
| Tabla 4: Costo de talento humanos..... | 34 |
| Tabla 5: Costo de implementación del servicio. | 34 |
| Tabla 6: Cronograma de actividades para la ejecución del proyecto | 35 |

INTRODUCCIÓN

Debido a la demanda de información que se genera en estos días es necesario que sea proporcionada de forma segura, eficiente, eficaz y automatizada, dicho esto, es que se hace obligatorio implementar un recurso tecnológico que satisfaga estas necesidades, en nuestro caso hemos elegido cómo solución a una aplicación que se basa en Amazon Web Services (AWS). Esto nos servirá para resolver problemas de seguridad con respecto a la data en el sistema de Recursos Humanos de la empresa Fractal, también permite almacenar grandes cargas de información que nos ayudará ahorrar tiempo en el proceso y sobre todo en el ahorro de costos.

En base a la seguridad de la información los conceptos que se hacen referencia en este trabajo de investigación contemplan la disponibilidad, integridad, confidencialidad, monitoreo y calidad de servicio, justamente Amazon Web Services se ajusta a estos preceptos, lo cual aporta de manera global a la solución en cuanto a la entrega y procesamiento de la información del sistema de Recursos Humanos en la empresa Fractal. Dado que Amazon Web Services es un servicio que se encuentra en la nube, cuenta con cualidades adicionales que permite un monitoreo constante, prevención de ataques, almacenamiento de grandes cantidades de información, revisión de tráfico de la red, etc.

Este trabajo se fundamenta en el uso de tecnologías de la información no solamente para optimizar los procesos y resolver problemas de vulnerabilidades que puedan existir en el tratamiento de la información en un sistema, también cambia la forma de pensar que la seguridad de la información debería ser gestionada con los recursos inhouse y con una inversión grande en hardware, software y personal especializado. Es poner en practicar la disrupción digital en servicio de la sociedad.

CAPÍTULO I: DESCRIPCIÓN DEL PROBLEMA

1.1. Descripción de la realidad problemática

Hoy, por hoy, más organizaciones mantienen extensamente sus activos de información de forma digital, la cual se procesa con la ayuda de los sistemas de información que se comunican a través de redes privadas e internet. Un ejemplo de esto es la medición realizada sobre brechas de seguridad de información, en el año 2004 se señaló que aproximadamente el 90% de los negocios del Reino Unido enviaba correos electrónicos por la internet, navegaban por la web y tenían su propio Web-Site.

Actualmente los sistemas de información e internet no sólo son usados por las organizaciones, también por los delincuentes informáticos, esto ha llevado a elevar las consideraciones de la seguridad en los sistemas de información. En este sentido, las prioridades estratégicas y los esquemas prácticos que las organizaciones aplican en materia de seguridad de información se focalizan en controles técnicos y procesales, ignorando frecuentemente el factor humano. No obstante, concentrarse en aspectos meramente técnicos y procesales es inadecuado, en vista que los usuarios no pueden entender y seguir muchas de estas medidas.

Por consiguiente, la investigación pretende desde este punto de vista, mostrar que la efectividad de la seguridad de información requiere de un programa institucional que cree un clima de concientización donde cada usuario haga lo que debe hacer, con entusiasmo y dedicación, sin necesidad de supervisión externa, en consonancia con la misión de la organización siguiendo las normas y procedimientos establecidos en materia de seguridad informática.

Hernán Torres Álvarez, (2005 pág. 66), este problema está vinculado de cierta manera al problema de la integridad de los mensajes, pues en este caso se interceptan los mensajes con el simple propósito de conocer su contenido.

Hoy en día la empresa se hace cargo del manejo de una gran cantidad de información que conlleva a utilizar diversas herramientas. Por lo cual la empresa Fractal maneja la información de terceros, además brinda otros tipos de servicios informáticos. Otro problema de la empresa es la enorme información que se despliega cada fin de mes, los

siguientes motivos son las excesivas cargas masivas a finales de mes, esto conlleva a la saturación de las herramientas o sistemas a los cuales el cliente hace uso y la empresa en cuestión ofrece. Esto incluye las gigantescas colas de envíos de correos masivos que cada cliente hace diariamente. Por lo tanto, se hace necesario optar por una nueva tecnología que garantice la integridad de la información brindada para nuestros clientes.

Según el estudio de un analista de seguridad de información contratado por la empresa Fractal, realizó un cuadro comparativo del nivel de envío de correos masivos aproximados durante el último semestre del 2019.

| Meses | Aproximación de envío de Correos x día | Aproximación de envío de correos por mes | % Recibido por mes | % Pérdida por mes |
|-----------|--|--|--------------------|-------------------|
| Julio | 5600 | 156.800 | 96% | 4% |
| Agosto | 5200 | 145.600 | 95% | 5% |
| Setiembre | 5910 | 153.660 | 94% | 6% |
| Octubre | 6052 | 169.456 | 92% | 8% |
| Noviembre | 5862 | 140.688 | 96% | 4% |
| Diciembre | 6350 | 177.800 | 94% | 6% |

Tabla 1: Cuadro comparativo de envío de correos semestral.

El cuadro comparativo indica un aproximado de correos enviados durante el mes de julio a diciembre del 2019, donde el mes de octubre tiene un aproximado de 8% en pérdida, esto indica que los correos o nunca llegaron al destinatario, o sufrieron pérdida, por lo que la empresa desea mimetizar todo tipo de pérdida ya que lo deseable es un 100% de envío y de recepción de correo, lo cual está afectando claramente a la integridad de la información enviada.

También se evaluó los formatos de cargas masivas, siendo 27 formatos los siguientes:

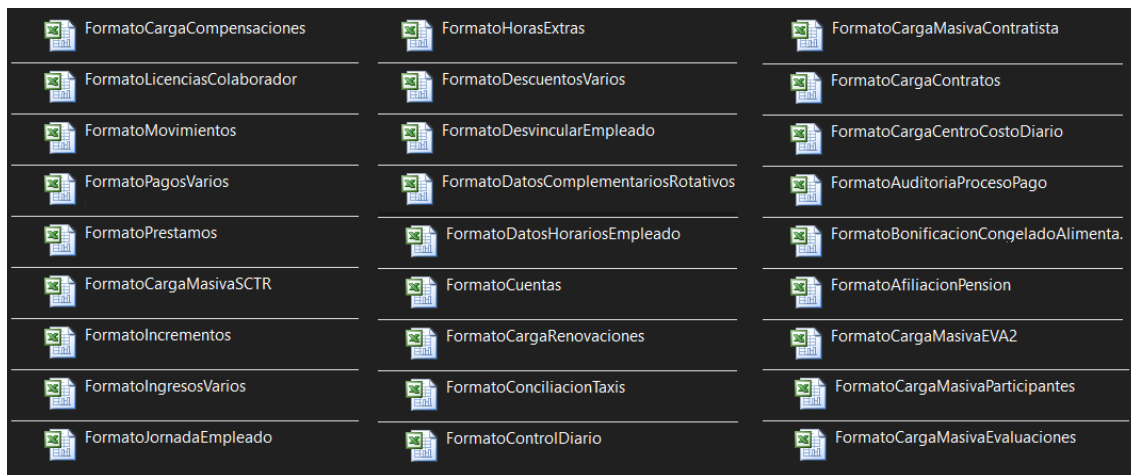


Figura 1: Listado de formatos de cargas masivas

Estos a su vez contienen más 6.000 registros de los cuales no deben exceder los 20.000 registros. Cada uno de ellos cuenta con 20 a 120 columnas cada formato.

También se indica que el tiempo promedio de subida es de 3 minutos a los servidores locales, pero se está tomando un tiempo de entre 15 min a 30 min por formato de carga.

Adicional al volumen de cada ejecución y almacenamiento a nuestros servidores locales. Se requiere guardar la información relevante de los 5 primeros años, lo cual trae dificultades por el crecimiento de la data lo que incluye el procesamiento de la información y backups.

Por lo tanto, los principales problemas encontrados son:

- a) No tener la capacidad suficiente de almacenamiento ya que la cantidad de data que administra el área de Recursos Humanos ya no es soportada por los servidores que se tiene en la actualidad.
- b) La saturación de carga de grandes cantidades de información afecta al rendimiento que es reflejado en la baja eficacia y gestión de nuestro personal de Recursos Humanos. Por ejemplo, la acción de cargar la planilla de empleados tiene un tiempo estimado de 30 minutos, lo cual en realidad debería trabajarse en 2 o 3 minutos como máximo.
- c) Al tener demora en el procesamiento de la información genera riesgos en la integridad y pérdida de datos. Por ejemplo, recepción de correos, cargas masivas, etc.

Por lo analizado en estos tres puntos puesto que los servidores ya no soportan la cantidad de información que se administra, existe pérdida de información y riesgos en la integridad de datos, se llegó a la conclusión que la mejor idea es contratar los servicios en la nube. En tal sentido se revisó cómo ha evolucionado los servicios en la nube, esto comenzó con los proveedores de internet en los 80's, posteriormente en los 90's fue donde se tuvo gran avance con aplicaciones en una web y virtualización, en los últimos 20 años ya existen diversos proveedores de servicios en la nube tanto para base datos, aplicaciones, infraestructura y desarrollo. Siendo específico para el tema se ciberseguridad al tener todo un abanico de servicios también genera oportunidades donde los atacantes pueden ingresar, ya sea por malware, phishing, durante el proceso de migración a la nube, entre otros; es por esto que también se tienen aplicaciones que administran otras aplicaciones e infraestructura con el fin de monitorear, alertar, prevenir y actuar ante ataques, como por ejemplo administrar todo un conjunto de firewalls y antivirus.

Una de las grandes ventajas que se tiene al contratar los servicios cloud es que todo el soporte e infraestructura para un determinado servicio es administrado por un tercero a un costo respectivo de acuerdo con lo que se necesita que se funcione. Las oportunidades que ofrece los servicios cloud para las empresas son muchas.

Con relación a la nube pública, tenemos desde finanzas, medicina, educación, IA, IoT, etc., donde la información se puede compartir, analizar y mejorar; con respecto a la nube privada, se ofrecen los servicios personalizados para mejorar la interoperabilidad, rendimiento, disponibilidad y seguridad. Es más, se puede en beneficio de los procesos de las empresas utilizar un servicio híbrido combinando ambos tipos.

Las dificultades que podemos notar para los servicios cloud son que, al depender de internet, este puede tener latencia. Otra posible dificultad es que si contratamos diferentes proveedores para nuestros servicios no necesariamente podremos integrarlos ya que aún no existe un estándar para poder comunicarlos entre sí por lo cual en muchos casos al tener un solo proveedor.

Esta evolución de los servicios cloud nos lleva a reflexionar que no solamente podemos trabajar los correos y la data que trabaja nuestra área de Recursos Humanos, en un futuro también podemos trabajar otros sistemas e incluso nuestra infraestructura

con lo cual solo los servicios indispensables para el funcionamiento del negocio quedarían en nuestros servidores.

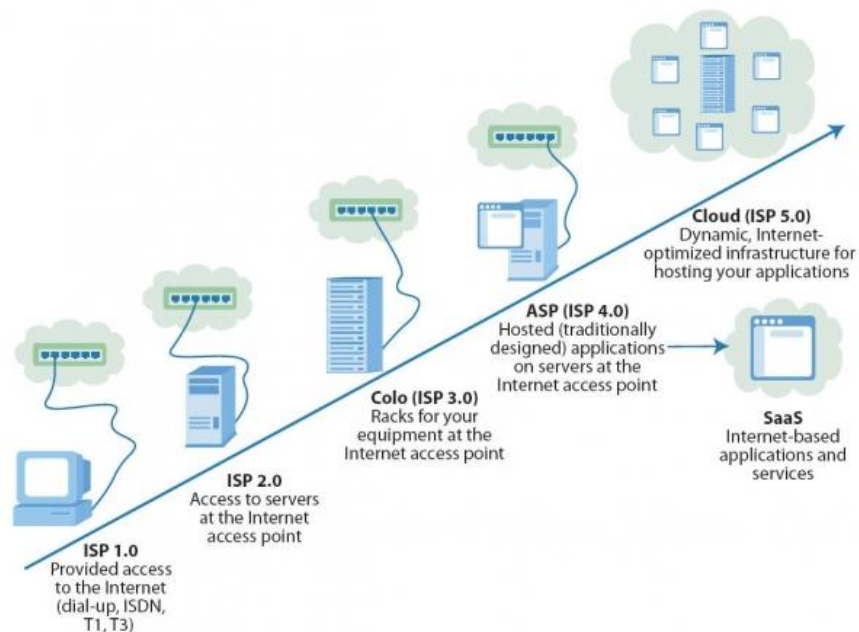


Figura 2: Evolución de Servicios Cloud.

Para nuestra problemática se ha decidido contratar AWS por los siguientes motivos:

1. Cuenta con una gran variedad de servicios en la nube, siendo uno de los pioneros y líder indiscutible en IaaS, considerando que ellos iniciaron desde el 2006 por lo cual tiene experiencia en este rubro.
2. La seguridad es otro punto fuerte ya que cumplen con una serie de certificaciones y acreditaciones, con lo cual nos permite tener funcionalidades de seguridad que automatizan las tareas de prevención, monitoreo, responder y solucionar eventualidades que se presenten.
3. Es flexible ya que se puede seleccionar el sistema operativo, base de datos e incluso el lenguaje de programación. Es una característica que ayuda bastante cuando se realiza la migración de aplicaciones.
4. Es altamente rentable ya que solo se pagará lo que se utiliza. Evitando de esta manera contratos largos y menos acuerdos obligatorios al principio del servicio.
5. De buen desempeño y escalable ya que se podrá configurar el servicio acorde a lo que necesita la empresa, esto se puede trabajar con las herramientas auto scaling y elastic load balancing.

6. Tiene clientes como Netflix, BBVA y Delaware por lo cual nos da un nivel de confianza en el servicio que proporcionan.

1.2. Objetivos del proyecto

1.2.1. Objetivo general

Determinar el impacto de la implementación de seguridad de la información mediante Amazon Web Services en el sistema de Recursos Humanos de Fractal S.A.C Lima 2020.

1.2.2. Objetivos específicos

- a) Implementar con Amazon Web Services la capacidad optima de almacenamiento cubriendo las necesidades actuales del Sistema de Recursos Humanos de la empresa Fractal, Lince 2020.
- b) Mejorar con Amazon Web Services el rendimiento en la gestión de procesos para la empresa Fractal en el sistema de Recursos Humanos, Lince 2020.
- c) Garantizar con Amazon Web Services la integridad y conservación de la información de los clientes de la empresa Fractal, Lince 2020.

1.3. Justificación del proyecto

La empresa Fractal ha decidido a través del trabajo de investigación, utilizar ciertas herramientas que ayuden a mejorar su rendimiento laboral en su gestión empresarial implementando seguridad de información utilizando Amazon Web Services. Esto permitirá a la empresa realizar:

- Simplificar procesos y tiempo al cuantificar la información de los diversos clientes a quienes se les brinda servicio.
- Mayor rendimiento en cuanto a la seguridad e integridad de la información.
- Un manejo eficiente y automatizado de la información, evitando riesgos / o pérdidas en la carga de datos, incluyendo un ahorro de tiempo y dinero.

El uso de esta herramienta Amazon Web Services permitirá a la empresa una mejor gestión en su empresa además de fidelizar a los clientes que prestan servicios de dicha empresa.

De forma práctica esta investigación aportará a la solución de problemas de seguridad de la información, ya que afectan directa o indirectamente a las organizaciones. En consecuencia, puede aportar a otras investigaciones que aborde problemas similares.

Para concluir, se estima que los resultados del trabajo sean como un ensayo de interpretación sobre una compleja situación para cuya caracterización se aportan indicios, elementos de juicio, evaluaciones parciales y nuevas consultas sobre la seguridad de información.

2. CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes

Hernández (2014) con su tesis titulada “Buenas prácticas para la implementación de la seguridad en un centro de cómputo de la Universidad Nacional autónoma de México, país – México”, para obtener el título de Ingeniero en Computación.

El autor muestra una guía de buenas prácticas, metodología, utilizando estándares como por ejemplo COBIT para garantizar la seguridad dentro de un centro de cómputo, esto a su vez se reflejan en implementar políticas, planeamiento, estrategias y diseño de plan de seguridad. Las amenazas tienen como propiedad ser las probables causantes de destruir sistemas, pueden tener su origen en: desastres naturales, inconvenientes en el hardware, de software, de red y amenazas humanas.

Ejemplos: La actividad humana puede alterar la seguridad de un software, como podría ser robo, sabotaje, fraude, ingeniería social o incluso ingeniería de reversa.

Las amenazas dañan a la disponibilidad e integridad de la información. Una amenaza se puede manifestar en un ataque el cual podría traducirse al ingreso, alteración o supresión

de información o data no autorizada; suspensión de un servicio o proceso de un sistema, etc. Es por ello necesario tener mapeada estas posibles amenazas para gestionar un plan de acción ante posibles ataques.

Además, la vulnerabilidad consiste en explotar cualquier debilidad que pueda generar pérdida o daño a un sistema. Con esto estamos dando a entender que los puntos más débiles de seguridad son los que concentran la mayor vulnerabilidad en un sistema donde es más probable que se manifieste un ataque.

En relación con nuestro trabajo de investigación:

- Diseñar, aplicamos las buenas prácticas con la implementación Amazon Web Services ya que es un proveedor reconocido y utiliza estándares internacionales. Por ejemplo, Amazon Web Services cuenta con el catálogo de controles de conformidad informática en cloud C5 el cual es una certificación con la garantía del gobierno alemán ante posibles ciberataques.
- Proporcionamos estas buenas prácticas de seguridad física y perimetral ya que el proveedor Amazon Web Services cuenta con personal especializado monitoreando los servicios que hemos contratado, adicional a ello también nuestro personal de TI se encargará de supervisar este servicio que se respalda mediante un SLA.
- Promovemos el concepto de seguridad y las buenas prácticas, esto quiere decir que hacemos participe al usuario desde el inicio y durante la implementación de Amazon Web Services en los procesos que afectan a su gestión. Con consecuencia concientizamos el buen uso de herramientas a nuestros usuarios para garantizar la solidez de la información.

Gonzales (2014) con su tesis titulada “Diseño e implementación de controles de seguridad para las comunicaciones de red en un centro de datos de una entidad del estado basado en la NTP-ISO/IEC 27001:2014 de la Universidad Tecnológica del Perú, País – Perú” para alcanzar el título de Ingeniero de Sistemas.

El autor muestra como objeto: “Los diversos enfoques teóricos del cumplimiento de la norma técnica peruana y conceptos” en él se planteó como objetivo de investigación el definir los diferentes tipos de medidas y modelos de implementación de controles de seguridad basados en la NTP-ISO/IEC 27001 ya sea primera edición que fue publicada el año 2005 y la segunda edición publicada el año 2013 y también se va a emplear por medio de una revisión bibliográfica.

Se puede definir dentro de estos resultados exitosos, competentes, honestos, inspirados y competentes. Se puede concluir que el liderazgo también puede ser aprendido. Dentro de estos bibliográficos se podría rescatar a: (Simón Foley; 2009) en su publicación “Security risk management using internal controls”; establece que, en lugar de tratar la seguridad como una preocupación, se debe de considerar como un riesgo más el cual debe ser gestionado junto con todos los demás riesgos empresariales. También propone un estructurar controles internos para la gestión del riesgo, esto significa aplicar a los procesos de negocio catálogos automatizados para mitigar el riesgo. La elevación en el tiempo real y la medición de la eficiencia de control en este modelo se vuelve esenciales para el manejo de riesgo utilizando estos catálogos y se describe un enfoque basado en el perfil de riesgos para medir el riesgo de seguridad.

En relación con nuestro trabajo de investigación: El analizar nuevas herramientas y proponer soluciones para gestionar el riesgo de seguridad el cual debe ser manejable y administrable ya que implica mucho la integridad de la información o datos que puedan estar almacenados en este repositorio planteado.

Velásquez, Kenjiro (2015) con su tesis titulada “Análisis, diseño e implementación de un sistema de apoyo para una empresa de outsourcing documental” desarrollada en la Pontificia Universidad Católica del Perú, País – Perú” para alcanzar el título de Ingeniero de Sistemas.

El autor trata de describir que por la masiva cantidad de información que administran las empresas donde el giro de negocio es el outsourcing documental, en pocas palabras a organizar, alojar y proteger los documentos, pero es una tarea que se debe hacer diligentemente según las indicaciones del usuario y conforme a la ley. Debe apuntar en la gestión de las versiones digitalizadas de los archivos y documentos, de los cuales ofrecen superioridad respecto a los backups, de igual manera con el acceso de los archivos cuando los usuarios lo requieran. La solución consiste del desarrollo de una aplicación de escritorio que permita ayudar a los usuarios de la entidad de outsourcing documental.

En relación con nuestro trabajo: la influencia de una mejora en cuanto al manejo de la información optimizará no solo los procesos que implican la administración de la información si no también la gestión empresarial y mayor fidelización de los posibles clientes que esté prestando servicio.

2.2. Bases teóricas

Soriano (2014) en su libro “Seguridad en redes y seguridad de la información”. Este autor nos habla sobre la seguridad en términos de su aplicabilidad, este caso la seguridad de redes, de la información e informática. Básicamente muestra los puntos similares entre estos tres tipos y también sus diferencias.

- La seguridad de la información salvaguarda las plataformas de información para evitar un acceso, inspección, propagación, modificación, lectura, manejo o destrucción que no se haya autorizado. Por ejemplo, proteger documentos físicos confidenciales y el sistema que guarda estos mismos documentos en formato digital.
- La seguridad informática protege mediante un pool de herramientas y mecanismos la data en servidores o máquinas de cómputo de los ciberataques y posibles amenazas que se puedan identificar.
- Seguridad en la red protege todo el recurso que hace posible el envío de información mediante la red pública o privada.

En conexión con nuestra investigación la seguridad de información es protegida por nuestro usuario de Recursos Humanos, personal de TI y el proveedor Amazon. En la seguridad informática y de red el personal de TI realiza trabajos de monitoreo en los servidores donde se administra los correos y datos de Recursos Humanos, considerando también todos los recursos tecnológicos que respaldan a la seguridad perimetral.

Baca (2016) en su libro “Introducción a la seguridad informática”. El autor define en cuanto a seguridad informática como una protección de la información ubicada en un servidor o pc en base a sus características como integridad y privacidad, todo esto con el fin de estar preparados ante posibles amenazas. A parte de esto va un punto más allá que es la recuperación de la información y la prolongación del servicio que lo incluye bajo este concepto.

Dentro de seguridad informática se adiciona una propiedad que es la privacidad, el cual tiene relación con la protección de la identidad de cada usuario y sus actividades que realizadas. Por otro lado, la confidencialidad apunta a la protección contra accesos no autorizados dentro de una información, y como dice COBIT, el cifrado de datos y el seguimiento a los estándares sobre el control de acceso a la información. La UIT-T

adiciona al concepto de seguridad en la comunicación, esto significa que la data e información sólo se conectará y transmitirá entre los puntos que estén autorizados, de esta manera se maneja y hay un control al tránsito de información y data dentro de la red de esta forma se puede evitar que sea interceptada. COBIT menciona siete características principales para preservar la información. Al omitir alguna de las que menciona, ya se considera que la entidad o empresa no ha sido diligente con la seguridad requerida. La seguridad se ha estructurado en dos aspectos: las áreas y los sectores.

Estas áreas de infraestructura, aplicaciones y servicios pueden ser vulnerables en cualquier forma. El área de infraestructura el cual se incluye todo medio o dispositivo que permite hacer la transmisión ya sea a través de la red, servidores, switches se halla vulnerabilidad desde esos dispositivos mencionados. Por otro lado, el área de servicios, lo cual incluye todos los servicios de conectividad, arrendamiento de mensajería instantánea y líneas, reconoce que es vulnerable. El área de aplicaciones, como el servicio de internet es la mayor fuente de vulnerabilidad. Los tipos de seguridad puede clasificarse en: externos, internos y electrónicos también llamados como seguridad lógica y son riesgos que provienen de internet y de los sistemas lógicos del funcionamiento de los terminales. El primer riesgo puede darse cuando la información recibida no es de la fuente deseada o de donde se generó la conexión. Se aplica la autenticación, donde consiste en probar que las credenciales ya sea para solicitar un servicio o aplicación pueda ser verificada. Este proceso de autenticación garantiza que no puedan usurpar una identidad o que emita una acción no autorizada. (Pág. 53,54)

Romero, Figueroa, Vera (2017) en su libro “Introducción a la seguridad informática y el análisis de vulnerabilidades”

En varias ocasiones es usual confundir dos términos, la seguridad informática y la seguridad de la información, ambos tienen puntos que hacen la diferencia.

Para tener el concepto claro, la seguridad informática se enfoca en la seguridad del medio informático, ya que esta aplica las técnicas, procesos y métodos que hallan la manera de procesar, almacenar y transmitir la data. Por otro lado, la seguridad de la información no solo apunta por el medio informático, también se inquieta por todo lo que pueda tener data o información. El término de seguridad informática se puntualiza como la ciencia delegada en proyectar, diseñar los procedimientos, normas y métodos con la finalidad de obtener un resultado de un sistema de información seguro y disponible.

La primordial actividad de la seguridad informática es la de menguar los peligros, ya que ello proviene de muchos lados, puede ser el ingreso de datos, del medio que traslada la data o información, del dispositivo que se usa para transferir y recepcionar, o incluso los mismos usuarios. Sin embargo, la actividad primordial es de menguar las amenazas para obtener mayor seguridad.

Existen 3 puntos muy importantes en la seguridad:

- Los usuarios, en varias ocasiones suelen ser los responsables en cometer un error, olvidar o tener un accidente, y lamentablemente eso hace perder el trabajo de mucho tiempo, esto quiere decir que los sistemas en muchos casos también deben protegerse de los mismos usuarios.
- La información, es lo más importante en la seguridad informática ya que es lo que se desea proteger, en resumen, es el activo primordial.
- Finalmente, la infraestructura, este se puede controlar, pero de la misma manera corre riesgo, todo dependerá de los procesos que se manejan. Esto comprende problemas complejos como los de un acceso no autorizado, robo de identidad, de equipo, inundaciones, incendios e incluso un desastre natural el cual puede destruir o maltratar un hardware.

Postigo Palacios, Antonio, en su libro "Seguridad informática (Edición 2020)" define la seguridad informática como la capacidad de redes capaces de generar un nivel de confianza ante accidentes, malintencionadas o cualquier tipo que pueda comprometer la integridad, permanencia y autenticidad de los datos guardados, en dichas redes o sistemas ofrecidos. Para ello se debe realizar un análisis de riesgos e impactos, los cuales se debe identificar posibles daños o peligros con el fin de tomar medidas eficientes.

La seguridad informática también hace mención sobre los mecanismos que se debe seguir en cuanto a la seguridad lógica y física para mencionar algunos:

- Se debe limitar el acceso a determinados programas o ficheros mediante el uso de cifrados o claves.
- Solo debe existir los privilegios necesarios a los usuarios del sistema.
- Controlar la información entrante y saliente, y debe ser gestionado eficientemente.

Revista Polo del conocimiento (2017), incluye variada información relacionada a la seguridad informática, donde fuentes como ISOTools Excellece, que hacen mención a la seguridad informática como una disciplina y esta se encarga de brindar soluciones técnicas que protegen la información. Se resalta también que la seguridad informática protege el sistema informático lo que asegura a la organización, privacidad e integridad de la información que contiene. Además, podemos incluir que todas estas técnicas son medidas que preservaran la infraestructura y comunicación de procesos implementados por la empresa. También hace referencia que la seguridad informática y la seguridad de información son temas que se encuentran ligadas entre sí y ambos dependen uno del otro describiendo al primero como una distinción táctica y operacional de la seguridad, al otro como una línea estratégica. Ambas partes atienden datos, uno por su manera física en la protección de instalaciones, el siguiente integra la información independientemente al medio en el que se encuentre.

Luis. F. Gonzales (2016) Menciona sobre las amenazas frecuentes, las que se encuentra comprometida la tecnología cloud (Amazon Web Services), se describe como las acciones que los usuarios finales influyen y manejan en los diferentes servicios de la nube.

Y para salvaguardar la información que están en la nube, se debe considerar el trabajo colaborativo entre las dos partes es decir el proveedor que brinda el servicio y el cliente. Ambas partes deben asumir las responsabilidades.

Estos peligros se pueden aplacar a través de una planificación de seguridad como manejo hacia el acceso, lo que se traduce en generar a los backups, y todo lo establecido por políticas, acuerdos de privacidad y seguridad. Además, enumera ventajas del uso del cloud (Amazon Web Services) como lo siguiente:

- Acceso a la información desde cualquier momento y lugar.
- Rapidez en cuanto servicios y bases de datos lo que permite saltarse la adquisición del hardware.
- Es actual, ya que la mayoría de los proveedores están en constante actualización.
- Mínima inversión de infraestructura, por lo que muchas empresas se benefician por solo adquirir lo que necesitan.
- Actualizaciones automáticas, estas no afectan de forma negativa a los recursos de TI, más bien las actualizan con componentes de versiones recientes.

Areitio B. Javier (2008), en su libro "Seguridad de la información. Redes, informática y sistemas de información" Nos dice que la confidencialidad de datos es un requisito de la cual esta no debe ser revelada a individuos no autorizados, también menciona que la confiabilidad es como el aseguramiento que garantiza confianza en las medidas técnicas ideadas para proteger el sistema y la información que procesa. El autor también hace referencia a la ingeniería de seguridad, esta se desarrolla como otras disciplinas, donde se puede determinar e implementar soluciones a diversos problemas que se pueden presentar, además es parte central de todo proceso. También se encarga de garantizar que los productos o sistemas informáticos se encuentren debidamente configurados, estos no deben ocasionar riesgos. Es por eso que la organización debe ser capaz de identificar los impactos o consecuencias de pérdida o destrucción de ciertos activos. (Pág. 3, 8, 23)

Juan Voutssas M. (2013) expone en su libro "Como preservar mi patrimonio digital". Hace mención de la seguridad informática, confirmando que es "importante para los diversos conceptos básicos que la dominan, ya que de otra forma no es posible establecer una base de estudio" (Pág. 34). Recursos informáticos: telecomunicaciones, dispositivos de cómputo, los sistemas, programas y plataformas, así como la data de una empresa. También se les conoce como "activos informáticos" donde se puntualizan como:

- Amenazas informáticas: Son eventos potenciales o incidentes estos pueden estropear a los bienes informáticos de las organizaciones, proliferando malware o software malicioso con el objetivo de espiar y generar destrucción o pérdida de la información.
- Riesgos informáticos: Es cuando un evento perjudicial transcurra y se presente cuando una amenaza actúa sobre la inseguridad.
- Vulnerabilidades informáticas: Es una característica de inseguridad o debilidad de un recurso o activo informático que puede ser provocada de manera deliberada o en algunas ocasiones de forma eventual, fallas de fabricación, etc.
- Impactos: Son efectos nocivos que van en contra de la información de la organización y como consecuencia derivan a la destrucción del patrimonio documental digital o datos almacenados.

Regla básica de la seguridad informática: Tener en cuenta que la seguridad informática no se le considera como un producto, sino se le puede catalogar como un proceso.

El enfoque primordial de la seguridad informática es el de reducir lo máximo posible, los peligros y esto también conlleva los recursos informáticos, ello debe avalar la continuación de los procesos de la compañía, a su vez se debe administrar los peligros informáticos, estos no deben lograr perjudicar los costos.

2.3. Definiciones conceptuales

Seguridad física: Es aquella que brinda seguridad a los usuarios de posibles amenazas, no obstante, esta no te anticipa de todas las posibles amenazas que esté en riesgo. (Luis Daniel Álvarez Basaldúa, 2010).

Reducción de riesgo: Deben dividirse por diferentes niveles de impacto y gravedad de pérdida, primero “Estimación de riesgos de perder el recurso (Ri)”, segundo “Estimación de la importancia del recurso (Wi)”.

La evaluación de amenazas y los riesgos no debe ser una actividad, estas deben realizarse con regularidad. (Luis Daniel Álvarez Basaldúa, 2010).

Confidencialidad datos: “El perjuicio que puede ocasionar un manejo negligente de información confidencial puede traer como resultado de que se haga pública, o accedan a ella en contra de los intereses del sujeto.” (Jonás Gonseth, 2009, p.35)

Evolución de sistemas: Los sistemas de información han evolucionado sistemáticamente, y dividiéndose en partes, el primero de ellos sistemas de información empresariales, simplifican las distintas labores de la compañía con el uso de herramientas contables y particulares en su necesidad. Luego el desarrollo de la informática y las telecomunicaciones han incrementado la capacidad en la ejecución de las actividades, simplificar tiempo en el desarrollo de las tareas y guardar grandes cantidades de información en un espacio reducido (Alejandro Hernandez Trasobares, 2011, p.54)

Supervisión y monitoreo: La supervisión y la valoración son primordiales para cualquier proceso de ejecución, ya sea de un proyecto o programa. El trabajo requiere una acumulación de datos de procesos cotidianos para evaluar los avances hacia la meta de los objetivos del programa. Se maneja un registro del desempeño de los programas en el lapso de tiempo, y su fin es ayudar a los interesados a tomar decisiones registradas con respecto al rendimiento de los programas y el uso de los medios. (Nina Frankel, 2009)

Seguridad Amazon Web Services: Amazon Web Services (AWS). Contiene diversos complejos como AppDefense [seguridad de las aplicaciones en entornos virtualizados

y cloud] y varias soluciones de rendimiento del datacenter. Esto incluye la migración desde los centros de datos – concebidos como “nubes privadas” – hacia las nubes híbridas que serán el modelo de computación dominante en los próximos años. (Norberto Gallego, 2017)

Disciplina administrativa: Se enfoca en un estudio sistemático de las actividades, el análisis de procedimientos y la manera de hacerlos competentes incluyendo identificar sus objetos y sujetos de estudio. Por otro lado, la parte teórica de la administración gerencial (o gerencia administrativa) concentra su atención en la manera de aumentar los sistemas de control, de acuerdo con la estructura organizacional; además de analizar la eficiencia y efectividad.

Mercadotecnia: Esta es una diligencia que se relaciona con los mercados, que se traduce en laborar con ellos para renovar los intercambios potenciales con el propósito de cumplir con las necesidades de la población. Y se inclinan en cuatro pilares:

Necesidades del usuario, mercado meta, marketing integrado y beneficio; por ello, (el concepto de mercadotecnia) cambia un panorama de afuera hacia adentro; es decir comienza con un mercado bien definido, se enfoca en las necesidades de los clientes, organiza todas las actividades que alterarán a los usuarios y crea utilidades al satisfacerlos. (Philip Kotler, 2012)

Supervisión con CloudWatch: Amazon CloudWatch dispone la verificación de los bienes e información de la nube de Amazon Web Services y de las plataformas que los usuarios corren en Amazon Web Services. Los administradores del sistema y desarrolladores la usan para juntar y recopilar medidas y ejecutar el seguimiento que se registró, de esta manera se pueda responder rápidamente para que sus aplicaciones y empresas sigan operando sin inconvenientes. (Franco Bocchio ,2014)

Arquitecturas orientadas a servicios: También abreviado a SOA es una interfaz que construye toda una topología de la aplicación. Esta suministra una separación entre la interfaz y el modelo de servicio con sus posibles agregaciones. Por lo que las aplicaciones que consumen un servicio pueden interactuar con diversos proveedores. (Alier, M, 2009)

Calidad de servicio: La calidad de un producto o servicio no se define por ser una percepción subjetiva; sin embargo, se puede definir que es la impresión que el usuario tiene. Es una imagen del cliente que da aprobación de un servicio o producto, que solo

permanece hasta el punto de requerir nuevas indicaciones. (María V. Requema Ponce, Gabriela C. Serrano, 2007)

Análisis de tráfico de redes: El aumento de nuevas plataformas y tecnologías han incrementado la complejidad en redes públicas y privadas. Por lo cual los protocolos para ingresar de manera segura a estos datos podría ser por ejemplo http, https, ftps, firewall, nats.

3. CAPÍTULO III: DESARROLLO DEL PROYECTO

3.1. Arquitectura empresarial

3.1.1. Arquitectura de Información (Datos)

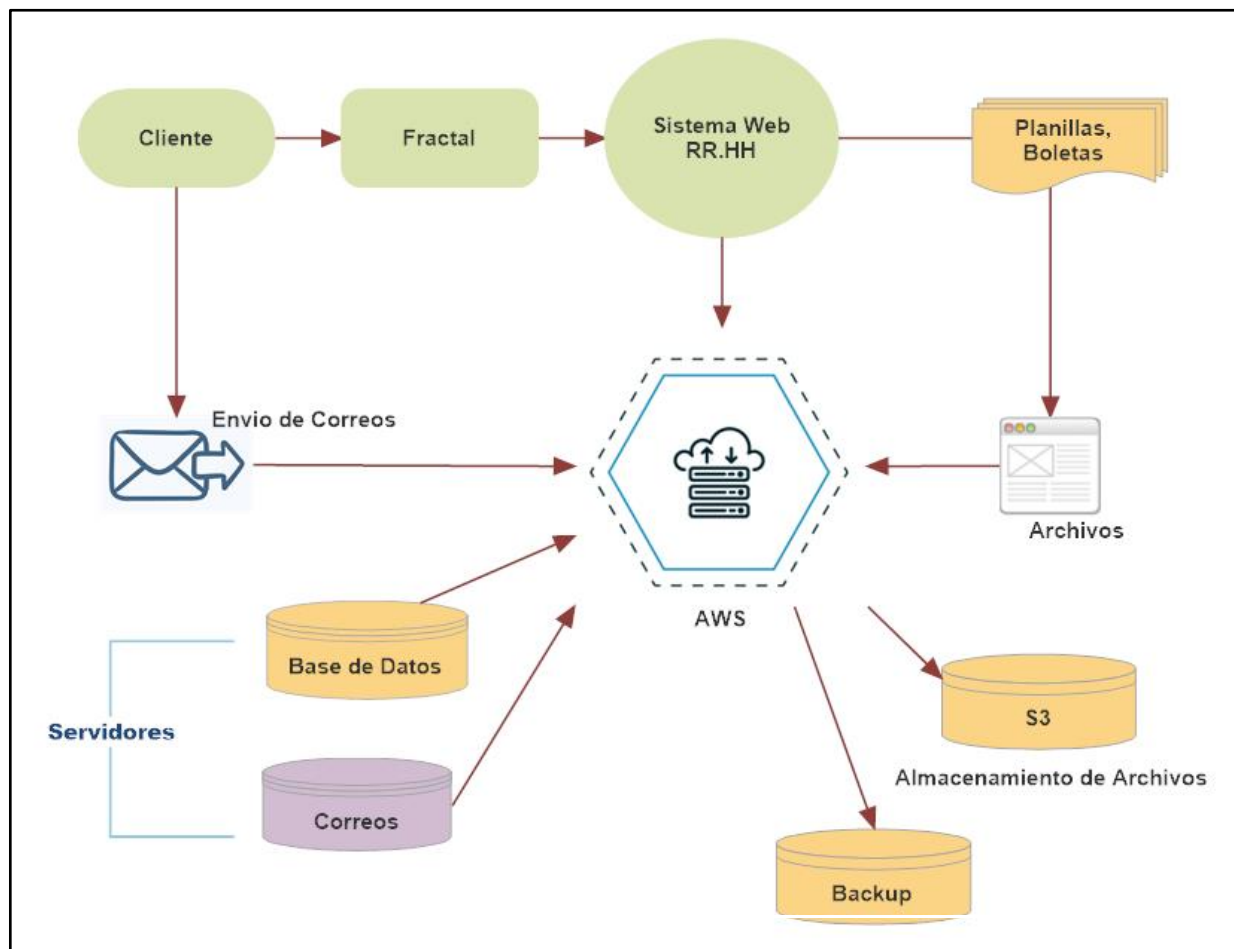


Figura 3: Flujo del proceso al acceso de la aplicación

La ejecución y plan de gestión de servicio en la nube con Amazon Web Services se estableció de la siguiente manera:

El Cliente, tiene a su disposición el envío de correos directamente con el servicio de Amazon Web Services, además toda solicitud o carga será realizada por las respectivas áreas de la empresa Fractal.

Fractal (Áreas correspondientes), interactúan con el sistema web de Recursos Humanos, se encarga de emitir toda información relacionada y/o enviada por el cliente respectivo.

Sistema Web, El sistema registra, actualiza toda información aplicada por las áreas correspondientes de Fractal a su vez se encarga de la ejecución de notificación de registro de planillas, boletas previamente firmadas digitalmente a los correos, de las cuales deben estar almacenados en los repositorios de Amazon Web Services s3 y bases de datos.

Amazon Web Services, Está configurado para realizar un backup por un determinado tiempo, además está configurado para borrar correos antiguos del servidor por un tiempo máximo de 6 meses.

3.1.2. Arquitectura de Negocios (Procesos)

Mapa de procesos de la empresa Fractal SAC

Procesos clave: Servicios, nuevos proyectos

Objetivo: Otorgar soluciones que contribuyan al mejoramiento de los procesos y negocios de los clientes, donde las solicitudes de servicio abarquen el desarrollo y mantenimiento de los sistemas en uso, ayuda completa al usuario, atención de requerimientos e incidencias.

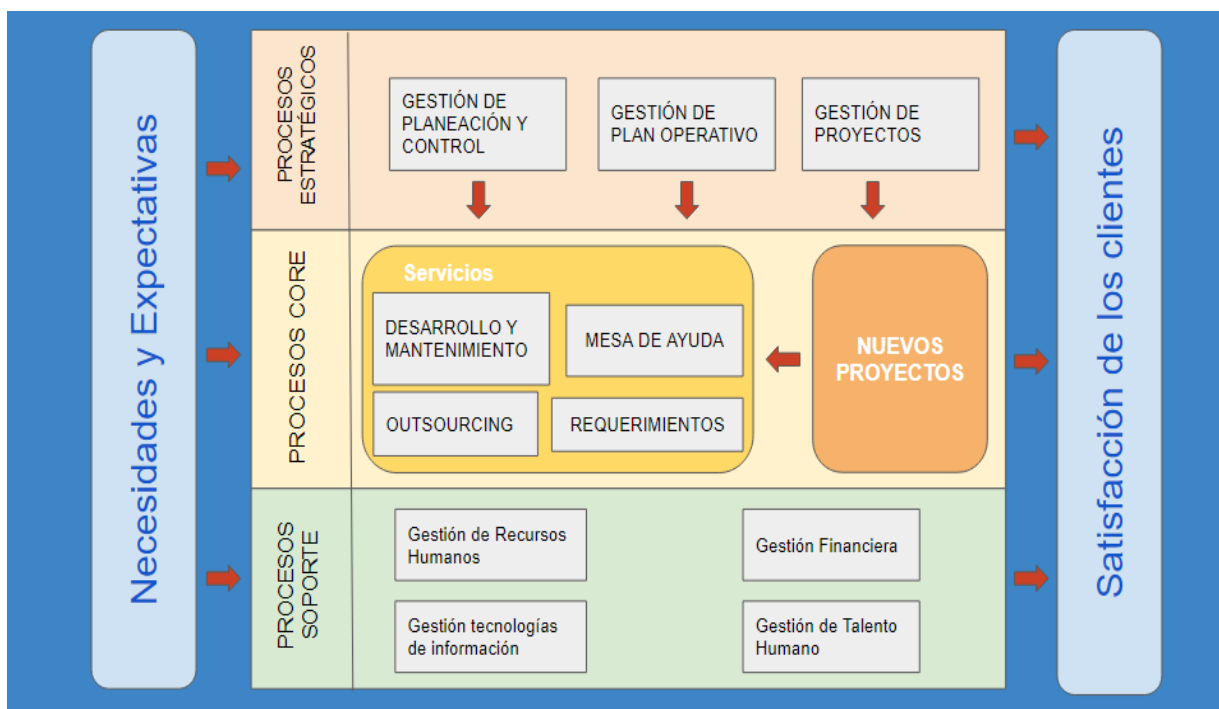


Figura 4: Macroproceso de la empresa Fractal

A continuación, se muestra el siguiente diagrama (Business Process Management) BPM del proceso clave objeto de nuestra investigación considerando la implementación de Amazon Web Services.

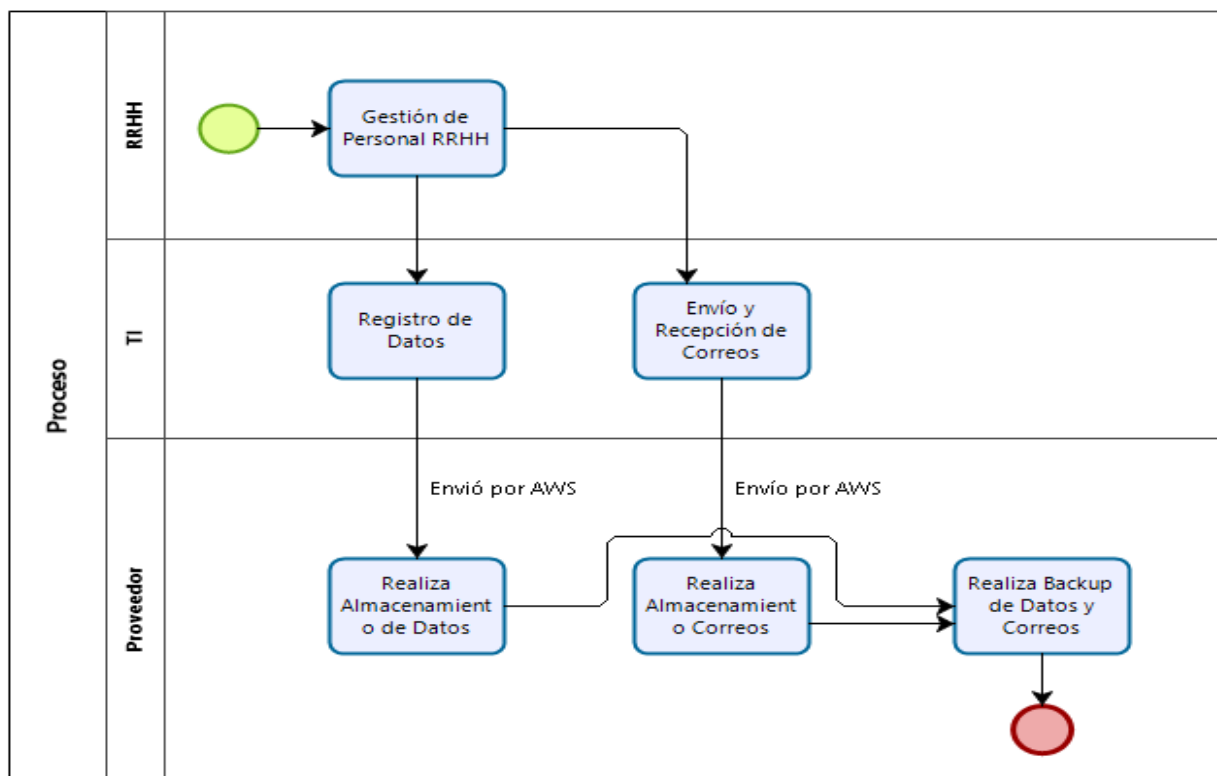


Figura 5: Proceso con la implementación con Amazon Web Services

3.1.3. Arquitectura de Aplicación

El sistema de Recursos Humanos Fractal actualmente cuenta con diversos subsistemas para la administración del personal de diversos clientes este sistema se asemeja a un Enterprise Resource Planning (ERP) y está parametrizado para el uso y necesidad de cada cliente. El sistema de Recursos Humanos de Fractal tiene una arquitectura integrada donde interactúan diferentes componentes como módulos, plugins, librerías, frameworks, APIs entre sí y de manera estructurada; esta arquitectura resuelve diferentes necesidades y aspectos de manera versátil y sencilla.

Arquitectura N-Capas

Esta arquitectura se compone generalmente por las tres siguientes capas:

Capa cliente o presentación: Representa la interfaz al usuario.

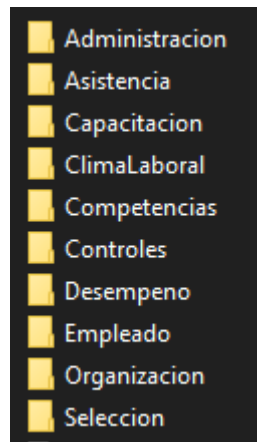


Figura 6: Desarrollo de capa presentación

Capa de lógica de negocio: Procesa la información mediante las reglas y lógica del negocio lo que implica recibir las peticiones de la capa datos y mostrar resultados en la capa presentación.

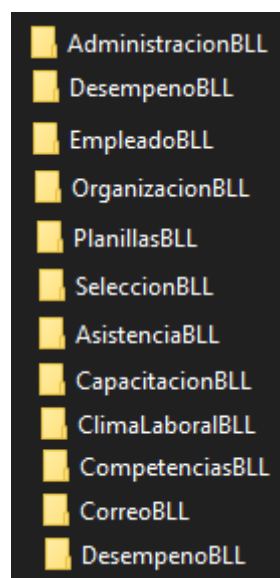


Figura 7: Desarrollo capa lógica de negocio

Capa de acceso a datos: Se encarga del almacenamiento o recuperación de los datos, todas emitidas por la capa negocio.

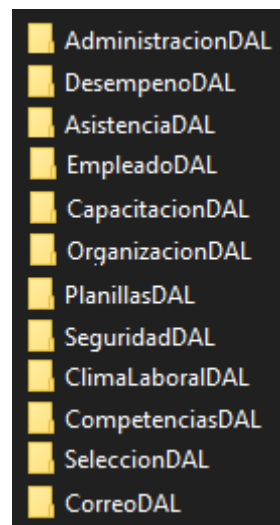


Figura 8: Desarrollo de capa datos.

Arquitectura del Sistema de Recursos Humanos de Fractal a Amazon Web Services

El sistema de Recursos Humanos de Fractal es una plataforma adaptable por a las necesidades de los clientes gracias a que es parametrizada, y la estructura de trabajo es adecuada para el servicio de Amazon Web Services ya que es un sistema web la capa lógica y la capa de datos están situadas en el servicio de Amazon Web Services haciendo más sencilla la emisión y recepción de las solicitudes.

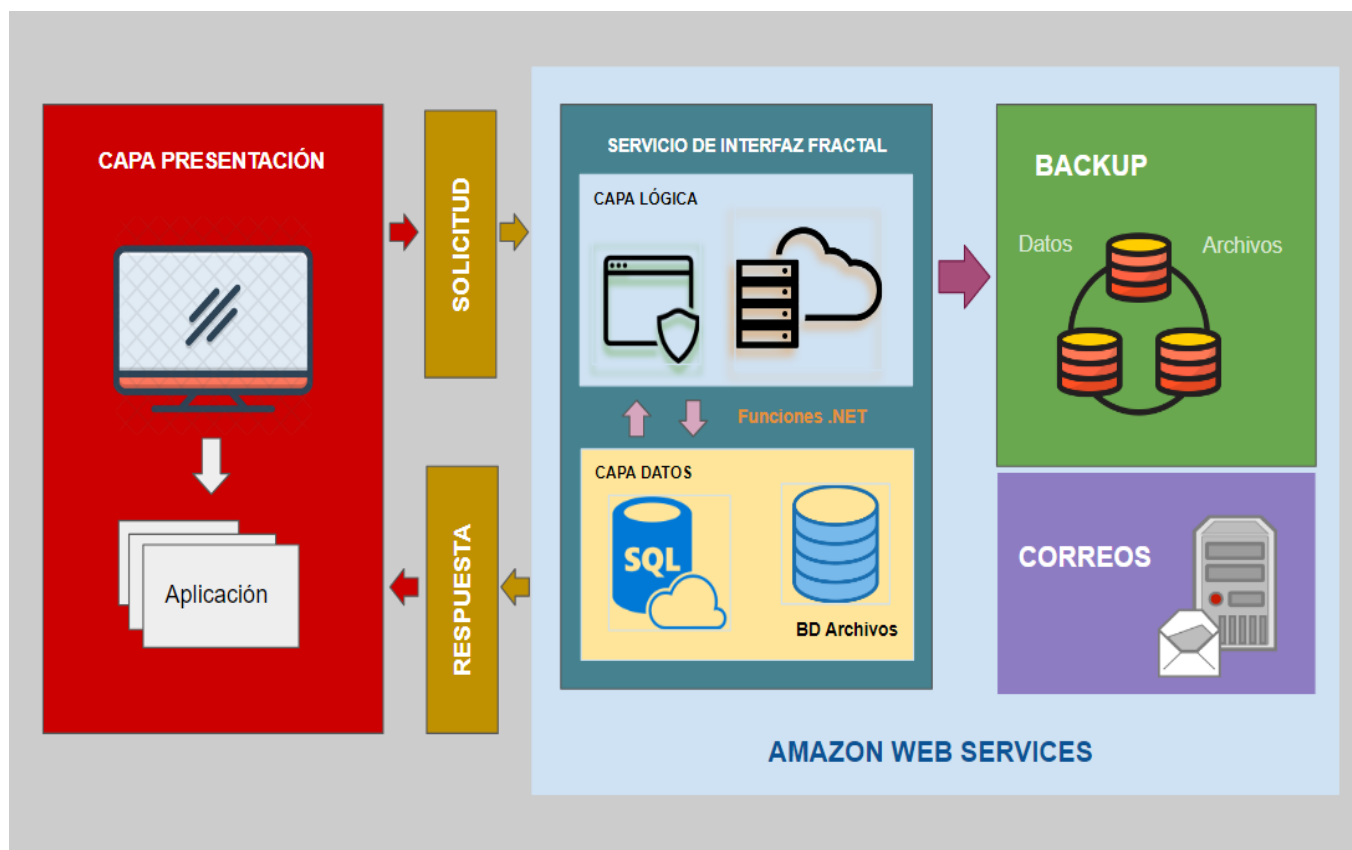


Figura 9: Arquitectura del Sistema de Recursos Humanos de Fractal.

3.1.4. Arquitectura Tecnológica

La aplicación de la empresa Fractal, está compuesta por servidores, sistemas informáticos, redes alámbrica e inalámbrica, esta arquitectura está diseñada e implementada para red LAN del Fractal y para que diferentes usuarios puedan acceder desde cualquier punto.

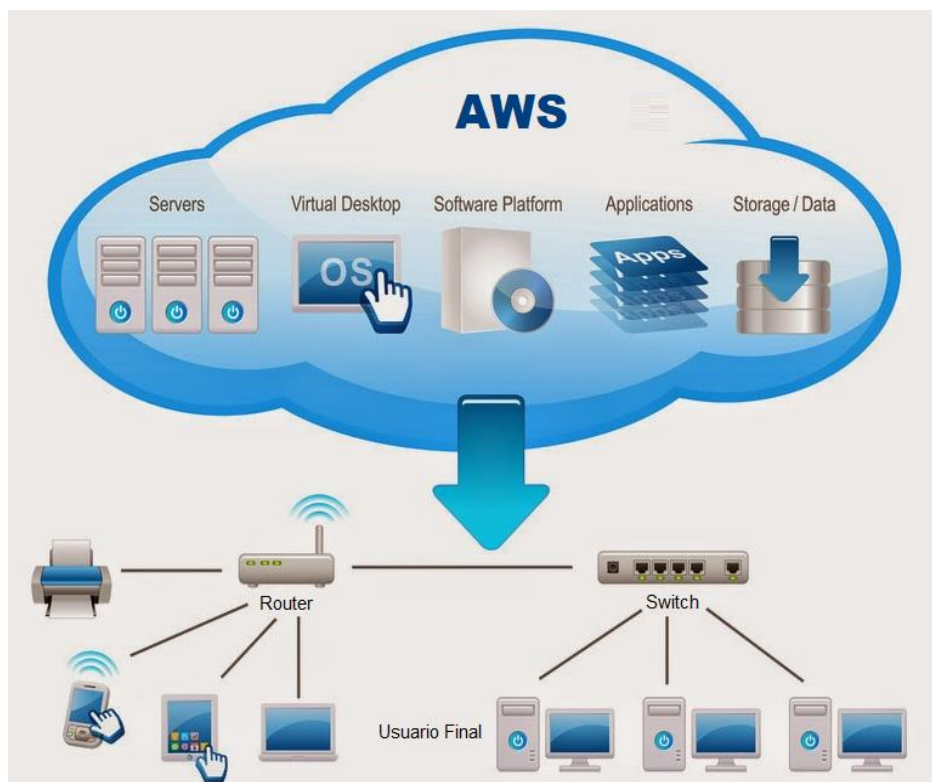


Figura 10: Arquitectura tecnológica de la empresa Fractal

La infraestructura tecnológica que se requiere para la implementación se describe lo siguiente:

a) Hardware

Referimos al hardware a los equipos que van a hacer parte de la implementación porque se requiere de equipos que permitan el uso adecuado y bastante potente, entre ellas tenemos.

- **Servidor**

Se requiere como servidor un equipo diseñado para el proceso de trabajo a realizar, este equipo se describe de las siguientes características.

| N.º | ACTIVO FIJO | MARCA | MODELO | MEMORIA RAM | HDD |
|-----|-------------|-------|-----------|-------------|--------|
| 1 | SERVIDOR BD | IBM | POWER 730 | 6 GB | 500 GB |

| | | | | | |
|---|-----------------|-------|-------------|------|--------|
| 2 | SERVIDOR BD | CISCO | UCS B200 M4 | 6 GB | 500 GB |
| 3 | SERVIDOR BD | CISCO | UCS B200 M4 | 6 GB | 500 GB |
| 4 | SERVIDOR BD | IBM | POWER 710 | 4 GB | 350 GB |
| 5 | SERVIDOR BD | IBM | POWER 710 | 6 GB | 500 GB |
| 6 | SERVIDOR APLIC. | IBM | POWER 710 | 16GB | 1TB |
| 7 | SERVIDOR APLIC. | IBM | POWER 710 | 16GB | 1TB |
| 8 | SERVIDOR FILE | CISCO | UCS B200 M4 | 12GB | 1TB |

Tabla 2: Descripción de servidores de la empresa Fractal.

| CARACTERÍSTICAS | Amazon |
|--------------------------|--|
| SERVICIOS DE COMPUTACIÓN | <ul style="list-style-type: none"> - Soporte para plataformas Windows y Linux. - Escalado automático. - Instancias básicas. - Informática de alto rendimiento. -Instancias de GPU. |
| ALMACENAMIENTO | <ul style="list-style-type: none"> - Almacenamiento (S3) para el respaldo de objetos. - Elastic Block Storage (EBS) respaldo de bloques persistentes para usar con EC2. - Elastic File System (EFS) respaldo de archivos. - Base de datos y archivos: SQL llamada Aurora, Relational Database Service (RDS), base de datos DynamoDB NoSQL. |
| IMPLEMENTACIÓN | <ul style="list-style-type: none"> - La nube de Amazon dispone una web de colocación muy fácil e intuitiva de utilizar para iniciar a usar sus herramientas y soluciones. |

Tabla 3: Características de la implementación del servicio Amazon Web Services.

b) Software

Las plataformas para usar para la implementación el módulo desarrollado es la aplicación de reclutamiento, visual studio, SQL server 2019, sistema operativo Windows 10, Altova reporting y Amazon Web Services.

Amazon Web Services cuenta con una gran cantidad de herramientas que continúan creciendo exponencialmente, las capacidades de Amazon son inigualables. No obstante, su forma de costos puede ser confusa al inicio, y su enfoque particular en la nube pública en lugar de la nube híbrida o la nube privada, significa que la interacción con tu centro de datos no es la prioridad de Amazon Web Services. Cuenta con más clientes de alto perfil y conocidos como Netflix, Airbnb, Unilever, BMW, Samsung, MI, Zynga, etc.

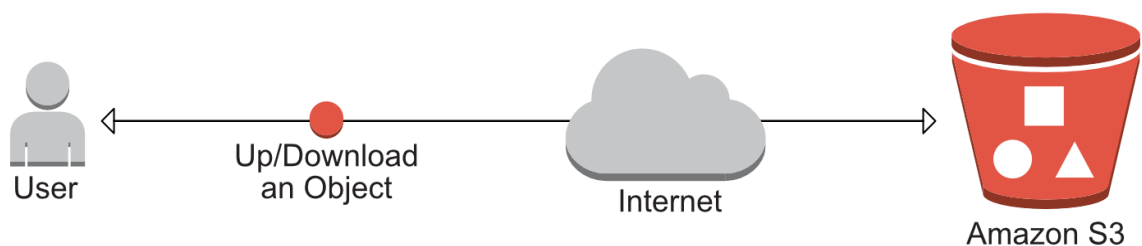


Figura 11: Flujo de conexión del usuario con Amazon Web Services

Dentro de las características que cuenta Amazon Web Services -S3 es:

Durabilidad de los datos

Protege los backups con una durabilidad de datos. Los backups de todos los archivos subidos a Amazon S3 Glacier y Amazon S3 empiezan y se guardan en al menos tres mecanismos en una sola región de Amazon Web Services.

Flexibilidad y escalabilidad

Es configurable los recursos de generación de backup en poco tiempo. Esto permitirá mejorar la operatividad, invención y haciendo ágil el proceso.

Copias de seguridad para todos los tipos de datos

Permite la carga de copias de seguridad de cualquier tipo de archivo, además de contener una variedad de servicios de reserva, esto aporta a que sea accesible en el momento que se requiera.

Seguridad y conformidad

Protege los backups con una red establecida para las organizaciones exigentes en cuanto al tema con la seguridad. Cuenta con una interfaz para poder administrar el acceso, detectar las actividades irregulares, poder cifrar los datos y realizar auditorías con los servicios de Amazon Web Services security. Amazon Web Services también cuenta con programas de conformidad que ayudan a cumplir todos los requisitos normativos.

Métodos de transferencia de datos

Optimiza la transferencia de grandes cantidades de información por internet, sin conexión y de forma local.

4. CAPITULO IV: RECURSOS Y CRONOGRAMA

4.1. Recursos

A continuación, se muestra el cuadro de recursos considerando los costos por mes.

| Actividades | Recurso | Costo en (USD) |
|----------------------------|------------|----------------|
| Recursos Humanos | | |
| Desarrollador | 3 personas | 3000.00 |
| Analista Funcional | 1 persona | 1200.00 |
| Analista QA | 1 persona | 1100.00 |
| Ingeniero de requerimiento | 1 persona | 1100.00 |
| Arquitecto de software | 1 persona | 1500.00 |
| Consultor | 2 persona | 2600.00 |
| Analista DBA | 1 persona | 1400.00 |
| Infraestructura | 1 persona | 1200.00 |
| Soporte | 2 persona | 2200.00 |
| Jefe proyecto | 1 persona | 1800.00 |

Tabla 4: Costo de talento humanos.

| | | |
|--------------------------|-------------|-----------------|
| Recursos Software | | |
| Visual Studio 2019 | Gratuito | 0.00 |
| Microsoft Office 365 | 8 usuarios | 960.00 |
| Altova Reporting | 3 licencias | 513.00 |
| Amazon Web Services S3 | Por 500 TB | 1050.00 |
| Sql Server 2019 | 3 licencias | 3856.00 |
| TOTAL | | 34279.00 |

Tabla 5: Costo de implementación del servicio.

4.2. Cronograma de ejecución

Ejemplo:

Continuando con el diagrama de Gantt, el cronograma de actividades corresponde desde 01 mayo hasta 31 de octubre del 2020. A continuación, se pone a detalle las actividades y el tiempo destinado para su realización.

| ACTIVIDADES/SEMANA | 2020 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|------|---|---|---|-------|---|---|---|-------|---|---|---|--------|---|---|---|------------|---|---|---|---------|---|---|---|--|--|--|--|--|
| | Mayo | | | | Junio | | | | Julio | | | | Agosto | | | | Septiembre | | | | Octubre | | | | | | | | |
| | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | | | | | |
| PLAN DE TRABAJO | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Planeación del proyecto Análisis de requerimientos, alcance, elaboración de actas, planeación de recursos, análisis arquitectura | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Análisis infraestructura, redes e implementación de escenario desarrollo | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Desarrollo, pruebas unitarias, documentación de desarrollo | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Elaboración de plan de pruebas, ejecución de pruebas (stress, usuarios, trazabilidad, base de datos, código) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Reunión de control de cambios, acta control de cambios | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Implementación escenario certificación, pruebas de BD, validación de funcionalidades | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Capacitación de usuarios y pruebas de usuarios | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Ejecución cambios finales, pruebas de integración | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Implementación escenario producción, pruebas de BD, pruebas finales | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Salida a producción, acompañamiento al usuario | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Fin de proyecto | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Tabla 6: Cronograma de actividades para la ejecución del proyecto

5. CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

De acuerdo con las investigaciones realizadas podemos concluir:

- Por el mismo hecho de contratar los servicios de un proveedor en la nube como es Amazon los temas respecto a monitoreo de red, ciberseguridad y capacidad de almacenamiento los podemos derivar en manos del personal especializado ya que estos han sido garantizados mediante un SLA el cual podemos ir manejándolo y adaptándolo a las necesidades actuales de Fractal, por lo tanto esto quiere decir que el personal de TI solo supervisará el servicio del proveedor y se enfocará en mayor medida a los requerimientos propios de Fractal. También a largo tiempo se podrá visualizar un ahorro en costos ya que es más beneficioso contratar los servicios de un proveedor en la nube en comparación a la adquisición de servidores y especialistas propios que se encarguen de mantener este servicio.
- Al realizar la migración hacia la nube del sistema de Recursos Humanos a Amazon Web Services. Se realizó un plan de soporte, el cual tiene tareas que permiten a la empresa continuar con sus actividades en caso haya un incidente. Además, se respetó el modelo de trabajo de la empresa Fractal, mejorando de forma productiva los procesos iniciales. Esto contribuyó a agilizar las actividades que ejercen los colaboradores diariamente, de las cuales quedaban en stand by o en cola. Aunque no todo fue favorable al momento de la ejecución. Ya terminada la implementación de Amazon Web Services los resultados fueron satisfactorios para los clientes y colaboradores.
- Amazon Web Services tiene un alto nivel de protección de datos de sus clientes ante situaciones sospechosas, alertando a los usuarios de lo sucedido. Esta característica puede ser configurable con múltiples reglas de seguridad, desencadenando eventos que ayudan a desviar e impedir exponer los datos. Además, la plataforma de Amazon Web Services es muy flexible para crear un proyecto de cualquier dimensión. En Amazon Web Services se tiene toda una infraestructura, contando con un abanico de opciones y configuraciones

que se pueden seleccionar, desde el tipo de sistema operativo con el que se va a trabajar hasta opciones de escalamiento si la organización crece.

5.2. Recomendaciones

- Se recomienda investigar sobre la facturación de los servicios cloud ya que están apareciendo nuevos proveedores que brindan dichos servicios, los cuales pueden ser más económicos debido a que recién están saliendo al mercado. En tanto se recomienda contar con herramientas alternativas en caso sea necesario, debido a que se puede dar el caso que alguna de las políticas cambie e impacten negativamente al proyecto.
- Se recomienda realizar la migración de los servidores ya sean virtuales o físicos en un horario que no afecte las operaciones del negocio, en caso no sea posible hacerlo, se recomienda que el procedimiento ocasione el menor impacto posible.
- Es recomendable para el tema de resguardo de información se establezca de forma precisa mediante un acuerdo los puntos que garanticen que no se genere pérdida, filtración y el tratamiento indebido de la información proporcionada. Esto es más que todo porque se almacena información confidencial de la empresa Fractal que como bien sabemos son correos y data de Recursos Humanos.

6. CAPÍTULO VI: FUENTES DE INFORMACIÓN

6.1. Referencias electrónicas

Bibliografía

3Ciencias Editorial Científica. (2018, 16 octubre). Introducción a la seguridad informática y el análisis de vulnerabilidades. Recuperado de <https://www.3ciencias.com/libros/libro/introduccion-a-la-seguridad-informatica-y-el-analisis-de-vulnerabilidades/>

Arango Moreno, C. (2015). EVOLUCIÓN E IMPACTO DE CLOUD COMPUTING EN EMPRESAS GRANDES DE DIFERENTES INDUSTRIAS DEL SECTOR CORPORATIVO EN ANTIOQUIA. Recuperado de <https://core.ac.uk/download/pdf/47251881.pdf>

Areitia Bertolin, J. (2008). Seguridad de la información. Redes, informática y sistemas de información. Recuperado de https://books.google.com.pe/books?id=_z2GcBD3deYC&lpg=PP1&dq=seguridad%20de%20la%20informaci%C3%B3n&pg=PR3#v=onepage&q=seguridad%20de%20la%20informaci%C3%B3n&f=false

Castro Martínez. (2019). Seguridad Informática y Seguridad de la Información - Docsity. Recuperado de <https://www.docsity.com/es/seguridad-informatica-y-seguridad-de-la-informacion/5683841/>

Córdova Rodríguez, N. E. (2003). Plan de seguridad informática para una entidad financiera. Recuperado de https://sisbib.unmsm.edu.pe/bibvirtualdata/tesis/basic/Cordova_RN/Cap6.PDF

EditorE. (2015, 10 abril). ISO 27001: Seguridad informática y seguridad de la información. Recuperado de <https://www.isotools.org/2015/01/05/iso-27001-seguridad-informatica-seguridad-informacion/>

Escorcía, K. A. M. (2014). Seguridad en redes y seguridad de la información. Recuperado de https://www.academia.edu/40156122/Seguridad_en_redes_y_seguridad_de_la_informaci%C3%B3n

Figuroa Suárez, J. A. (2018, 12 marzo). Polo del Conocimiento. Recuperado de <https://polodelconocimiento.com/ojs/index.php/es/article/view/420/pdf#>

González Hernández, L. F. (2016). Aspectos de Seguridad Informática en la Utilización de Cloud Computing. Recuperado de

<https://repository.unad.edu.co/bitstream/handle/10596/6173/6662779.pdf?sequence=1&isAllowed=y>

- Granados, M. (2015, 8 noviembre). INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA | SEGURIDAD INFORMÁTICA. Recuperado de <https://diarium.usal.es/martagmx/2015/11/08/introduccion-a-la-seguridad-informatica/>
- Hernández Trasobares, A. (2003). Los sistemas de información: evolución y desarrollo. Recuperado de <https://dialnet.unirioja.es/servlet/articulo?codigo=793097>
- IICD. (2011). Computación en la nube - Imaginar. Recuperado de <https://www.yumpu.com/es/document/read/22619193/05-computacion-en-la-nube-imaginar>
- Instituto Nacional de Ciberseguridad. (2017, 20 marzo). Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? Recuperado de <https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian>
- La virtualización y el centro de datos definido por software. (2020, 17 diciembre). Recuperado de <https://www.vmware.com/latam/solutions/software-defined-datacenter/in-depth.html>
- Meléndez Barzanallana, R. A. (2013, 13 octubre). 12.1 Introducción a la calidad. Recuperado de <https://www.um.es/docencia/barzana/IAGP/IAGP2-Calidad-informatica.html>
- Morales, R. M. (2012, 4 julio). seguridad informatica. Recuperado de https://es.slideshare.net/raisa_22_acuario/seguridad-informatica-13543798
- Rodrigo, J. M. (2014, 14 agosto). Arquitectura Orientada a Servicios (SOA). Recuperado de <https://emergingtechuva.wordpress.com/2013/11/25/arquitectura-orientada-a-servicios-soa/>
- Rodríguez, T. (2019, 18 junio). La otra guerra entre Microsoft, Google y Amazon: la batalla por controlar los servicios en la nube para... Recuperado de <https://www.xataka.com/servicios/otra-guerra-microsoft-google-amazon-batalla-controlar-servicios-nube-para-desarrolladores>
- Solorzano, E. M. (2020, 24 septiembre). Historia y evolución de la nube. Recuperado de <https://blog.smartekh.com/historia-y-evoluci%C3%B3n-de-la-nube>

- Thompson, I. (2006, julio). EL CONCEPTO DE MERCADOTECNIA - Promonegocios.net. Recuperado de <https://www.promonegocios.net/mercadotecnia/concepto-de-mercadotecnia.html>
- Tivit Latam. (2019). AWS o Microsoft Azure. Recuperado de <https://latam.tivit.com/blog/aws-o-microsoft-azure-cual-es-la-mejor-opcion-para-mi-empresa>
- Toro Rodríguez, R. (2015, 20 octubre). ISO 27001: Consejos del experto en seguridad informática. Recuperado de <https://www.isotools.pe/iso-27001-consejos-experto-en-seguridad-informatica/>
- Universidad Nacional de Valencia. (2019). ¿Qué es la seguridad informática y cómo puede ayudarme? | VIU. Recuperado de <https://www.universidadviu.com/co/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme>
- Voutssas Marquez, J. (2011). Cómo preservar mi patrimonio digital personal. Recuperado de <http://www.librosoa.unam.mx/handle/123456789/2178>