ALIANZAEFI
economía formal e inclusiva

Protocolo de captura, gestión y gobernanza de la información para el Centro de Datos Alianza EFI

Jefferson Arias Gómez
Javier Ríos
Julián Peñuela

Documentos Alianza EFI
Junio 2020
Número de serie: D7-2020-001

COLOMBIA CIENTÍFICA
Conocimiento Global para el Desarrollo

Protocolo de captura, gestión y gobernanza de la información para el Centro de Datos Alianza EFI.

Proyecto 7. Laboratorio social

Corporación Universitaria Minuto de Dios

***Abstract*— This document contributed to the documentation about the security of the data center, its characteristics, its construction at a logical and physical level, complying with certain safety, performance and efficiency regulations. The following document describes the protocol for data capture, management and governance that will be managed from the Center for Development Thought, in accordance with the activities established in the project 7 Social Laboratory of the program of productive and social Inclusion: programs and policies for the promotion of a formal economy of the National Government Colombia Scientific Program *.**

Resumen— Este documento contribuye a la documentación sobre el funcionamiento del centro de datos, sus características, su construcción a nivel lógico y físico, especificando normas de seguridad, rendimiento y eficiencia.

El siguiente documento describe el protocolo de captura de datos, la gestión y la gobernanza que se gestionará desde el Centro para el Pensamiento del Desarrollo, de acuerdo con las actividades establecidas en el proyecto 7 Laboratorio Social del programa de Inclusión productiva y social: programas y políticas para la promoción de una economía formal del Programa Científico del Gobierno Nacional de Colombia *.

The data capture, management and governance protocol of the Center for Development Thought seeks to be generated from the creation of working groups among the members of the EFI Alliance - Formal and Inclusive Economy - and will define: i) the capacities of each member in the technical and technological contribution for the implementation of the hardware and software infrastructure; ii) The utilities that allow data manipulation and analysisis, maintaining privacy, legally and security reserve of sensitive information; and iii) the articulation of the primary information (result of the different projects of the program) and secondary, in order to generate added value.

I. INTRODUCCIÓN

En el siguiente documento se expone el protocolo de captura de datos, la gestión y la gobernanza de los mismos que se desarrollará en el centro de datos, de acuerdo con las actividades establecidas en el proyecto 7 Laboratorio Social del programa de Inclusión productiva y social: programas y políticas para la promoción de una economía formal del programa de Gobierno Nacional Colombia Científica*.

El programa “Inclusión productiva y social: programas y políticas para la promoción de una economía formal” de la Alianza EFI es desarrollado bajo el componente de Ecosistema Científico el cual hace parte del programa del Gobierno Nacional Colombia Científica (2017), que busca “apoyar la consolidación de un sistema de investigación e innovación de excelencia científica articulada con el sector productivo, para contribuir a mejorar la competitividad, productividad y desarrollo social del país.

La Alianza EFI – Economía Formal e Inclusiva – dentro de su programa “Inclusión productiva y social: programas y políticas para la promoción de una economía formal” tiene como objetivo general diagnosticar, examinar e intervenir factores y barreras que afectan la inclusión social y productiva, integrando un ecosistema interdisciplinario en el cual participan diferentes entidades públicas y privadas.

El programa está conformado por una totalidad de siete proyectos de investigación de los cuales en el siguiente documento se presenta el protocolo de captura de datos, la gestión y la gobernanza del centro de datos para el Desarrollo del proyecto 7. Laboratorio Social: estrategias de innovación social, tecnologías experimentales y apropiación social del conocimiento para la promoción de la formalización e inclusión social y productiva de diferentes agentes económicos.

El protocolo de captura de datos hace referencia a la recopilación manual o automatizada de información, la gestión es un conjunto de procesos con los cuales se controla el ciclo de vida de la información, desde su obtención hasta su disposición final, la gobernanza hace referencia a los deberes que tiene el recolector de la información con esta y su buen manejo; estos métodos y acciones que se aplicarán y desarrollarán en el centro de datos, buscan garantizar el acceso y la disponibilidad de la información de las diferentes intervenciones que tienen lugar en el Ecosistema Científico, el cual busca el fortalecimiento de las capacidades investigativas de todo el proyecto.

II.ALCANCE

Para el proyecto 7, Laboratorio Social, la gobernanza de datos que garantiza la gestión global de la disponibilidad, facilidad de uso, la integridad y la seguridad de los datos provenientes de diferentes fuentes y disciplinas es uno de los principales activos no solo para el desarrollo de investigación científica, sino también un recurso para la generación de valor agregado en un contexto de innovación social. Por otra parte el centro de datos facilitará la identificación, monitoreo y evaluación de intervenciones que tiene lugar en este ecosistema científico y los datos serán utilizados i) en procesos de toma de decisiones, donde diferentes tipos de análisis de la información son requeridos; ii) en las estrategias de integración y iii) en el diseño

de las estructuras de datos que se utilizan para soportar dichos análisis, así como en el uso de algunas metodologías, tecnologías y herramientas de apoyo.

III.DEFINICIONES GENERALES

A. *Base de Datos*

Una base de datos es un contenedor que almacena información de manera organizada, la cual tiene un propósito específico o diferentes usos dentro de un contexto.

B. *Centro de datos*

Un centro de datos es un término usado en la informática que hace referencia a un espacio que sirve como un contenedor de recursos tecnológicos que permiten procesar una cantidad masiva de información.

C. *Protocolo informático*

Se refiere a un conjunto de normas o reglas que rigen y regulan la manera de comunicación entre dos o más sistemas informáticos a través de varios canales o medios de conexión.

II. CENTRO DE DATOS

Un centro de datos es un término usado en la informática que hace una referencia a un espacio que sirve como un contenedor de recursos tecnológicos que permiten procesar una cantidad masiva de información.

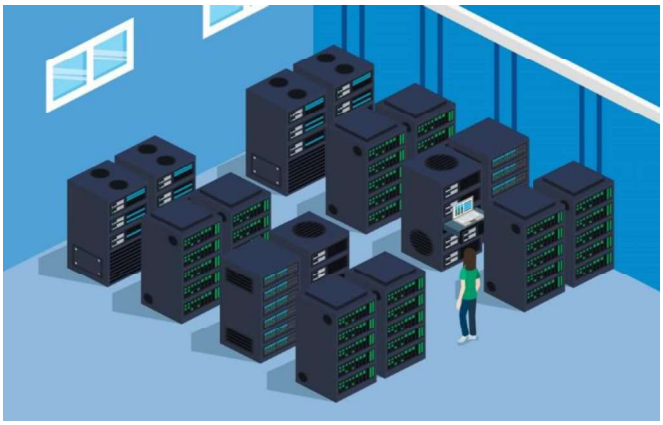

Fig1.Imagen de un Centro de datos.

A. *Estructura física*

Un centro de datos en su parte física está acondicionado por una serie de computadores y otros dispositivos de hardware tales como servidores, routers, sistemas de almacenamiento y sistemas de comunicaciones. Este tipo de contenedor de datos almacena gran cantidad de datos, posee sistemas de respaldo de energía, así evita inconvenientes de tipo eléctrico entre los componentes y la pérdida o daños en la información.

El modelo para el centro de datos cuenta con 4 procesos fundamentales en las cuales se trata el tema de la disponibilidad y su tiempo fuera de línea, los casos de emergencia y los procesos de mantenimiento de forma offline u online.

B. *Ubicación*

Como está estipulado en el cronograma de productos de la alianza el centro de datos estará ubicado en un cuarto especialmente acondicionado en el Colegio Mayor de Nuestra Señora del Rosario, y deberá cumplir con características técnicas requeridas para el acondicionamiento, tenencia, seguridad y capacidad de espacio para escalabilidad y sostenibilidad a lo largo del proyecto de la Alianza EFI.

La ubicación exacta del centro de datos será en la calle 12C N. º 6-25 en el departamento de tecnología informática y comunicaciones.

El centro de datos estará ubicado dentro del centro de tecnología del Colegio Mayor de Nuestra Señora del Rosario según lo estipulado en el plan de trabajo del centro de datos.

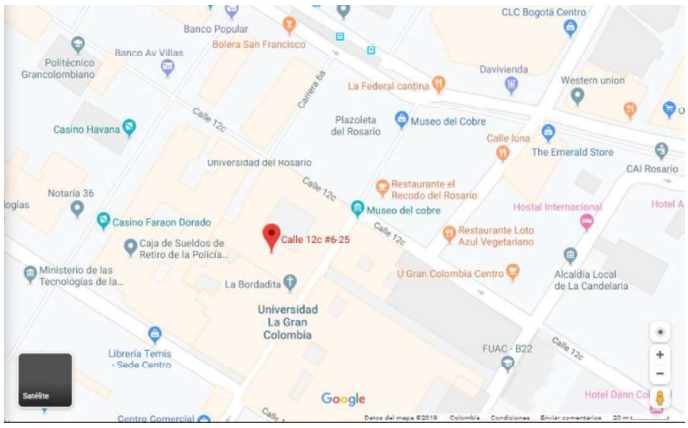

Fig 2. Ubicacion geográfica del centro de tecnología del Colegio mayor de nuestra señora del Rosario.

C. *Disponibilidad del centro de datos*

El concepto de disponibilidad del centro de datos está orientado al contexto de los procesos que se encuentran contemplados en el marco de trabajo de la Alianza EFI, esto hace referencia a la capacidad para garantizar el acceso de los usuarios, procesos, servicios e información a almacenar en un tiempo de operación especifico.

La disponibilidad de la información contenida en el centro de datos está sujeta a los permisos definidos en cada proyecto y a los métodos de seguridad definidos por el administrador del centro de datos.

D. *Tiempo offline del centro de datos.*

Para garantizar el tiempo de disponibilidad del centro de datos según la clasificación TIER (nivel de fiabilidad de un centro de datos asociados a cuatro niveles de disponibilidad definidos) se ha especificado que el centro de datos puede pertenecer al nivel 1 en donde el servicio puede interrumpirse por actividades planeadas o no

planeadas, puede o no tener suelos elevados, generadores auxiliares o UPS, la infraestructura del centro de datos deberá estar fuera de servicio al menos una vez al año por razones de mantenimiento y/o reparaciones. Los niveles TIER que se mencionan anteriormente son:

a. Nivel uno

El nivel uno determina que el centro de datos debe contar con una única ruta que le proporcione energía y refrigeración, además tener pocas piezas redundantes y elementos para copia de seguridad de ser necesarias, este nivel establece el tiempo de actividad del centro de datos del 99, 671 por ciento anualmente.

b. Nivel dos

El nivel dos determina qué el centro de datos debe contar con una única ruta de energía y refrigeración, algunos componentes redundantes y de seguridad, además de un tiempo de actividad anual aproximadamente del 99, 741 por ciento.

c. Nivel tres

El nivel tres determina que el centro de datos debe tener implementadas por lo menos tres rutas de energía teniendo una principal y una de respaldo, al igual que una refrigeración, también debe contar con sistemas de implementación de actualizaciones para mantener el centro de datos con las últimas novedades y mantenerlo en un constante funcionamiento, para este nivel el centro de datos tiene aproximadamente un tiempo de actividad del 99. 982 por ciento anual.

d. Nivel cuatro

Este nivel representa la seguridad total de un centro de datos, que basa su diseño en una estructura tolerante a fallos de cualquier tipo, además de que presenta redundancia para cada componente del centro de datos, este nivel es también éste proyecta un mayor tiempo de actividad anual del centro de datos teniendo aproximadamente el 99,995 por ciento.

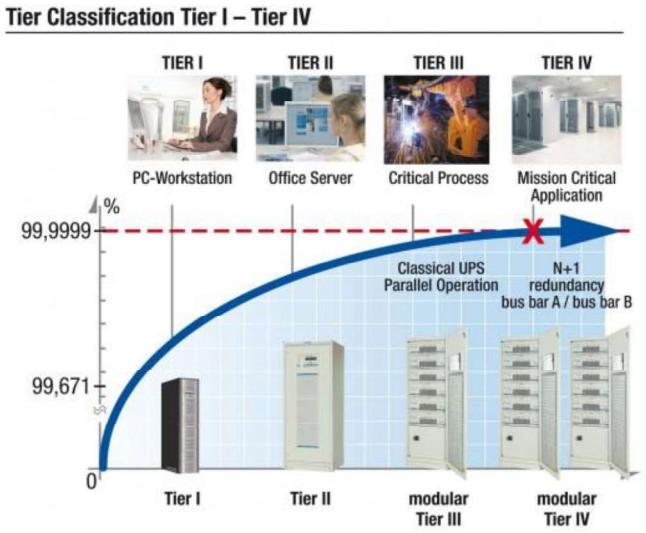

Fig3. Niveles de tier de un centro de datos.

E. Casos de emergencia del centro de datos.
Como cualquier sistema de información, el centro de datos está expuesto a ataques informáticos, problemas técnicos, daños físicos entre otros, por eso desde el principio se debe garantizar la seguridad teniendo en cuenta procedimientos generales de redivisión, además de diseñar un sistema de seguridad robusto para la salvaguarda de la información. Un objetivo es tener un sistema flexible que se pueda adaptar rápidamente y gestionar un plan efectivo contra las emergencias identificadas.

F. Procesos de mantenimiento del centro de datos.
Según un estudio realizado en el UpTime Institute se calcula que las fallas presentadas en los centros de datos se deben hasta en un 40% a interrupciones del sistema debido a falencias en la infraestructura.

El Centro de datos de la Alianza EFI tiene contemplado realizar planes de mantenimiento al centro de datos periódicamente para evitar un deterioro de los equipos, prevenir reiteración de fallas, maximizar la confiabilidad del centro de datos además de garantizar la seguridad y disponibilidad de este.

G. Captura de los datos.
El centro de datos de la alianza EFI dentro de su fase de diseño y creación planea el almacenamiento de información de encuestas, cálculos, registros, documentos de texto, videos, fotos, mapas y demás de los 7 grupos de trabajo, también a partir de las necesidades de dichos grupos apoyar en los procesos de recopilación, procesamiento, consulta y divulgación de dicha información.

Existen convenios entre miembros de la Alianza EFI y entidades gubernamentales que facilitarán la consulta y utilización de información de sus bases de datos, el centro de datos puede ser utilizado también como repositorio de las mismas o como facilitador en la solicitud de registros específicos. Estos convenios son los que podemos ver a continuación en la figura 4.

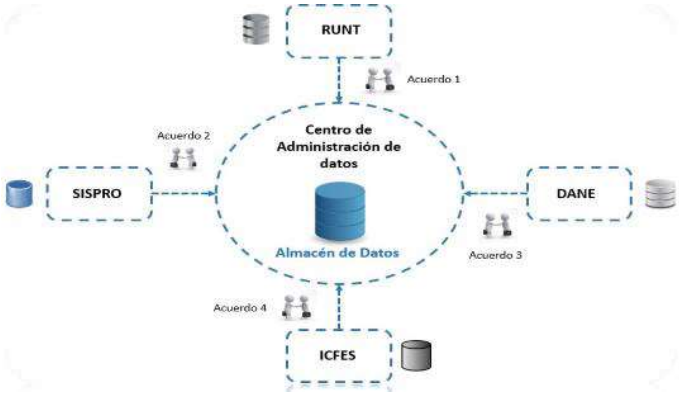

Fig4. Convenios para la utilización de datos.

H. Gestión de los datos

Para el proceso transversal de la gestión de la información, teniendo en cuenta lo pactado en las reuniones que ha tenido el componente del centro de datos, se especifica que los datos que se recopilen **deben** estar anonimizados o pasar por un proceso para lograrlo. Por datos anonimizados entendemos a los datos procesados de tal manera que no se puedan identificar específicamente individuos de una sociedad, además de ocultar la información sensible que implique una vulneración a los derechos de la protección de datos de las personas y organizaciones que dispongan de dicha información.

En coherencia con lo expuesto, el proceso de compilación de la información del centro de datos contará con herramientas informáticas que permitan, previo a su tratamiento, la anonimización y agrupamiento de los datos, de manera rápida y confiable. Si bien es necesaria la información individual para consolidar información agregada, el centro de datos también proporcionará una manera segura de hacer esta transición de agregación, sin poner en riesgo la información individual.

I. Gestión de la tecnología.

El centro de datos contará con una capacidad de almacenamiento escalable a la medida que se desarrollen los proyectos que componen la alianza EFI. Por el momento se tiene 4x 3.84 Tb de almacenamiento, ya que se empezará con un único servidor y posteriormente se vinculará otro servidor nuevo para expandir las capacidades del centro de datos.

El centro de datos constantemente está en mantenimiento, optimización para asegurar un funcionamiento óptimo, las necesidades del centro de datos a medida que el tiempo pase se evaluaran y añadirá nuevos servicios dependiendo las necesidades que presenten los demás proyectos de la alianza EFI.

Para garantizar las estrategias de redundancia y recuperación de data se planea usar el modelo RAID (Redundant Array of Independent Disk) para la duplicación y salvaguarda de los datos, esta técnica replica de manera exacta toda la información contenida en el disco duro del centro de datos sin crear la preocupación de copias de seguridad.

RAID garantiza obtener la redundancia, menos latencia y aumentar el ancho de banda para leer o escribir en discos maximizar la probabilidad de recuperar la información suponiendo que se allá presentado una amenaza o cuando el disco no funciona correctamente.

El método RAID plantea también ciertos niveles en su estructura, en este caso se necesitan 2 o más discos de almacenamiento del mismo tamaño, de esta manera garantizamos que todo lo que escribamos en un disco se copie al otro automáticamente; en dado caso que uno de los dos discos falle se tiene la otra unidad con la información guardada, así se evita la pérdida de información.

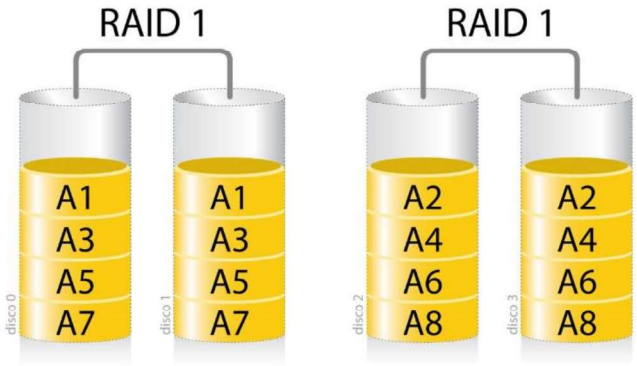

Fig5. Modelo RAID nivel1.

J. Protocolos de transferencia de archivos.

a. FTP(File Transfer Protocol)

Es un protocolo utilizado para la transferencia de archivos entre sistemas, la lógica de este protocolo consiste en que desde un equipo el cliente se puede conectar al centro de datos, para recibir o enviar archivos independientemente del sistema operativo que esté utilizando cada uno , dado que cada transferencia se realiza sin ningún tipo de cifrado se propone como solución la aplicaciones del paquete SSH que permite la transferencia de archivos cifrando todo el tráfico.

b. HTTPS (Hypertext Transfer Protocol Secure)

El protocolo http es un protocolo creado por al WWW el cual nos permite realizar la transferencia de archivos y la realización de peticiones peticiones de datos por

medio de la web , este protocolo esta basado en la arquitectura cliente servidor.

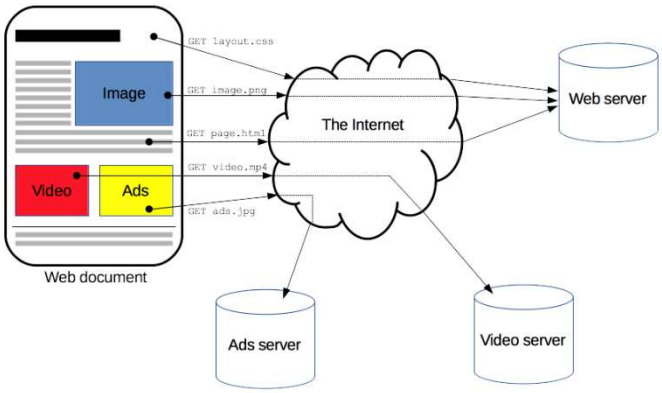

Fig5. Lógica del protocolo HTTP.

c.M2M (machine to machine)
M2M es un protocolo orientado al intercambio de información o como canal de comunicación en forma de datos entre dos máquinas remotas. Para poder implementar este protocolo se necesitan los elementos y configuraciones que se conectan a una máquina remota, estas conexiones proveen de comunicación al servidor, posteriormente el servidor gestiona la acción a realizar ya sea recepción o envió de información, por último se necesita la red de comunicación por cable o a través de redes inalámbricas

IV.SEGURIDAD DEL CENTRO DE DATOS

La seguridad de un centro de datos se ve desde dos aspectos que son:

A. *Físico*

La seguridad física del centro de datos es un aspecto importante, que se abordará desde dos ejes. En primer lugar, la verificación de los usuarios que tendrán acceso al centro de datos usando herramientas de hardware y software de reconocimiento biométrico para su identificación; esto proporcionará al centro de datos una seguridad más robusta en la infraestructura física y el control de misma. Los métodos de verificación biométrica en el mercado actualmente para este proceso y sus características de calidad son:

a. Voz
b. Escritura y firma
c. Huellas Dactilares
d. Escaneo de retina
e. Escaneo de iris
f. Geometría de la mano
g. Validación de tarjeta.

	Voz	Escritura Firma	Huellas Dactilares	Ojo Retina	Ojo Iris	Geometría de Mano
Fiabilidad	alta	alta	alta	muy alta	muy alta	alta
Facilidad de Uso	alta	alta	alta	baja	media	alta
Prevención de Ataques	media	media	alta	muy alta	muy alta	alta
Aceptación	alta	muy alta	media	media	media	alta
Estabilidad	media	media	alta	alta	alta	media
Identificación	no	si	si	si	si	
Autenticación	si	si	si	si	si	si
Interferencias	ruidos, resfriados	firmas fáciles	suciedad, heridas	irritación	gafas	artritis, reumatismo

Fig7. Métodos de autentificación biométrica tomada de la plataforma virtual https://www.estrategiamagazine.com/tecnologia/los-controles-biometricos-verificacion-de-voz-escritura-huellas-patrones-oculares-retina-iris-geometria-de-la-mano/.

En segundo lugar, las instalaciones físicas del centro de datos estarán vigiladas por personal de seguridad profesional de confianza para la Universidad, además de estar grabado 24 horas al día por un circuito cerrado de televisión.

El centro de datos tendrá instalado hardware de control electrónico especializado para la seguridad biométrica, ya que esto ayuda a la identificación de las personas y/o visitantes para controlar su acces, se debe además tener un modelo de seguridad multinivel, qué hace referencia a tener una caja fuerte dentro de otra caja fuerte ya que reduce los riesgos de intrusión física y digital de la información.

B. Software y lógica

A nivel de software, debe garantizarse el tratamiento de la información en un ambiente seguro. Con este objetivo, el centro de datos debe estar protegido contra las interceptaciones de datos a través de las comunicaciones entre el usuario y el centro de alojamiento de datos; para ello se utilizará un protocolo de seguridad para la base de datos, para la conexión y para la manera en que se envían los datos, el cual se diseñará acorde a estándares de seguridad como ISO27000 y sus apartados tales como ISO27000-1, ISO27000-2 ISO27000-3 ISO27000-4, ISO27000-5 , ISO27000-6, ISO27000-7., respecto a la protección contra delincuentes informáticos, el centro contará con un firewall de alto nivel y/o un antivirus corporativo que aporte aspectos fuertes de seguridad y un control estricto de las contraseñas de acceso al centro de datos, ya que el usuario puede ser víctima de virus, spyware, malware, pishing etc. dando acceso al centro de datos y su información.

Es importante recalcar que la información individual estará salvaguardada de su mal uso por parte de cualquier agente. Para lo anterior, el centro de datos contará con las herramientas informáticas necesarias para proteger la información individual sensible, previamente a cualquier uso. Esto brindando procedimientos de agregación automáticos, cuando la información requerida sea a niveles superiores; y anonimizando la información, cuando el uso de la información sea a nivel individual.

V.CATÁSTROFES Y PÉRDIDAS

Uno de los servicios que proporciona el centro de datos es un cubrimiento total de la información ante situaciones que podría causar riesgos en la integridad física y digital, si algún error llegar a ocurrir y que Este sea de carácter potencial, el centro de datos sufriría pérdidas inevitables que probablemente causan daños irreversibles, aplicando esta lógica en el centro de datos de nuestro proyecto si la información ,la infraestructura y demás sufre un daño irreversible llevará al proyecto a un posible cierre o una pausa, ya que en el centro de datos se encuentra toda la información y datos que recopilen los demás equipos, esta información a su vez es de vital importancia para contribuir en el desarrollo y la solución de una problemática en el país por esto lo más recomendable es periódicamente tener un backup (respaldo) de la información del centro de datos en un lugar confiable y seguro, los centros de datos pueden pasar por una serie de riegos en su funcionamiento que lo afectan de manera física o lógica y los más comunes se encuentran evidenciados en la fig5.

Fig8. Incidentes más comunes que generan fallas en el servicio de un data center.

VI.CARACTERÍSTICAS QUE DEBE TENER UN CENTRO DE DATOS.

El servicio principal del centro de datos además de almacenar la información para una empresa o proyecto también es proteger la información que en él se almacena y garantizar la calidad del servicio de este, para ello el centro de datos tiene ciertas características de seguridad y de calidad que son 8:

A. Escalable

El centro de datos debe ser escalable con esto se hace referencia a que el centro de datos puede manejar y soportar un crecimiento continuo sin ser propenso a fallas y si las fallas se presentan puede restablecer el servicio nuevamente usando partes que sirvan para ello, se aconseja organizar los racks o los contenedores de una manera que permitirá un crecimiento ordenado y sustentable, esto también permitirá como se dijo anteriormente que si se presenta una falla poder conectar el sector daño con un sector funcionando y posteriormente realizar el mantenimiento pertinente para restablecer el servicio .

B. Flexible

El centro de datos debe ser capaz de adaptar y sostener los nuevos requerimientos que se vayan integrando a su infraestructura, ya que los componentes del centro de datos se van modernizando porque son piezas de tecnología las cuales cada vez evolucionan más para proveer al centro de datos de características de optimización, estas decisiones estructurales y cambios en el centro de datos mejoran el funcionamiento, rendimiento y demás servicios de este.

C. Confiable

El centro de datos debe tener una disponibilidad total para las personas que tienen acceso a él y un servicio ininterrumpido, ya que si se crean interrupciones en el servicio se pueden generar pérdidas de información, dañar la información, sufrir vulnerabilidades o pérdidas económicas importantes.

Para garantizar la confiabilidad del centro de datos es necesario tener elementos de contingencia para fallas eléctricas, de red, de refrigeración y protocolos de seguridad de red para el componente de la comunicación y tratamiento de datos.

D. Seguridad

La seguridad del centro de datos es un apartado de vital importancia, es la prioridad que se debe tener a la hora el manejo de información debido a que la información que contenía en el centro de datos es de un gran valor para el propósito del proyecto y su perdida significaría grandes pérdidas económicas.

La información que se alberga acá deberá tener varios mecanismos de seguridad, para poder asegurar su integridad dentro de la base de datos, para probar la vulnerabilidad en la seguridad del centro de datos en el tema de información se deben calcular todos los escenarios posibles qué pueden afectar a esta, se debe designar a una persona cómo Tester para qué haga casos de prueba y poder así identificar fallas seguridad y poner suplir estas amenazas.

E. Modular

El centro de datos debe tener un diseño modular ya que al separar las funciones y componentes en módulos es más fácil el mantenimiento, manejo y replicación de información en los módulos.

F. Estandarizado

Se debe tener estandarizados la mayoría de los servicios y procedimientos del centro de datos, ya que esto provee una capacitación interna del funcionamiento del centro de datos y esto genera beneficios a nivel de costos de mantenimiento, implementación y optimización de servicios establecidos.

G. Seguridad y rendimiento

Se propone aplicaciones orientadas al monitoreo del rendimiento del centro de datos que arroje estadísticas y alertas sobre el funcionamiento y demás características de las cuales se puede avaluar la calidad y optimización del centro de datos, se propone usar las siguientes opciones:

* Nagios (Nagios Open Software License, GPL)

*Solaris (Solaris pc Netlink, Solstice Disksuite, Netscape Comunnicator 4.5)

*Solarwinds (Application-Centric Monitos, SAM, WPM)

*Icinga

*PandoraFMS (de pago) (Monitorización SAP)

H. *Certificación del cableado estructurado*

El centro de datos debe estar ordenado y deberá buscar una certificación de cableado estructurado, esta certificación plantea un proceso de comparación de rendimiento de transmisión de un sistema de cableado instalado con un determinado estándar en el centro de datos implementando una metodología definida por el estándar para poder medir esta característica.
Esta certificación demuestra la calidad de los componentes, instalación y nos indica si hay un correcto funcionamiento físico.

Para medir y estructurar lo mencionado anteriormente se propone para el centro de datos el estándar **EIA/TIA-568-B** que son estándares que tratan el tema del cableado comercial , distancias, conectores, arquitecturas , terminaciones de cables y características de rendimiento orientado a los productos y servicios de telecomunicaciones , edificios comerciales y estructuras en entornos de campus, el estándar pretende cubrir un rango de vida de más de diez años para los sistemas de cableado comercial.

.

VII. MEDIDAS DE SEGURIDAD DEL CENTRO DE DATOS

Las medidas de seguridad de un centro de datos se deben diseñar desde el principio de la planeación de la infraestructura de este, el centro de datos debe tener seguridad tanto física como lógica, para la parte física se debe tener en cuenta los estándares de infraestructura del centro de datos, el marco legal de construcción, de este y los demás componentes como, por ejemplo, la potencia eléctrica, las opciones de conexión y la protección de las comunicaciones el centro de datos.
Se tendrán en el centro de datos sistemas instalados para la detección de sobrecalentamiento, fugas de agua e incendios, ya que sí no se manejan correctamente estos accidentes se podrían generar pérdidas millonarias en infraestructura y también se pueden causar pérdidas irreversibles en el centro de datos.

VIII. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DATOS

Se propone que el centro de datos va a contar con un sistema de gestión de la seguridad de la información, ya que el propósito de este sistema es garantizar que los riesgos de seguridad de la información contenida en el centro de datos Sean conocidos, asumidos, gestionados, y minimizados Por el proyecto de manera documentada, sistemática, estructurada, eficiente y que se adapte a las variaciones o cambios que se produzcan en los riesgos, el entorno y la tecnología (ISO, 2014)

El sistema de gestión de la seguridad de la información ayuda a definir ciertas políticas y algunos procedimientos basados en los objetivos del negocio de la organización con un propósito de tener un bajo perfil de exposición de la información de la organización,

Fig9. SGSI lógica según la ISO

A. ¿Qué elementos y políticas genera un sistema de gestión de la seguridad?

Un sistema de gestión de la seguridad está contemplado gráficamente como un sistema jerárquico de 4 niveles (Fig. 10) qué son:

a. Manual de seguridad.

El manual de seguridad de un sistema de gestión de la información está contemplado como el documento qué específica y rige el funcionamiento de todo el sistema, en él se exponen los criterios de alcance, objetivos, responsabilidades y las demás políticas de la organización y características definidas del centro de datos.

b. Procedimientos.

Define un documento donde se explica la forma correcta que asegura que se efectúen de manera eficaz y controlada los procesos de seguridad de la información. (ISO, 2014)

c. Instrucciones, chekclist y formularios.

Define un documento donde se explica cómo se deben realizar todas las tareas y actividades en el manejo de información para asegurar el tratamiento de ésta. (ISO, 2014)

d. Registros, políticas de seguridad, alcance y objetivos.

En este nivel el SGSI Define documentos que contribuyen cómo soporte de cumplimientos de los servicios y requisitos del sistema de gestión de seguridad de la información, además también se incluyen varios documentos de soporte y reglamentación como por ejemplo alcance del sistema de gestión de la seguridad, política y objetivos de seguridad, procedimientos y mecanismos de control, informe de evaluación de riesgos y plan de mitigación y tratamiento de riesgos (ISO, 2014)

Fig10. Niveles de un sistema de gestión de la seguridad.

B. Implementación de un sistema de gestión de seguridad de la información

Para implementar un sistema de gestión de la seguridad de la información basándose en el estándar ISO 27001, se debe utilizar y gestionar un ciclo continuo que es denominado como PDCA qué escribe ciertos pasos a seguir en el sistema de gestión de calidad, estas iniciales hacen referencia a 4 pases importantes que son:

a. Plan (Planificar)

El centro de datos en su fase de planificación determinara las necesidades básicas del centro de datos, además de especificar ciertas funcionalidades teniendo en cuenta los demás proyectos que pertenecen a la Alianza EFI; una vez se define esto, se tiene en cuenta la constante evolución del centro de datos, se tendrán opciones de escalabilidad para optimizar a lo largo del proyecto la optimización y sostenibilidad del centro de datos.

b. Do (Hacer)

El componente del centro de datos determinó una necesidad inicial en temas de hardware y por ello se cotizó con el proveedor DELL un servidor con características específicas que se ajustan a las necesidades del proyecto de la Alianza EFI.

Se planeará también una definición de roles en el centro de datos. Hasta el momento el único rol definido con más fortaleza es el del administrador del centro de datos, el cual gestionara y llevara a cabo la siguiente parte del planeamiento inicial del centro de datos.

c. Check (verificar)

Constantemente se monitoreará el rendimiento y salud del sistema por medio de un software, ya que gracias a una constante verificación se pueden mitigar a tiempo problemas que afecten la integridad del centro de datos.

d. Act (actuar)

El proyecto tendrá una durabilidad de 4 años, se planea dar sostenibilidad al centro de datos en este periodo de tiempo y posteriormente tener un centro de datos funcional que pueda seguir contribuyendo a proyectos de investigación.

IX. CARACTERÍSTICAS DE LA SEGURIDAD DE LA INFORMACIÓN.

Por seguridad de la información se entiende que es el conjunto de reglas, métricas, parámetros que permiten proteger y resguardar la información, buscando mantener ciertas características principales que son la confidencialidad, la disponibilidad, la integridad de los datos y la autenticación.

A. Integridad

Esta característica es la información de la seguridad busca mantener la información y los datos exentos de cambios o modificaciones no autorizadas por el administrador del centro de datos, la integridad también hacer referencia a la propiedad de guardar los datos importantes con precisión y completitud sin pérdida alguna en su traslado, esta característica puede ser violada cuándo un emplead o software que elimina o modifica parte o toda la información almacenada en el centro de datos.

Para asegurar esto se tendrán medidas de seguridad en la conexión autentificando a los usuarios del centro de datos, así como a su miembro, para ello se propone un sitio web o una conexión con certificados digitales o el protocolo SSH

B. Confidencialidad

Esta característica especifica e impide la divulgación de información a personas que no se encuentren autorizadas por el centro de datos además de asegurar el acceso a la información única y estrictamente a las personas que cuenten con la debida autorización para hacer cambios en su estructura realizar alguna operación con ella.

Para mantener confidencialidad de la información se la presentará a los usuarios del centro de datos los términos y condiciones de uso de la plataforma y la manera del manejo de la información del centro de datos, el usuario deberá leer y aceptar estas políticas para informarse del uso correcto, el

acuerdo de confidencialidad y por último las consecuencias de incurrir en una infracción a las políticas el centro de datos de la Alianza EFI y su información.

C. Disponibilidad

Esa característica especifica que la información debe estar completamente a disposición para las personas que necesitan acceder a ella, esta disponibilidad debe ser de tiempo completo y sin restricciones.

El concepto de disponibilidad aplicado al centro de datos orientado al contexto de los procesos que se encuentran contemplados en el marco de trabajo de la Alianza EFI se refiere a la capacidad de garantizar el acceso los usuarios a los procesos, servicios y datos que se van a almacenar en el centro de datos.

D. Autenticación

Esta propiedad permite verifica e identificar quién es la persona responsable de generar cierta información, al verificar e identificar la persona que genera la información podemos saber qué operaciones realizó dentro del centro de altos y así poder determinar si fue una operación entre la información o trato de generar daños, cambios, eliminar o dañar la información.

X. USUARIOS DEL CENTRO DE DATOS

Un usuario se define técnicamente como los usuarios y objetos que interactuaran dentro del sistema.

A. Clasificación de usuarios

Los usuarios se clasifican dentro de un conjunto de funciones, privilegios, recursos a los que una persona, máquina o recurso involucrado en el centro de datos tiene acceso

.

B. Tipos de usuarios

Los usuarios básicos para cualquier sistema de información como el centro de datos son:

a. Invitado

Se clasifica para un usuario del centro de datos como invitado si no es un usuario registrado con permisos para poder realizar operaciones y cambios en la información.

b. Miembro

Son usuarios que ya están identificados dentro del sistema por medio de un nombre y una contraseña esto le permite el acceso a la información que el sistema está permitido a mostrarle, un sistema puede tener tantas vistas como usuarios tenga.

c. Usuario Registrado

Son personas que sé encargan de crear usuarios en el centro de datos y tienen el acceso a modificar ciertos aspectos y contenidos adicionales a los que un miembro no puede entrar.

d. Administradores

Son usuario con acceso total al centro de datos o el sistema de información, se encargan de añadir nuevos servicios al módulo, además de gestionar la alta y baja de usuarios registrados entre otros.

C. Autenticación de usuarios.

El centro de datos verificara a un usuario por medio de un formulario de logueo donde se valide un nombre de usuario y una contraseña, como se hace en distintas plataformas de varias entidades públicas y privadas.

El nombre de usuario será asignado por la plataforma dependiendo los datos personales que el usuario proporcioó al registrarse, la contraseña se generará de manera automática la primera vez y se le notificará al usuario cual es, cuando el usuario acceda al sistema inmediatamente se le pedirá un cambio de contraseña con caracteres alfanuméricos de mínimo 8 elementos.

XI.CANALES DE TRANSMICIÓN DE ATAQUE A SISTEMAS DEINFORMACIÓN.

Las principales amenazas que afectan a los sistemas de información en general y las herramientas más usadas para generar ataques son:

*Malware y Spam
*Ataque contra el XML de tráfico y la arquitectura orientada a servicios web
*Ataques de suplantación de páginas.
*ataques de phishing por medio de sitios web.
*Interceptación de la información a hora de enviarla al centro de datos
*Corrupción de la información para dañar el resto.

XII.MARCO LEGAL PERTINENTE AL CENTRO DE DATOS.

A. DELITOS INFORMÁTICOS.

a. Artículo 269A: Acceso abusivo a un sistema informático.

"El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes."(CONGRESO DE LA REPÚBLICA, 2009, ley 1273).

b. Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.

"El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96)

meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor." (CONGRESO DE LA REPÚBLICA, 2009, ley 1273).

c. Artículo 269C: Interceptación de datos informáticos.
"El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses." (CONGRESO DE LA REPÚBLICA, 2009, ley 1273).

d. Artículo 269D: Daño Informático.
"El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes." (CONGRESO DE LA REPÚBLICA, 2009, ley 1273).

B.LEY HABEAS DATA (LEY ESTATUTARIA 1266 DE 2008)

a. Derecho de la ley habeas data.

El derecho que promueve la ley habeas data es el de que toda persona tiene el derecho a conocer, modificar y validar la información que se halla recogido sobre ella en bancos de datos o información de naturaleza pública y privada.

La información recolectada es propiedad del titular y como titular se entiende como la persona jurídica o natural a quien se refiere la información recolectada, la relación de intercambio de datos reposa sobre un acuerdo comercias o de servicio donde el titular de la información debe o no aceptar el tratamiento licito de su información. (CONGRESO DE LA REPÚBLICA, 2008, ley 1266).

b. Artículo 7o. DEBERES DE LOS OPERADORES DE LOS BANCOS DE DATOS.

Sin perjuicio del cumplimiento de las demás disposiciones contenidas en la presente ley y otras que rijan su actividad, los operadores de los bancos de datos están obligados a:

1. Garantizar, en todo tiempo al titular de la información, el pleno y efectivo ejercicio del derecho de hábeas data y de petición, es decir, la posibilidad de conocer la información que sobre él exista o repose en el banco de datos, y solicitar la actualización o corrección de datos, todo lo cual se realizará por conducto de los mecanismos de consultas o reclamos, conforme lo previsto en la presente ley. (CONGRESO DE LA REPÚBLICA, 2008, ley 1266).

2. Garantizar, que, en la recolección, tratamiento y circulación de datos, se respetarán los demás derechos consagrados en la ley.

3. Permitir el acceso a la información únicamente a las personas que, de conformidad con lo previsto en esta ley, pueden tener acceso a ella.

4. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los titulares.

5. Solicitar la certificación a la fuente de la existencia de la autorización otorgada por el titular, cuando dicha autorización sea necesaria, conforme lo previsto en la presente ley.

6. Conservar con las debidas seguridades los registros almacenados para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento.

7. Realizar periódica y oportunamente la actualización y rectificación de los datos, cada vez que le reporten novedades las fuentes, en los términos de la presente ley.

8. Tramitar las peticiones, consultas y los reclamos formulados por los titulares de la información, en los términos señalados en la presente ley.

9. Indicar en el respectivo registro individual que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma y no haya finalizado dicho trámite, en la forma en que se regula en la presente ley.

10. Circular la información a los usuarios dentro de los parámetros de la presente ley.

11. Cumplir las instrucciones y requerimientos que la autoridad de vigilancia imparta en relación con el cumplimiento de la presente ley.

12. Los demás que se deriven de la Constitución o de la presente ley. (CONGRESO DE LA REPÚBLICA, 2008, ley 1266).

c. ARTÍCULO 8o. DEBERES DE LAS FUENTES DE LA INFORMACIÓN.

Las fuentes de la información deberán cumplir las siguientes obligaciones, sin perjuicio del cumplimiento de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

1. Garantizar que la información que se suministre a los operadores de los bancos de datos o a los usuarios sea veraz, completa, exacta, actualizada y comprobable.

2. Reportar, de forma periódica y oportuna al operador, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

3. Rectificar la información cuando sea incorrecta e informar lo pertinente a los operadores.

4. Diseñar e implementar mecanismos eficaces para reportar oportunamente la información al operador.

5. Solicitar, cuando sea del caso, y conservar copia o evidencia de la respectiva autorización otorgada por los titulares de la información, y asegurarse de no suministrar a los operadores ningún dato cuyo suministro no esté previamente autorizado, cuando dicha autorización sea necesaria, de conformidad con lo previsto en la presente ley.

6. Certificar, semestralmente al operador, que la información suministrada cuenta con la autorización de conformidad con lo previsto en la presente ley.

7. Resolver los reclamos y peticiones del titular en la forma en que se regula en la presente ley.

8. Informar al operador que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma, con el fin de que el operador incluya en el banco de datos una mención en ese sentido hasta que se haya finalizado dicho trámite.

9. Cumplir con las instrucciones que imparta la autoridad de control en relación con el cumplimiento de la presente ley.

10. Los demás que se deriven de la Constitución o de la presente ley. (CONGRESO DE LA REPÚBLICA, 2008, ley 1266).

C.LEY 1581 DE 2012 (Por la cual se dictan disposiciones generales para la protección de datos personales.)
dictan disposiciones generales para la protección de datos personales.

a. ARTÍCULO 4o. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES.

En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

a) Principio de legalidad en materia de Tratamiento de datos: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrolle.

b) Principio de finalidad:
El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

c) Principio de libertad:
El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

d) Principio de veracidad o calidad:
La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

e) Principio de transparencia:
En el Tratamiento debe garantizarse el derecho del Titular a obtener del responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan;

f) Principio de acceso y circulación restringida:
El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;

g) Principio de seguridad:
La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

h) Principio de confidencialidad:

Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma. (CONGRESO DE LA REPÚBLICA, *2012*).

XIII.REDIRECCIÓN DE PUERTOS

La redirección de puertos en la informática se concibe como una técnica basada en el encapsulamiento de protocolos de red sobre otros protocolos de red para crear un canal de comunicación.

Para la construcción de esta conexión entre equipos se debe implementar al centro de datos una unidad de datos de protocolo con el objetivo de que transmita desde un lado del túnel hasta el otro extremo sin una interpretación adicional de la unidad de datos de protocolo encapsulado, si se implementa de esta manera los paquetes si envían sobre nodos intermedios qué tienen una restricción sobre la visión del contenido encapsulado en estos paquetes

La conexión qué edad definida por los extremos del canal de comunicación y el protocolo asignado para este, un protocolo podría ser el protocolo SSH qué determina el acceso desde un punto remoto a un servidor otra vez de un canal seguro en el cual toda la información que se transporta por él está cifrada, además este protocolo permite duplicar y respaldar los datos de forma segura y generar contraseñas RSA.

Para el redireccionamiento de puertos existen 3 tipos que son:

A. Redirección local de puertos.

La redirección local de puertos consiste en que el canal de comunicación o la conexión del equipo local a una máquina con características remotas qué tiene un puerto determinado con el protocolo SHH pueda crear un canal o túnel local con la opción o el comando "-L".

B. Redirección remota de puertos.

La redirección remota de puentes establece un puerto de recepción para que redireccione una solicitud operación concreta, al crear un túnel de redirección remota se abre un puerto en el servidor con el protocolo SSH y luego este puerto apunta a la dirección concreta qué se quiere llegar.

C. Redirección dinámica de puertos.

La redirección dinámica del puerto establece un canal de comunicación dinámico que transforma el protocolo del servidor SSH en un servidor de proxy SOCKS, El cual es un protocolo que se usa generalmente para programas qué soliciten una conexión a la red de internet por medio de un servidor proxy, partiendo de este hecho cualquier programa puede utilizar este puerto y enlazar cualquier tipo de conexión de una manera segura sin exponerse a vulnerabilidades pon medio del servidor SSH.

Su principal característica es que cuando se establece el canal de comunicación en el puerto del servidor proxy este no lo redirecciona a una ruta específica, por el contrario, el puerto verifica el estado del servidor SSH y direccionará a una dirección que el cliente solicita.

XIV. CERTIFICADOS DIGITALES

Se propone que para el centro de datos se implementen certificados digitales generados por la administración del centro de datos que asocie a una persona con datos que lo identifiquen dentro del sistema, este certificado valida legítimamente a la persona que quiere entrar al sistema.

Los certificados digitales son eficientes para autenticar a un usuario en una página web o sistema.

XVI.BASES DE DATOS RELACIONALES VS NO RELACIONALES

A. Base de datos relacional

Una base de datos relacional es un contenedor de información y datos que tienen relaciones predefinidas entre ellos.

La información de la base de datos relacional estar organizada de en un conjunto de registros, tablas y columnas, las tablas son generalmente usadas para guardar la información de los objetos modelados del mundo, cada columna de la base de datos representa un conjunto de valores relacionados de una entidad.

Una ventaja de la base de datos relacional es que se puede acceder a la información de varias maneras y sin tener algún orden especifico en las tablas de la base de datos.

a. Motores de las bases de datos relacionales.

a. Oracle (Enterprise edition)
b. Microsoft SQL server (Enterprise edition)
c. MySQL
d. PostgreSQL
e. MariaDB

b. Base de datos no relacional

Las bases de datos no relacionales son aquellas en las que su diseño está orientado a modelos de datos específicos para la creación de aplicaciones modernas, este tipo de bases implementa una gran cantidad de modelos para el

manejo de datos que incluye elementos como gráficos, Clave-Valor y búsqueda.

El centro de datos manejara sistemas de bases de datos relacionales y no relacionales, dependiendo de los objetivos, alcance e información requerida por cada proyecto y que tienen una relevancia en cuanto a modularidad, escalabilidad y rendimiento.
A continuación, se presentan algunas diferencias entre estos modelos.

SQL:
*Se propone usar cuando el volumen de datos no crece o lo hace poco a poco.
*Cuando las necesidades de proceso se pueden asumir en un solo servidor.
*Cuando no tenemos picos de uso del sistema por parte de los usuarios más allá de los previstos.
NoSQL:
*Cuando el volumen de los datos crece de manera rápida y en momentos puntuales.
*Cuando las necesidades de proceso no se pueden preveer.
*Cuando se tienen picos de uso del sistema por parte de los usuarios en múltiples ocasiones.

XVI.PROTOCOLOS SUGERIDOS PARA FORTALECER EL CENTRO DE DATOS.

A. Protocolo de usuario

El protocolo de usuarios que se sugiere es un protocolo que gestione la creación , disponibilidad de usuarios y bajas de usuarios del centro de datos dadas las políticas que defina el administrador del centro de datos , para ello se deberá llevar un estricto control de tiempos, verificación e identificación de usuarios del centro de datos , además se deberá tener un procedimiento acertado para dar de baja a un usuario del centro de datos sin afectar la información que este allá alojado en la memoria central o sus aportes a otros documentos.

B. Protocolo de historial de cambios

Se propone tener un protocolo de historial de cambios que permita tener un seguimiento de los cambios en la información, procesos y demás servicios del centro de datos llevando el detalle exacto de que se modificó, quien lo modifico, cuando lo modifico y a qué hora, esto con el fin de tener evidencias y tener por decirlo así un respaldo de la información que se modifica en el centro de datos.

C. Protocolo de atención a incidentes

Se propone que el centro de datos tenga un protocolo de atención a incidentes en donde se detalle de manera precisa el procedimiento a llevar en caso de emergencia ya sea física o lógica en el centro de datos.

XII.HISTORIAS DE USUARIO SOBRE CENTROS DE DATOS ORIENTADOS A LA EDUCACIÓN E INVESTIGACIÓN EN COLOMBIA.

A. Proyecto RENATA

La red nacional académica de tecnología avanzada tiene un centro de datos con el propósito de albergar datos sobre temas de investigación y educación en Colombia, este proyecto se articulas los sectores educativos, científicos, productivo y el estado.
Este proyecto tiene una infraestructura donde es posible la articulación de proyectos colaborativos de ciencia, educación, innovación usando herramientas y técnicas de telepresencia, procesamiento de información entre otros beneficios,

a. Objetivo Social

El objetivo principal del proyecto RENATA es promover el desarrollo de la infraestructura y servicios de red de alta velocidad, además de vincular y apropiar el desarrollo de proyectos educativos, innovación.

b. Visión

El proyecto RENATA para el año 2018 será el principal aliado estratégico del SNCTI como una herramienta de transformación del país.

C. Papel central del proyecto RENATA.

Renata se ha venido establecimiento en el ambiente de la innovación y la investigación como un aliado del gobierno de Colombia para la apropiación de la tecnología que gradualmente ayuda a la productividad y desarrollo científico en Colombia.

c. Características Específicas de la red RENATA.

*100 Gbps de capacidad en el anillo nacional, con posibilidad de crecer a 80 lambdas (cada una de 100 Gbps).
*27 nodos de conexión, en las principales ciudades del país.
*Network Operation Center (NOC) exclusivo para atender las necesidades del SNCTI.
*Mesa de ayuda para acompañar los procesos de apropiación de las herramientas tecnológicas por parte de la comunidad académica y científica del país.
* Posibilidad de interconectar las múltiples sedes de una misma institución sobre la infraestructura de la red.
* Internet pública dedicada con capacidades de entre 30 Mbps y 500 Mbps, capacidades incluidas dentro del costo de la afiliación.

REFERENCIAS

[1] *B. analytics, "Características y tipos de bases de datos", Ibm.com, 2014. [Online]. Available: https://www.ibm.com/developerworks/ssa/data/library/tipos*

_bases_de_datos/index.html. [Accessed: 19- Sep- 2019]

[2] S. Alestra, "5 Básicos del Data Center", Blog.alestra.com.mx, 2015. [Online]. Available: http://blog.alestra.com.mx/5-b%C3%A1sicos-del-data-center. [Accessed: 19- Sep- 2019].

[3] G. Pacio, Data Centers Hoy, 1st ed. Buenos Aires: Damián Fernández, 2014, pp. 3,1.

[4] M. Guilarte and M. Guilarte, "¿Qué es un Tier?", MuyComputerPRO, 2019. [Online]. Available: https://www.muycomputerpro.com/2013/03/14/que-es-un-tier. [Accessed: 20- Sep- 2019].

[5] "¿Qué son los niveles del centro de datos? - Definiciones de TI empresarial", Hpe.com, 2019. [Online]. Available: https://www.hpe.com/es/es/what-is/data-center-tiers.html. [Accessed: 20- Sep- 2019].

[6] "Seguridad en Data Center - Medidas de seguridad en un centro de datos", MAD 3 DATA CENTER, 2018. [Online]. Available: https://www.madrid-interxion.com/medidas-de-seguridad-de-un-data-center/. [Accessed: 20- Sep- 2019].

[7] Seguridad y Administración del DATA CENTER, 1st ed. Argentina: Cucaier, pp. 24-30.

[8] Sistema de Gestión de Seguridad de la Información (SGSI), 1st ed. Organización Internacional de Normalización, 2019, pp. 1-10.

[9] "Seguridad de la información", Es.wikipedia.org, 2019. [Online]. Available: https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#Gobierno_de_la_Seguridad_de_la_Informaci%C3%B3n. [Accessed: 25- Sep- 2019].

[10] De la protección de la información y de los datos, vol. 47223. Bogotá, D. C.: Congreso de la república colombiana, 2009.

[11] "Secure Shell", Es.wikipedia.org, 2019. [Online]. Available: https://es.wikipedia.org/wiki/Secure_Shell. [Accessed: 26- Sep- 2019].

[12] "Redirección de puertos", Es.wikipedia.org, 2019. [Online]. Available: https://es.wikipedia.org/wiki/Redirecci%C3%B3n_de_puertos#Redirecci%C3%B3n_local_de_puertos. [Accessed: 26- Sep- 2019].

[13] "Red privada virtual", Es.wikipedia.org, 2019. [Online]. Available: https://es.wikipedia.org/wiki/Red_privada_virtual#Caracter%C3%ADsticas_b%C3%A1sicas_de_la_seguridad. [Accessed: 26- Sep- 2019].

[14] "Bases de datos SQL | AWS", Amazon Web Services, Inc., 2019. [Online]. Available: https://aws.amazon.com/es/relational-database/. [Accessed: 27- Sep- 2019].

[15] "Bases de datos no relacionales | Bases de datos de gráficos | AWS", Amazon Web Services, Inc., 2019. [Online]. Available: https://aws.amazon.com/es/nosql/. [Accessed: 27- Sep- 2019].

[16] "Replicación (informática)", Es.wikipedia.org, 2019. [Online]. Available: https://es.wikipedia.org/wiki/Replicaci%C3%B3n_(inform%C3%A1tica). [Accessed: 27- Sep- 2019].

[17] "maestro-esclavo | Real Academia de Ingeniería", Diccionario.raing.es, 2019. [Online]. Available: http://diccionario.raing.es/es/lema/maestro-esclavo. [Accessed: 27- Sep- 2019].

[18] "Usuario (Informática) - EcuRed", Ecured.cu, 2019. [Online]. Available: https://www.ecured.cu/Usuario_(Inform%C3%A1tica)#Cuentas_de_usuarios. [Accessed: 27- Sep- 2019].

[19] "info@citel", Oas.org, 2006. [Online]. Available: http://www.oas.org/en/citel/infocitel/2006/junio/seguridad_e.asp. [Accessed: 01- Oct- 2019].

[20] "Origen de RENATA - Red RENATA", Red RENATA, 2018. [Online]. Available: https://www.renata.edu.co/origen-de-renata/. [Accessed: 01- Oct- 2019].

[21] "¿Qué es Renata?:: matematicaspizarro", Matematicaspizarro.webnode.com.co, 2016. [Online]. Available: https://matematicaspizarro.webnode.com.co/products/%c2%bfque-es-renata/. [Accessed: 01- Oct- 2019].

[22] A. Molano, "Renata: Infraestructura e innovación para la academia", Corporación Colombia Digital|, 2017. [Online]. Available: https://colombiadigital.net/actualidad/articulos-informativos/item/9447-renata-infraestructura-e-innovacion-para-la-academia.html. [Accessed: 01- Oct- 2019].

[23] LEY ESTATUTARIA 1266 DE 2008, vol. 1-8. Bogotá, D. C.: CONGRESO DE LA REPÚBLICA COLOMBIANA, 2008.

[24] P. Servicios and H. dominios, "TIER y disponibilidad en Centros de Datos - Proyecto Albedo", Proyecto Albedo, 2018. [Online]. Available: https://proyectoalbedo.com/tier-disponibilidad-centro-datos/. [Accessed: 24- Oct- 2019].

[25] "La importancia del mantenimiento preventivo para data center", Dcd.media, 2017. [Online]. Available: https://www.dcd.media/noticias/la-importancia-del-mantenimiento-preventivo-para-data-center/. [Accessed: 24- Oct- 2019].

[26] "▷ ¿Qué es la Autenticación Biométrica? Los 5 Tipos - Estr@tegia Magazine", Estr@tegia Magazine, 2018. [Online]. Available: https://www.estrategiamagazine.com/tecnologia/los-controles-biometricos-verificacion-de-voz-escritura-huellas-patrones-oculares-retina-iris-geometria-de-la-mano/. [Accessed: 24- Oct- 2019].

[27] "Prevención y herramientas de seguridad contra hackers", Solvetic, 2013. [Online]. Available: https://www.solvetic.com/tutoriales/article/251-prevenci%C3%B3n-y-herramientas-de-seguridad-contra-hackers/. [Accessed: 24- Oct- 2019].

[28] "TIA-568B", Es.wikipedia.org, 2019. [Online]. Available: https://es.wikipedia.org/wiki/TIA-568B#Objetivos. [Accessed: 24- Oct- 2019].

[29] U. S.L.U., "¿Como se realiza el proceso de certificación del cableado estructurado? España", Unitel - Soluciones e infraestructuras Tecnológicas. [Online]. Available: https://unitel-tc.com/certificacion-del-cableado-estructurado/. [Accessed: 24- Oct- 2019].

[30] EstrategiaMagazine, Tabla Comparativa de los diferentes métodos biométricos. 2019.

[31] PROTECCIÓN A LA PROPIEDAD INTELECTUAL, Colombia: constitución colombia, 1991.

[32] LEY NÚMERO 23 DE 1982. REPÚBLICA DE COLOMBIA - GOBIERNO NACIONAL: CONGRESO DE LA REPÚBLICA, 1982.

[33] PROTECCIÓN A LA PROPIEDAD INTELECTUAL, vol. 61. Colombia: constitución colombia, 1991.

[34] [4] C. Roberto, "Certificados digitales, para qué sirven y cómo obtenerlos", Blog de Lenovo, 2015. [En línea]. Disponible: https://www.bloglenovo.es/certificados-digitales-para-que-sirven-y-como-obtenerlos/. [Acceso: 25- oct- 2019].

[35] "Biblioguias: Gestión de datos de investigación: Anonimización de los datos", Biblioguias.cepal.org, 2019. [Online]. Available: https://biblioguias.cepal.org/c.php?g=495473&p=4961125. [Accessed: 30- Oct- 2019].

[36] LEY ESTATUTARIA 1581 DE 2012. República de Colombia: secretariasenado, 2012.

[37] "Arreglo redundante de discos independientes (RAID)",

Web.mit.edu, 2003. [Online]. Available: http://web.mit.edu/rhel-doc/3/rhel-sag-es-3/ch-raid-intro.html. [Accessed: 14- Nov- 2019].

[38] "Intercambio electrónico de datos", Es.wikipedia.org, 2019. [Online]. Available: https://es.wikipedia.org/wiki/Intercambio_electr%C3%B3nico_de_datos. [Accessed: 14- Nov- 2019].

[39] J. LÓPEZ, "Cómo configurar un sistema RAID 1 para duplicar tus datos", PCActual.com, 2014. [Online]. Available: https://www.pcactual.com/noticias/trucos/como-configurar-sistema-raid-para-duplicar-datos-2_8443. [Accessed: 14- Nov- 2019].

[40] "protocolo ftp", Neo.lcc.uma.es. [Online]. Available: http://neo.lcc.uma.es/evirtual/cdd/tutorial/aplicacion/ftp.html. [Accessed: 14- Nov- 2019].

[41] M. Guilarte, "¿Qué es un Tier?", MuyComputerPRO, 2013. [En línea]. Disponible: https://www.muycomputerpro.com/2013/03/14/que-es-un-tier. [Acceso: 14- nov.2019].

[42] e. instrumentos, "Captura de datos - Definición y más información | ecom instruments", Ecom-ex.com, 2018. [En línea]. Disponible: https://www.ecom-ex.com/es/seguridad-intrinseca/glosario/termino/captura-de-datos/. [Acceso: 14- nov.2019].

[43] I. Instituciones, "¿QUE ES GESTIÓN DE LA INFORMACIÓN?", Instituciones.sld.cu, 2017. [En línea]. Disponible en: https://instituciones.sld.cu/toximed/2017/04/16/que-es-gestion-de-la-informacion/. [Acceso: 14- nov.2019].

REFERENCIAS DE IMAGENES

[44] Alfaomega, incidentes más comunes que generan fallas en el servicio mayor a 12 horas. 2014.

[45] M. Guilarte, Tier Clasification tier 1-tier IV. 2013.

[46] Mersen Ep, Data Center.

[47] Organización Internacional de Normalización, Niveles de un SGSI. 2019.

[48] Organización Internacional de Normalización, Flujo de gestión de un SGSI. 2019.

[49] Universidad Internacional Iberoamericana, CIBERSEGURIDAD: LAS PÉRDIDAS QUE GENERAN LOS ATAQUES INFORMÁTICOS. 2017.

[50] Fercuter, Una función de hash en funcionamiento. 2011.

[51] Estrategia Magazine, Tabla Comparativa de los diferentes métodos biométricos. 2018.

[52] Y. Rendon, ¿Entonces cuándo utilizar SQL o NOSQL? 2019.

[53]]S. Araya, RAID Nivel 1. 2012.

[54] Desarrollador Mozilla, Generalidades del protocolo HTTP. .