ALIANZAEFI
economía formal e inclusiva

Consideraciones en seguridad informática para la implementación de un centro de datos de uso en proyectos de investigación

Jefferson Arias Gómez
Javier Ríos
Johnn Eduard Criollo
Julián Peñuela

Documentos Alianza EFI
Marzo 2021
Número de serie: D7-2021-001

COLOMBIA CIENTÍFICA
Conocimiento Global para el Desarrollo

Consideraciones en seguridad informática para la implementación de un centro de datos de uso en proyectos de investigación.

Proyecto 7. Laboratorio social

Corporación Universitaria Minuto de Dios

***Abstract*—**

The following written document presents a technical report and / or security article on the data center of project No.7 of the Productive and Social Inclusion program: programs and policies for the promotion of a formal economy which will serve as a scoring document In Colciencias, in addition to giving an overview of the security that must be in a data center from the moment of construction and initial planning, giving a basis for future constructions, either from the project or from external agents *.

Resumen—

El siguiente documento escrito presenta un informe técnico y/o artículo de seguridad sobre el centro de datos del proyecto No.7 de el programa Inclusión productiva y social: programas y políticas para la promoción de una economía formal, además de dar un panorama general de la seguridad que se debe tener en un centro de datos desde su momento de construcción y planeación inicial, uno de los énfasis del presente documento es una mirada a los conceptos de seguridad informática y seguridad de la información que implica el desarrollo del proyecto actual.

I. INTRODUCCIÓN

En el siguiente documento se expone un artículo técnico sobre la seguridad del centro de datos desde el momento de su diseño e implementación física y digital, 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 artículo científico relacionado con el 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.

Este informe técnico hace referencia a la definición de un margo general acerca de la seguridad del centro de datos del proyecto No.7, en este documento se pretende establecer los aspectos que se deberían considerar teniendo en cuenta estándares y metodologías de seguridad informática en la construcción de un centro de datos.

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.

La estrategia de protección de la información cubre los componentes tecnológicos utilizados para el envío, entrega, almacenamiento y procesamiento de información de terceros con fines de investigación. Esto involucra los procesos y políticas asociadas al manejo de la información como el levantamiento de requerimientos técnicas para tal fin.

III. DESCRIPCIÓN TÉCNICA

El centro de datos será el encargado de almacenar y procesar la información referente a los diferentes frentes del proyecto Colombia científica; cómo componente principal del centro de datos, actualmente está el laboratorio de computación avanzada ó HPC, este laboratorio será el encargado de suplir las necesidades de almacenamiento y procesamiento masivo. Por otra parte, para necesidades de almacenamiento y cómputo no intensivo, se propone un conjunto de servidores y repositorios de almacenamiento que podrán estar on-premise o en la nube, según las necesidades que surjan durante el desarrollo de cada frente del proyecto.

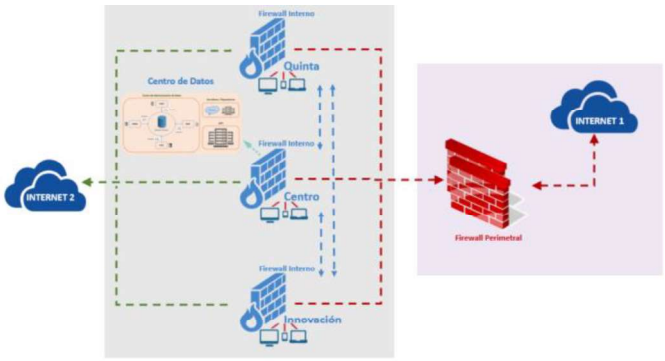

Figura 1.Arquitectura preliminar del centro de datos.fuente de información propia.

III.I. Arquitectura del centro de datos.

El centro de datos de Colombia Científica se encuentra protegido,inicialmente por dos firewalls locales de cada máquina, un firewall interno que es la puerta de entrada al centro de datos, que se encuentra localizado en la sede centro de la universidad y un firewall perimetral. El centro de datos consta de la infraestructura actual de QUE y los servidores requeridos para cada frente del proyecto. Los servidores se encuentran localizados físicamente en las instalaciones del centro de datos o pueden estar instalados en alguno de los proveedores de nube según el estudio de viabilidad y necesidad de cada proyecto.

Para ello el centro de datos contará con una arquitectura HPC (High performance Computing) esta arquitectura cuenta con una la agregación de potencia de cálculo para resolver problemas complejos en ciencia, ingeniería o gestión, en este caso teniendo en cuenta el contexto del centro de datos de Colombia Científica todos estos recursos estarían orientados al procesamiento y cálculos entre la información recopilada por medio de la investigación, Para lograr este objetivo, la computación de alto rendimiento se apoya en tecnologías computacionales como los clusters, los supercomputadores o la computación paralela.

El cluster HPC que se encuentra almacenado en el Colegio Mayor de Nuestra Señora del Rosario cuenta con las siguientes características para brindar aspectos de seguridad y calidad:

- ❏ 1 nodo de acceso DellEMC PowerEdge R630
- ❏ 7 nodos de cómputo para procesamiento CPU DellEMC PowerEdge FC430
- ❏ 1 nodo de cómputo DellEMC PowerEdge C con 4 tarjetas gráficas NVIDIA TESLA P100
- ❏ 1 sistema de almacenamiento SAS DellEMC Strage SCv2020 de 12Gbps con una capacidad de 36 TB.
- ❏ 1 switch Mellanox para conectividad de alto desempeño de 56 Gbps.

Dentro de los aspectos mencionados anteriormente notamos cierta relevancia en que el cluster HPC cuenta con 36 tb para almacenamiento exclusivo para el clúster, de los cuales 25 TB son efectivos. Parte del almacenamiento del clúster HPC es compartido entre sus diferentes nodos utilizando el protocolo NFS v3. Esto implica que todos los archivos que se generen en estos directorios son vistos por todos los nodos del sistema.

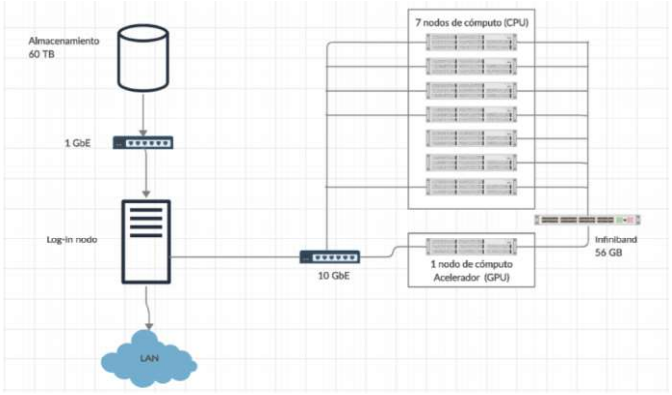

Figura 2.Arquitectura del cluster HPC. Fuente de generación propia

El centro de datos estará manejado por la dirección de Tecnología de la Universidad del Rosario, esta dirección cuenta con una oficina de Seguridad Informática. Y en lo relacionado a la Seguridad de la Información, se cuenta con el oficial de seguridad de la Información y protección de datos personales que depende de la dirección de planeación y efectividad institucional.

III. II.Comunicación

La interconexión entre los nodos de cómputo y el nodo de acceso es a través de una red Infiniband FDR de 56 Gbps. Por esta misma red de 56 Gbps se comparte el almacenamiento adicional al directorio $HOME entre todos los nodos del sistema, esto es, los directorio /data<xxx>.

Por otra parte, los usuarios utilizan para acceder al sistema y realizar la transferencia de sus archivos a una red Ethernet de 1Gbps. Por esta misma red de 1Gbps también es compartido el directorio $HOME de los diferentes usuarios entre todos los nodos.

IV. SEGURIDAD

La estrategia de protección de la información sugerida en el presente artículo, cubre los componentes tecnológicos utilizados para el envío, entrega, almacenamiento y procesamiento de información de terceros con fines de investigación. Esto involucra los procesos y políticas asociadas al manejo seguro de la información . El Centro de datos de Colombia Científica tiene como objetivo principal determinar y seleccionar las estrategias apropiadas de seguridad de la información para proteger y garantizar la confidencialidad, integridad y disponibilidad de la misma; implementar medidas para anular cualquier impacto de compromiso sobre el uso y manejo de información confidencial (datos sensibles) y desarrollar mecanismos de acceso a la información de forma segura que son descritos en seguida.

Es importante recalcar que la información individual estará salvaguardada de su mal uso por parte de cualquier agente mediante la validación de usuario y permisos para ellos, además de un registro de cambios e historial de versionamiento para poder un control total del cambio de información y demás características de esta . Para asegurar lo anterior el centro de datos planea administrar de manera eficiente herramientas de hardware y software necesarias para proteger la información sensible, previamente ante cualquier uso, estas herramientas pueden ser validaciones de usuarios por medio de contraseñas de sesión y claves cifradas para poder ingresar a la información, para evitar el acceso a la parte física las herramientas a usar son elementos de detección biométrica o elementos digitales como paneles con contraseñas entre otras para restringir el acceso .

Seguridad física del CPD:

Un centro de datos en su parte física está condicionado por una serie de computadores y otros dispositivos de hardware tales como servidores, routers, sistemas de almacenamiento además sistemas de comunicaciones los cuales se explicaran más adelante. Este tipo de contenedor de datos almacena gran cantidad de datos, posee sistemas de respaldo de energía, para evitar 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 para asegurar el funcionamiento y confiabilidad del centro de datos, estos elementos o procesos son la disponibilidad y su tiempo fuera de línea, los casos de emergencia y los procesos de mantenimiento de forma offline u online.

Teniendo en cuenta la normatividad TIER (*TIA 942*) para centros de datos, son parámetros recomendables a cumplir en un centro de procesamiento de datos los siguientes:

	Tier I	Tier II	Tier III	Tier IV
Building Type	Tenant	Tenant	Stand-alone	Stand-alone
Staffing	None	1 Shift	1 + Shifts	"24 by Forever"
Useable for Critical Load	100% N	100% N	90% N	90% N
Initial Gross Watts per Square Foot (W/ft²) (typical)	20-30	40-50	40-60	50-80
Ultimate Gross W/ft² (typical)	20-30	40-50	100-150[1,2,3]	150+[1,2]
Uninterruptible Cooling	None	None	Maybe	Yes
Support Space to Raised-Floor Ratio	20%	30%	80-90%[2]	100+%
Raised-Floor Height (typical)	12"	18"	30-36"[2]	30-36"[2]
Floor Loading lbs/ft² (typical)	85	100	150	150
Utility Voltage (typical)	208, 480	208, 480	12-15 kV[2]	12-15 kV[2]
Single Points-of Failure	Many + human error	Many + human error	Some + human error	None + human error
Annual Site-Caused IT Downtime (actuals)	28.8 hours	22.0 hours	1.6 hours	0.4 hours
Site Availability	99.671%	99.749%	99.982%	99.995%
Months to Implement	3	3-6	15-20	15-20
Year First Deployed	1965	1970	1985	1995
Construction Cost (±30%)[1,2,3]				
Raised Floor	$220/ft²	$220/ft²	$220/ft²	$220/ft²
Useable UPS Output	$10,000/kW	$11,000/kW	$20,000/kW	$22,000/kW

Figura 3. fuente TIA 942

Correspondiente a esto el proyecto contempla los siguientes elementos:

- El Centro de datos de la Alianza EFI tiene contemplado realizar planes de mantenimiento al centro de datos periódicos 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.

- Cuenta con dos UPS, una que soporta todo piso donde está el datacenter y otra es dedicada totalmente al CPD..
- Dispone de un sistema de control de incendios para combatir el fuego en caso de una emergencia y evitar la pérdida de información a causa de este.
- Contempla un sistemas eléctrico diferencial dado que es conveniente que los CPD cuenten con dos acometidas de potencia diferentes en cada Rack, ya que los servidores cuentan con fuentes de alimentación redundadas, para evitar que un fallo en una fuente deje al servidor sin energía, si se llegara a quemar una regleta no se interrumpiría el servicio .
- Incorpora un cableado de alta prestaciones para atender el tráfico SAN por medio un sistema de almacenamiento DellEMC Storage SCv2020 SAS, además Los cables de datos serán tipo Ethernet o fibra óptica y estarán separados de los cables eléctricos, para evitar interferencias..
- Cuenta actualmente con una topología de y un sistema de almacenamiento con discos espejos y RAID 10 en caso de fallos.
- La infraestructura del CPD está instalada 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.
- Para la protección física de los equipos el CPD cuenta con un sistema de polo a tierra y mecanismos de dispersión de sobra cargas eléctricas basado en polo a tierra.
- La manipulación de equipos del CPD para tareas de mantenimiento y/o monitoreo se realizarán de forma remotas dado a que la mayoría de actividades son remotas, aún se tiene en consideración la manera de realizar estas actividades se sugiere el uso de una VPN para suplir esta necesidad.Solamente reemplazos de partes defectuosas se hacen presencial, además se establecen políticas para el retiro de equipos, y conexión de pendrives, entre otros al interior del CPD, los tiempos de permanencia y las ventanas de mantenimiento están plenamente establecidas en un mapa de proceso de gestión del CPD.
- Para garantizar las estrategias de redundancia y recuperación de data se el CPD contempla 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.
- Según explicó Eduardo Rocha, Presidente Internacional de ICREA.

"Se pueden realizar las mejores prácticas desde el punto de vista de elección y gestión de los recursos TI, pero si el personal no está capacitado ni es seleccionado mediante un riguroso proceso, el Datacenter puede estar en graves riesgos en materia de seguridad. Hablamos de errores humanos, omisiones, robos de información, y demás escenarios que hacen vulnerables a los Centros de Datos"

También se explica que el 95% de los errores en un centro de datos son de carácter humano y parte técnica por ello Eduardo Rocha, Presidente Internacional de ICREA propone :

"Una buena operación debe establecer los procedimientos y tiene que mantener al día los recursos como la gestión de la energía eléctrica, la gobernabilidad o el clima".

- El Centro de datos de la Alianza EFI tiene contemplado realizar planes de mantenimiento al centro de datos, se sugiere que este mantenimiento sea una vez por

bimestre a lo largo del tiempo de trabajo del centro de datos, 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.

- El centro de datos tendrá instalado hardware de control electrónico especializado para la seguridad biométrica debido a, ya que esto ayuda a la identificación de las personas y/o visitantes para controlar su acceso, se debe además tener un modelo de seguridad multinivel, esto hace referencia a tener una la asociación no literal de caja fuerte dentro de otra caja fuerte ya que reduce los riesgos de intrusión física y digital de la información.

Según la norma ISO/IEC 17799:2005 y las buenas prácticas de seguridad ISO 27001, NIST Cybersecurity Framework y CIS Controls se considera algunas politica de seguridad informática en el proyecto en cuanto a:

- Seguridad de la red (*Asegurar la protección de la información en redes y la protección de la infraestructura de soporte*): de estas se incorporan las siguientes:
    - Cualquier conexión de red debe realizarse de forma segura para preservar los principios de confidencialidad, integridad y disponibilidad de la información.
    - Se deberá contar con sistemas de alertas de fallas de seguridad en la infraestructura de red para realizar las correcciones de manera eficaz.
    - Realizar pruebas de vulnerabilidades y Pentesting a la red de la entidad para verificar posibles fallas que puedan generar accesos no autorizados.

.Protección de los elementos básicos de seguridad o informáticos (Hardware):

Los elementos de hardware son un componente esencial del centro de datos debido a su importancia y sus funciones además de ser uno de los elementos más costosos del centro de datos por ellos es muy importante velar por su seguridad física, usualmente el equipo de hardware se puede enfrentar a tres problemas principales que son:

- ***Desastres de carácter natural***

  Los desastres naturales son cosas que pueden pasar si previo aviso y por ello el equipo de cómputo debe estar listo para una catástrofe de estas, debido a que puede tener consecuencias irremediables y generar pérdida de información y dinero ya que son activos importantes del CDP, los principales desastres que podrían presentarse son terremotos, inundaciones, incendios y tormentas eléctricas.

  Por ello se deben concebir medidas que garanticen que el equipo no tendrá calidad en caso de vibraciones, evitar que objetos ajenos se coloquen sobre los sistemas, utilizar fijaciones, tener un respaldo de la información entre otras opciones.

Modificaciones o alteraciones en el entorno

Por último debemos considerar los cambios en el entorno del equipo de cómputo que pueda dañarlo como lo es la electricidad ya que el circuito que alimenta al servidor del centro de datos y sus demás componentes podría tener un accidente debido a esto por ello lo recomendable es instalar reguladores tensión para solucionar los picos de voltajes que se puedan producir

También podemos las temperaturas extremas como un problema principal que afectaría el equipo físico, usualmente se creería que lo que afecta es el calor extremo pero el frío también, para ello se debe regular la temperatura del equipo físico puede ser por medio de aparatos de aire acondicionado.

- ***Acceso físico sin autorización***

Para garantizar la seguridad del acceso físico debemos tener contemplados todos los posible escenarios donde se viole la privacidad y así tener el sistema contra cualquier amenaza para poder prevenir estos incidentes hay elementos de verificación biométricas que entran en el campo denominado elementos tecnológicos de control de acceso

Sistema de control de acceso

Para el centro de datos es esencial mantener al máximo los niveles de seguridad para ello se sugiere tener sistemas de control de acceso, un sistema de control de acceso es un sistema que se encarga de permitir o denegar el acceso de algún usuario del centro de datos a un espacio o sector.

Para poder validar si el usuario puede o no acceder a un elemento del CPD existen diferentes tipos de identificación para el regular el acceso al centro de datos y su información estos son:

- ❏ Escáneres de retina
- ❏ Detector de huellas
- ❏ Circuito de cámaras de vigilancia
- ❏ Tarjetas inteligentes (Zonas de acceso)
- ❏ Paneles numéricos
- ❏ Tags de verificación

Tipos de control de acceso

existen dos tipos de control de acceso, estos son primordiales y sugiere tener en consideración para el centro de datos y su estructura de planeación, estos tipos son:

- ***Sistemas de control de acceso autónomos.***

  Este tipo de control de acceso nos habla de sistemas que controlan de manera autónoma uno o más puntos de acceso del centro de datos sin estar conectados a un equipo de cómputo lo cual nos da la desventaja que es no tener registros de eventos.

  Dentro de estos métodos entran las claves, los sensores de proximidad y los elementos de biometría como los que se mencionaron anteriormente, básicamente estos elementos de verificación de acceso funcionan como una llave electrónica.

  Aunque esta es la principal limitante, algunos controles de acceso autónomos tampoco pueden limitar el acceso por horarios o por grupos de puertas, esto depende de la robustez de la marca. Es decir, los más sencillos solo usan el método de identificación (ya sea clave, proximidad o biometría) como una "llave" electrónica.

- ***Sistemas de acceso en red.*** A diferencia de los sistemas autónomos estos se integran a un equipo de cómputo ya sea de manera local o remota, esto permite que se haga un control de acceso con un historial de eventos y todas las características asociadas a él .

Técnicas de control de acceso

Dentro de las técnicas de control de acceso encontramos como tanto seguridad física para proteger las instalaciones físicas del CPD como también existen métodos de control lógicos que sirven para resguardar la información confidencial de accesos no autorizados.

Algunas de estas técnicas son:

- ***Identificación y autenticación.*** Esta técnica consiste en identificar al usuario cuando intenta acceder al sistema y posteriormente autentificar sus privilegios y así tomar la decisión de dejarlo pasar o no.

- ***Password Seguras.***
  Tener una contraseña segura es una técnica de autenticación eficaz debido a que puede ser tan compleja como la lógica de negocio lo quiera .

- ***Definición de roles.***
  Definir roles permite que el acceso a la información se pueda manejar por restricciones de roles dentro del sistema, En este caso los derechos de acceso y política de seguridad asociada pueden agruparse de acuerdo con el rol de los usuarios.

- ***Limitaciones de servicios.***
  Esta técnica se refiere a las restricciones que el administrador del CPD del centro de datos destine para cada tipo de usuario del sistema.

- ***Modalidad de acceso.***
  Se refiere a la manera de la cual accede un usuario al sistema estos tipos de acceso son :

    - Lectura
    - Escritura
    - Ejecución
    - Creación
    - Búsqueda

- ***Ubicación y establecimiento de horarios***
  El acceso a ciertos elementos del sistema también se puede restringir por la ubicación o horarios de trabajo ligados a los usuarios, logrando así controlar el tráfico de usuarios dentro del sistema.

Figura 4. jerarquía de usuarios en una base de datos

El centro de datos de Colombia Científica ya tiene definidos ciertos aspectos en cuanto a los mecanismos de autenticación de usuarios y control de acceso para los mismos, esto con el fin de proteger de manera eficaz el centro de datos y su integridad tanto física como lógica, estos son:.

Mecanismos de autenticación de usuarios:

- Se contempla un mecanismo de autenticación en el acceso a través de SSH, es de clave pública se basa en los pares de claves pública/privada.
- Se contemplan mecanismos de autenticación de acceso por VPN con usuario de directorio activo. Con acceso a los servidores con claves pública/privada.

Mecanismos de control de acceso
El equipo técnico del CPD definió para el control de acceso los siguientes elementos debido a su pertinencia en la lógica de negocio e intenciones de seguridad que se aplicaran al mismo.

- Huella digital + Tarjeta.

Para acceder físicamente al CPD, inicialmente se necesita autorización previa para ser registrado en el sistema de acceso. Posteriormente se necesita huella digital y tarjeta.

USUARIOS DEL CPD

El centro de datos al ser un sistema de información y un recurso informático para el proyecto de Colombia Científica cuenta con con ciertos tipos de usuarios, los cuales serán los que consuman los servicios que provee pero también se tendrán usuarios de mantenimiento, control y administración del mismo, para ello vamos a recurrir al ciertas definiciones sobre usuarios que se encuentran en el Anexo número uno de este artículo el cual se llama "_ Cartilla No.1 Conceptos básicos en centro de datos. ", estas definiciones son:

Un usuario se define técnicamente como el objeto que interactúa dentro del sistema.

Los usuarios en un sentido más general 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. 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 usuario y un password 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 se encarga de crear usuarios en el centro de datos y tiene el acceso a modificar ciertos aspectos y contenidos adicionales a los que un miembro no puede entrar.

D. Administradores: Son usuarios 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.

E. Usuarios en la base de datos. Según Natalia de la Peña Calvo (2019) en una base de datos podemos encontrar tres tipos de usuarios estos son administradores, programadores y analistas y por último usuarios finales, anteriormente explicamos las funciones del administrador, a continuación se mencionan los faltantes.

También una función muy importante es la definición de los perfiles de los usuarios usando la restricción de accesos a ciertas vistas del usuario.

Programadores y analistas de sistemas

Son los usuarios que codifican las aplicaciones del centro de datos o su adaptación dentro del CPD, dentro de sus funciones principales están documentar y mantener las aplicaciones y servicios además de determinar los requerimientos de los usuarios del mismo.

Usuario final

Estos usuarios son los que finalmente usarán el CPD y almacenarán, consultaron y descargar información, todo lo mencionado anteriormente dependerá de las restricciones que se le asignen, debido a que los usuarios del centro de datos tendrán tantas vistas como usuarios existan

Para las tareas de autenticación de usuarios el centro de datos verificará 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.

Gestión de acceso de usuarios

Los usuarios son usuarios de tipo Linux que se replican a lo largo de todos los servidores e infraestructura.

Se tendrá un usuario con el derecho a crear, borrar y modificar objetos además puede conceder privilegios a otros usuarios sobre los objetos que ha creado, en contraparte también tendremos un usuario con derecho a consultar, o actualizar, y sin derecho a crear o borrar objetos teniendo ciertos privilegios sobre los objetos, añadir nuevos campos, indexar,alterar la estructura de los objetos creado por el usuario mayor.

Se tendrá un mecanismo de autenticación en el acceso a través de SSH, es de clave pública se basa en los pares de claves pública/privada.

Se tendrá un mecanismo de autenticación de acceso por VPN con usuario de directorio activo. Con acceso a los servidores con claves pública/privada.

Responsabilidades de los usuarios

- Las credenciales de ingreso son de uso personal e intransferibles.
- Hacer un buen uso de la infraestructura de acuerdo al reglamento de usuarios.
- Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal. Dicha normativa puede consistir en normas, procedimientos, reglas y estándares, así como posibles guías.
- Conocer las consecuencias que se pudieran derivar y las responsabilidades en que pudiera incurrir en caso de incumplimiento de la normativa, que podrían derivar en sanciones.
- Evitar transmitir o comunicar datos considerados sensibles por medios poco fiables sin protección (telefonía de voz, correo electrónico, fax)

Control de acceso a sistemas y aplicaciones

El centro de datos contará con un control de acceso basado en roles (RBAC) este sistema de verificación se usará como un mecanismo de acceso neutral para que los usuarios tengan restringidos ciertos datos o sectores de la base de datos o la información .

Con RBAC se administrarán los privilegios de los usuarios dentro del sistema, se manejara la definición de roles dentro del sistema por medio de un jerarquía donde cada usuario tendrá acceso a diferentes vistas y se tendrán tantas vistas como roles en el sistema.

CONTROLES CRIPTOGRÁFICOS

- Se usará el control PKI para la autenticación de usuarios, debido a que PKI proporciona una infraestructura que permite un proceso de verificación de identidad por medio de certificados digitales como el cifrado y la firma electrónica, como resultado de estos procesos encontramos que pki es confiable dado a que garantiza el cifrado, autenticación y la integridad de la información a la hora de realizar una operación.
- Se sugiere la implementación de kerberos, kerberos es un sistema de autentificación de usuarios que tiene como objetivo impedir el acceso a las claves que se envían por medio de una res y además la autentificación de usuarios.

  Kerberos aplica criptografía de claves simétricas para poder cifrar y descifrar se usa la misma clave que para autentificar usuarios.

- Se sugiere usar el estándar X509 sobre los certificados ya que permite convertirlos a otros tipos, además de generar firmas de peticiones de firma sobre él y editar sus opciones de confianza o aceptabilidad.

Al usar la librería de SSL openSSL podemos encontrar recursos relacionados con X509 estos recursos son los certificados X509, Certificate Signing Request o CSR (petición de firma de certificado). Esto está definido como un objeto PKCS#10 y Certificate Revocation List o CRL

Teniendo en cuenta los lineamientos de seguridad que se deben tener para asegurar la integridad de la información se sugiere algunas políticas de seguridad :

Algunas de las políticas de seguridad de la información debe incluir las siguientes:

***Oportunidades y Riesgos*—**La amplia variedad de nuevos recursos, servicios e interconectividad disponibles a través de la Internet plantean nuevas oportunidades de negocio, así como nuevos riesgos en materia de seguridad y privacidad. La política oficial del C.P.D aquí descrita en relación con la seguridad en Internet y la forma de acceso de los usuarios, es una respuesta a estos riesgos.

***Confiabilidad de la Información*—**Toda la información adquirida de Internet debe considerarse no confiable hasta que se confirme con información proveniente de otra fuente. Antes de emplear información suministrada gratuitamente por Internet para la toma de decisiones del CPD, los trabajadores deben corroborar la información consultando otras fuentes.

***Verificación Anti Virus*—**Todos los archivos no texto descargados de Internet y provenientes de fuentes que no pertenecen al CDP, deben ser examinados con software antivirus antes de usarlos. Cuando el proveedor externo del software no es confiable, el software descargado debe probarse en una máquina independiente, no empleada para la producción, que haya sido respaldada recientemente. Los archivos descargados deben descifrarse y descomprimirse antes de ser sometidos a la verificación antivirus. Es recomendable el uso de firmas digitales para verificar.

***Confirmación de Identidad*—**Antes de que los trabajadores revelen cualquier información interna del CPD, celebren contratos o hagan pedidos de productos a través de redes públicas, debe confirmarse la identidad de las personas y las organizaciones contactadas. Lo ideal es hacerlo mediante firmas o certificados digitales; sin embargo, cuando éstos no estén disponibles, pueden emplearse cartas de crédito, referencias de terceros y conversaciones telefónicas.

***Anonimato del usuario*—**Queda prohibido falsear, ocultar o sustituir la identidad de un usuario en Internet o en cualquier sistema de comunicaciones electrónicas de CPD. El nombre del usuario, la dirección de correo electrónico, la afiliación a la organización y otros detalles incluidos en los mensajes o transcripciones deben señalar al verdadero autor de los mismos. Si los usuarios tienen necesidad de emplear redespachadores de correo y otras facilidades anónimas, deben hacerlo en su tiempo libre, con sus propios sistemas informáticos y cuentas de proveedores de servicio de Internet. Se permite el uso de conexiones anónimas FTP, UUCP, HTTP o exploración de la web y otros métodos de acceso establecidos donde se supone que los usuarios son anónimos.

***Archivos anexos al correo electrónico*—**Los usuarios del CPD deben abstenerse de abrir los archivos adjuntos a su correo electrónico salvo que provengan de un remitente confiable. Cuando los trabajadores reciban archivos adjuntos de remitentes conocidos y confiables, deben usar un paquete antivirus antes de abrirlos.

***Cambios a páginas web*—**Los usuarios del CPD no deben establecer nuevas páginas de Internet o realizar modificaciones en las páginas existentes

relacionadas con el CPD, a menos que obtengan una autorización del Administrador del centro de datos. Los cambios incluyen añadir enlaces a otros sitios, actualizar la información presentada y alterar la diagramación de una página. Este comité debe garantizar que todo el material publicado tenga una apariencia coherente e impecable, esté alineado con los objetivos empresariales y esté protegido con medidas adecuadas de seguridad.

***Archivos de Páginas Web*—**Cada versión del sitio de Internet y del sitio de comercio del CPD debe resguardarse en dos ubicaciones físicamente separadas. El comité gerencial de Internet designará un administrador web para guardar este respaldo y suministrar copias de las páginas históricas a solicitud.

***Interceptación de Mensajes*—**La información secreta, privada o propiedad del CPD no debe enviarse por Internet, a menos que haya sido cifrada con métodos autorizados. Salvo que se sepa que es del dominio público, el código fuente siempre debe cifrarse antes de enviarlo por Internet. Por las mismas razones

***Divulgación de Información Interna*—**Los trabajadores no deben divulgar públicamente información interna del CPD a través de la Internet que pueda afectar negativamente el precio de las acciones, las relaciones con los clientes o la imagen pública del CPD, a menos que hayan obtenido la autorización del director de Relaciones Públicas o de un integrante del equipo de alta gerencia. Esta información abarca las posibilidades de negocio, los productos que están en investigación y desarrollo, los análisis de rendimiento de los productos, las fechas de lanzamiento de los mismos y problemas internos de los sistemas de información. Quedan eximidas de esta política las respuestas a mensajes de correo electrónico de un cliente específico..

***Autentificación de Usuario Entrante*—**Todos los usuarios que deseen establecer una conexión en tiempo real con los computadores internos del CPD a través de la Internet deben emplear un producto de red privada virtual (VPN, por sus siglas en inglés) autorizado por el departamento de Seguridad Informática el cual puede cifrar todo el tráfico que se intercambia. Estos productos VPN también deben autentificar usuarios remotos en un cortafuego antes de permitirles el acceso a la red interna del CPD. Este proceso de autentificación debe completarse mediante un sistema de contraseña dinámica autorizado por el gerente corporativo de Seguridad Informática. Algunos ejemplos de tecnología autorizada incluyen tarjetas inteligentes portátiles con contraseñas dinámicas y sistemas de requerimiento y respuesta que sean transparentes para el usuario. Los sistemas públicos designados no requieren de procesos de autentificación de usuario porque se supone que las interacciones son anónimas.

***Seguridad Remota del Equipo*—**Los trabajadores que no hayan instalado las mejoras o los parches requeridos al software o cuyos sistemas estén infectados por virus deben desconectarse automáticamente de la red de la del CPD hasta que se restablezca un ambiente seguro de computación. Los computadores usados por todos los trabajadores que empleen tecnología VPN deben ser rastreados remotamente en forma automática para determinar si el software está actualizado y si el sistema ha sido protegido adecuadamente.

***Restricción de Acceso de Terceros*—**No deben otorgarse privilegios entrantes de acceso a la Internet a terceros, incluyendo proveedores, contratistas, consultores, personal temporal o personal de organizaciones externas u otros terceros a menos que el gerente del sistema en cuestión determine que estos individuos tienen una necesidad justificada de negocios para dicho acceso. Estos privilegios deben habilitarse únicamente para ciertos individuos y sólo por el periodo de tiempo requerido para completar las tareas autorizadas.

***Autentificación de Usuario de Explorador*—**Los trabajadores no deben guardar contraseñas fijas en sus exploradores web o en sus clientes de correo electrónico. Estas contraseñas fijas deben ser suministradas cada vez que se invoca un explorador o un cliente de correo electrónico. Las contraseñas

de explorador pueden ser guardadas cuando debe suministrarse una contraseña de arranque cada vez que se enciende el computador y cuando se solicita una contraseña de protector de pantalla cada vez que el sistema permanece inactivo por un periodo específico de tiempo. Los usuarios de los computadores del CPD deben rechazar todos los ofrecimientos del software de colocar cookies en su computador para que puedan conectarse en forma automática la próxima vez que visiten un sitio particular de la Internet. Los cookies que sirven para otros propósitos están permitidos.

***Agrupadores de Datos*—**Los trabajadores no deben suministrar sus identificadores de usuario de la Internet y las contraseñas a agrupadores de datos, a servicios de resumen de datos y de formato ni a ningún otro tercero.

Seguridad lógica del CPD

Para determinar qué elementos o protocolos se aplicarán al centro de datos es necesario definir todos los escenarios que se puedan provocar en el proceso de almacenar la información, por ello su aseguramiento depende del tipo de información que se recibirá .
Podemos recibir dos tipos de data que son :

- Data no estructurada
- Data estructurada

Data estructurada.

La data estructurada dentro del centro de datos del proyecto Colombia Científica puede llegar por medio de la conexión remota a bases de datos de terceros como por ejemplo DANE, SISPRO, ICFES (consultas directas a la base de datos) entre otras que se acuerden a lo largo del tiempo de vida del proyecto, además de la entrega y respuesta de información por medio de archivos planos por ejemplo CVS, TXT entre otros.

Data no estructurada

La data no estructurada se contempla como la recepción de información por medio de archivos con diferentes formatos, estos documentos pueden ser resultado del trabajo con algún software o el resultados de encuestas.

También se contempla un escenario donde se almacena la información que resulta como producto del procesamiento de la información .

Teniendo en cuenta lo anterior se consideró los aspectos necesarios para asegurar la información sin importar su origen por ello se contempló ciertas normas para el aseguramiento de la información

Para el aseguramiento de la información estructurada se pensaron la aseguración definiendo estrategias orientadas para la asignación y revocamiento de permisos según los roles y las necesidades del centro de datos, estos aspectos mencionados anteriormente son 8:

- .Creación y protección de vistas según usuarios.
- Enmascaramiento de la información sensible.
- Uso de una VPD (Virtual private database).
- Creación de funciones para manejar de manera interna la información.
- Definiciones de roles y usuarios para el acceso discriminatorio al sistema.
- Se encriptará la data para que solo se pueda acceder a ella por medio de llaves.
- Creación de puntos de acceso únicos dentro de la red.

Para el aseguramiento de la data no estructurada se contemplan tres procesos a tener en cuenta debido a la naturaleza de obtención de la información, esta información es:

- Encriptación de los archivos para prevenir su acceso desde fuentes externas.
- Definiciones de roles y usuarios para el acceso discriminatorio al sistema.
- Creación de políticas y permisos a nivel de usuario para mantener controladas las operación con la información.

El CPD para la gestion y analisis de riesgos implemente la metodología institucional basada en la ANZ 4360 y la ISO 31000,

La ANZ 4360 hace referencia a un estándar el cual provee una guía completa de los procesos para la administración, identificación, evaluación, tratamiento y comunicación de riesgos que puedan surgir a lo largo del contexto del trabajo del CPD.

Por otro lado la ISO 31000 especifica y define una serie de buenas prácticas para una gestión eficiente de la gestión de riesgos sin importar el nivel, esta ISO es más amigable a la hora de implementarse a nivel operativo, de gobierno y para generar confianza en las partes interesadas.

A nivel de seguridad lógica el CPD establece los siguientes bajo la norma ISO/IEC 17799:2005 a nivel de políticas de seguridad informática en el proyecto en cuanto a:

- ***Seguridad en SGBD***

  .La seguridad en un SGBD es tal vez el pilar más importante de todo el proyecto debido a que en él se almacenarán los resultados de cada una de las investigaciones o datos de los demás proyectos para ello el SGBD cuenta con los siguientes aspectos de seguridad lógica:

  - Los mecanismos de protección son simples, uniformes y están construidos en las capas más básicas del sistema.
  - Por defecto se restringirá el acceso a usuarios que no se identifiquen.
  - Se crearán según convenga perfiles de usuarios y vistas, el sistema tendrá tantas vistas como usuarios tenga para finalmente crear restricciones de uso de vistas a los usuarios para que cada uno tenga acceso solo a la parte lógica del proyecto que le interesa y no modifique información ajena a menos que se lo permitan.
  - El sistema está diseñado de tal manera que prevé la destrucción, modificación, interceptación de información por medio de validación en cuanto a las acciones de los usuarios siendo estas super vistas, de modo tal que pueda descubrirse cualquier acción indebida o errónea.
  - El SGBD mantendrá la confidencialidad de los datos a través de la encriptación para los datos en reposo, pero también a los datos que, por un motivo u otro, se encuentren en tránsito.
  - Se tendrá una disponibilidad casi total de la información alojada en el SGB, solo se mantendrá inactiva en periodos de mantenimiento y optimización.

- Seguridad en aplicaciones.
  - Se definirán para las aplicaciones diseñadas para el centro de datos entornos de trabajos diferenciados para garantizar la calidad y el desarrollo cuando son consumidos por un usuario, además de estar en constante actualización en los estándares de seguridad de la misma .
  - Se tendrá de un plan en caso de que la aplicación falle, esto para garantizar el funcionamiento de la página cuando se produzca un fallo en la página y que solo falle el sector mas no en totalidad.
  - Para la seguridad declarativa y lógica se deben definir métodos de autenticación, una definición de

usuario y los roles de los mismos, por último restringir el acceso a los recursos dependiendo la lógica del proyecto en el que se encuentren

- Seguridad en sistemas operativos
    - El registro del directorio activo deberá registrar los logs de los accesos exitosos y fallidos de inicio de sesión.
    - No se debe transmitir o almacenar contraseñas en texto claro.
    - Las contraseñas de acceso deben poseer un mínimo de ocho (8) caracteres y debe contener al menos una letra mayúscula, una letra minúscula, un número y un carácter especial. Estas deben ser cambiadas como mínimo cada mes.
    - Solamente los administradores de red podrán tener privilegios para la administración de los equipos de cómputo (instalación y desinstalación de software)
- Seguridad en mecanismos de acceso basado en contraseñas
    - Se hará uso de una infraestructura PKI (para gestión de claves de acceso para usuarios remotos, generación de credenciales etc,La autenticación usa PKI y se necesita llave para poder acceder por defecto con SSH.

      veamos

En cuanto a la norma ISO 27001:2013, se han considerado los siguientes controles para la confidencialidad, integridad y disponibilidad de la data en el CPD.

Pruebas de seguridad

El centro de datos al ser un sistema de información que contiene información sensible, puede ser vulnerable ante los ataques informáticos que podrían atentar no solo contra la información sino también a la integridad del centro de datos y su lógica de operación..

Por ello se propone aplicar diferentes técnicas de pentesting para la validación de vulnerabilidades y penetración del centro de datos, dentro de estas técnicas se proponen las siguiente pruebas:

Pentesting de seguridad en aplicaciones

Teniendo en cuenta que este tipo de prueba es la más completa se propone que se realice una valoración de toda la estructura de red del centro de datos, suponiendo que se detecte una anomalía para poder proceder a realizar la gestión de hackeo ético, esto con el fin de detectar que necesita ser re definido en el CPD.

Prueba de servicios de red:
Se propone esta técnica para evaluar la configuración del firewall y el filtrado de stateful .

Pruebas de aplicaciones
Esta técnica se propone para realizar de manera más exhaustiva una validación de la configuración de las aplicaciones para identificar puertos de operación, mecanismos de autenticación, vulnerabilidades a nivel de firmware, parches de actualizaciones y serialización de componentes funcionales;

Prueba del client side:
Esta técnica sugerida al CPD propone explorar el software del sistema además de las plataforma de creación de contenido y los sistemas que se ofertan para los usuarios del sistema, validando parámetros de seguridad para entrega remota de acceso a aplicaciones y servicios del CPD.

Prueba de la red inalámbrica
Se sugiere esta prueba debido a que se examinan

todas las redes que utiliza el CPD para asegurar el uso de mecanismos de encripción, seguridad a nivel de protocolos de red, puntos de acceso y credenciales de los administradores.

Pruebas de IPS/IDS

Se propone realizar un a realizar una prueba de IDS e IPS dado que al usar esta técnica el CPD podrá identificar de una mejor maneras como se procesan los paquetes el servidor, estas herramientas son fundamentales ya que protegen el perímetro de la red del CPD además ya que permite que los usuarios no deseados del centro de datos puedan entrar sin consentimiento al sistema.

Pruebas de WAF(Web Application Firewall)
Se propone revisar el WAF debido a que se debe garantizar la seguridad de las aplicaciones y/o servicios del CPD, la prueba del WAF consiste en poner a prueba la integridad de las aplicaciones que se ofrecen a los usuarios además de que la prueba añade al server ciertas reglas de un conjunto en los buses de datos por medio de HTTP para prevenir ataquede de criss.site scriptting e inyeccion de SQL.

Al implementar las pruebas mencionadas, el CPD puede considerar riesgos de compromisos en ciberseguridad para la data generada por los investigadores.

Dentro de otras ventajas se tiene que al realizar periódicamente las pruebas del sistema es posible la estimación de nuevas estrategias en cuanto a la seguridad de la información y garantizar el compromiso del CPD con los datos gestionados por los usuarios.

Las pruebas mencionadas, eventualmente, podrán prevenir amenazas al CPD que atenten a la integridad, confidencialidad y disponibilidad de los servicios, recursos y aplicaciones que el mismo ofrecerá, teniendo en cuenta la premisa anterior se mencionan las principales amenazas informáticas las cuales pueden afectar al CPD, estas amenazas son:

- Violacion de datos alojados en el CPD, sin importar su naturaleza es un peligro potencial ya que la información contenida al ser sensible puede causar grandes problemas si es publicada, vista o manipulada por personas ajenas al sistema.
- Las vulnerabilidades del CPD son errores que pueden ser producto de fallas en diseño, implementación o pruebas antes de salir a producción, a la hora de realizar los servicios que se ofertan, estas ventanas de fallos de seguridad son la oportunidad para que los atacantes informáticos alteren el servicio, corrompan el servicio o simplemente lo desconecten (DoS).
- También considerando que se tienen plataformas en línea se podría considerar al phishing como una amenaza ya que si el delincuente ingresa o consigue credenciales de los usuarios pertenecientes al CPD puede falsificar, robar y modificar la información para realizar con ellas un propósito solo conocido por el.
- Se debe considerar la opción de ejecución de malware que se puede alojar en el CPD, con los peligros derivados de robo de propiedad intelectual o datos de vital importancia, podemos hablar también que el malware podría saturar las comunicaciones del CPD e infectar otros sectores que puedan bloquear la red del mismo entre otros.

  Un riesgo latente es una amenaza de ransomware, su propósito es secuestrar datos informáticos y pedir una extorsión por la misma además de poder distribuirla y hacerla pública, esto en el CPD de Colombia Científica debe ser algo de vital cuidado ya que la información allí presente es de suma delicadeza.

- Se deben considerar los ataque DoS dado que su misión principal es evitar que el usuario pueda acceder a servicios del CPD o a sus datos.

Gestión de incidentes de la seguridad de la información

Para la gestión de incidentes de seguridad de la información el equipo de seguridad informática de la universidad del rosario supervisará las revisiones de seguridad de acuerdo a los estándares de la universidad.

Aspectos de seguridad:

Internamente el equipo del rosario realizará un análisis de vulnerabilidades anuales a todos los activos de TI. Complementando con análisis de vulnerabilidades a los nuevos activos que se despliegan a producción.

Además por medio con acompañamiento de un tercero, se realizará un ejercicio de pentesting (de caja gris) sobre los activos críticos donde los pentesters o analistas de seguridad pueden tener conocimiento sobre algunos aspectos del funcionamiento del sistema y de otros no.

Sobre el Uso de SLA´s

Ya que los programas que se adoptaran para el funcionamiento del CPD son externos y no de desarrollo propio, se sugiere establecer acuerdos de nivel de servicio que cubran los aspectos de:

- Respuesta a fallas
- Continuidad del servicio
- Actualización de software

La función principal de un SLA (Service Level Agreement) es establecer con el cliente indicadores para regular la prestación de servicios del sistema y así cumplir con las expectativas de uso; esto es extensible a los usuarios finales del CPD quienes están inmersos en el uso de los recursos del mismo, a continuación se sugieren SLA´s generales para el CDP:

Para garantizar el desarrollo y el mantenimiento y el sistema se sugiere usar un Service Level Agreement (SLA) que es un contrato donde se describe el servicio a desarrollar por un proveedor a un cliente a detalle asegurando la calidad del servicio y así de esa manera tener una constancia legal en caso de que el servicio inclumpla las normas.

A nivel de respuesta a fallas se debe establecer unos tiempos de servicio y atención a incidentes en algún de las categorías de un SLA de Servicio como son: 24×7 (24h los 7 días de la semana), 16×7 (16h los 7 días de la semana) ó 10×5 (10h de lunes a viernes) esto en negociación y acuerdo con el proveedor.

El nivel de respuesta a fallas es crítico para la continuidad y operación de los servicios que se espera implementar en el Centro de procesamiento de datos. Se debería considerar el nivel que se ha de otorgar a cada servicio estableciendo una distinción en alguno de estos tres niveles.

Se propone un SLA para la generación de informes donde se sugiere especificar entre otros parametros: *Reporte de casos del mes con los estados y tiempos de atención Indicadores de uso, solución de*

incidencias, peticiones, requerimientos y el cumplimiento oportuno de los compromisos; esto para garantizar el acuerdo de prestación de servicios para los usuarios y así como para llevar un registro y poder modificar el control de incidencias en el sistema, considerando lo anterior como un SLA basado la calidad del servicio.

A nivel de servicio técnico y soporte se debe programar las interrupciones del sistemas además de acordar con el área de gestión de servicios del Cliente, todo cambio sobre la plataforma o sobre el sistema de gestión deberá cumplir con los requisitos del procedimiento de Gestión de cambios establecidos por ambas partes, todo lo anterior para poder determinar así un SLA de .soporte del sistema entre las dos partes interesadas

Se considera crear un SLA con el usuario para acordar las responsabilidades del cliente, algunas de estas podrían ser la anonimización de la información que se subira al CPD, tambien se pueden considerar las responsabilidades dentro del sistema por ejemplo, el acuerdo de uso de la información que allí se aloja y el control de la misma, las políticas anteriores se pueden dejar en consideración dado que el admin del CPD deberá establecer las políticas tanto como de él como de los usuarios .

Se deberá definir un SLA que oferte una política que evite la duplicación entre varios acuerdo entre las partes interesadas del CDP

Por último se debe tener en cuenta un SLA donde se expliquen los elementos, usuarios y servicios que sean inmunes a los acuerdos pactados a su vez también se debería implementar un SLA para la atención de quejas, reclamos o sugerencias por parte de los usuarios o administradores del cpd y así tener un control de errores y calidad por parte de la experiencia del sistema.

Para poder diseñar un SLA es necesario garantizar que el CPD puede garantizar todos los acuerdos que se lleguen a pactar y a su vez ofrecer un buen catálogo de servicios de manera clara para así pactar con el cliente el acuerdo final.

Seguridad de las operaciones

- El CPD contempla una metodología Institucional basada en la ANZ 4360, ISO 31000, y complementada con Cobit 5 para suplir los riesgos.
- El CPD cuenta con ITIL (Biblioteca de infraestructura de tecnologías de información) para tener una buena

Cumplimiento

- ***Revisiones de seguridad el información***
  - A nivel de la Dirección de Tecnología de la Universidad Del Rosario, contamos con la oficina de Seguridad Informática. Y en lo relacionado a la Seguridad de la Información, se cuenta con el Oficial de Seguridad de la Información y Protección de datos personales que depende de la Dirección de Planeación y Efectividad Institucional.

ESTÁNDARES RELACIONADOS DE UN CENTRO DE DATOS.

Teniendo en cuenta que el CPD ya se encuentra en una fase de culminación física a lo largo de este artículo se mencionan a lo largo de este documento ciertas técnicas, que se deben tener en consideración para la implementación de un data center, por ello basándonos en la premisa anterior en la etapa de diseño de un CPS se evalúan ciertos estándares mínimos que debe cumplir o alcanzar a lo largo de su tiempo de vida, estos estándares satisfacen las necesidades de la lógica del proyecto de los usuarios del mismo por ello a continuación se nombran ciertos estándares los cuales el CPD debería cumplir:

A. Gestión Nivel de Servicio:
Se considera a la gestión de nivel de servicio como un proceso mediante el cual se definen y se determinan los servicios ofrecidos por el centro de datos en términos de TI. dentro de la gestión de servicios encontramos las siguientes subcomponentes que terminan de robustecer este documento.

La relevancia de la gestión de los servicios del CPD de Colombia Científica radica en el importancia de implementar alguno de los estándares para control y gestión de los servicios de IT con el fin de establecer herramientas de respaldo a los servicios principales ofrecidos a los usuarios a pesar de ocurrir situaciones anormales, teniendo en cuenta lo anterior la implementación de un estándar de calidad en los servicios satisface las necesidades de la lógica de negocio de Colombia Científica.

Para poder al gestión a nivel de servicio se deben tener en consideración los siguientes elementos:

- Definición de los servicios
- Oferta de los servicios
- Gestión de portafolio de servicios
- Gestión de reclamaciones y garantías
- Servicio de mantenimiento
- Facturación de servicios
- Gestión de clientes
- Documentación técnica
- Percepción del consumidor.

Los estándares asociados a gestión de nivel de servicio se agrupan en dos tipos

A. Organización de servicio

La organización de los servicios se encuentra definida a lo largo del marco contextual de la norma ISAE (3402) la cual define un estándar de aseguramiento internacional que permite a una empresa u organización la realización de un informe de seguridad y confidencialidad de la información para todos los usuarios de un sistema informático

.

Para saber más sobre esta norma y desarrollo consulte el siguiente enlace:

https://ingertec.com/compliance/isae-3402/

B. Gestión de Incidentes

El apartado de la gestión de incidentes se encuentra regido por la familia de estándares ISO/IEC 27035 la cual de manera general detalla un panorama de prácticas destinadas para generar controles de seguridad de la información teniendo en cuenta aspectos como la detección, corrección y creación de medidas preventivas ante cualquier evento inusual.

Para saber más sobre esta norma y desarrollo consulte el siguiente enlace: (https://www.iso.org/standard/60803.html)

B. Gestión de Seguridad:

La gestión de seguridad en el CPD es un estándar vital ya que la gestión de la seguridad nos permite la creación de políticas, controles y herramientas para proveer un control de calidad en las validaciones de seguridad dentro del sistema de información, la gestión de la seguridad se compone en dos elementos, estos elementos son: ***Protección de información:***

Dentro del marco contextual de la protección de la información se encuentran involucrados

varios estándares entre ellos el más conocido que destaca es la ISO 27000 y todo su contenido dado que esta norma contiene una serie de detalladas prácticas para garantizar la seguridad de la información dentro de un sistema de información .https://www.iso27000.es/

Además de la norma mencionada anteriormente podemos tener en cuenta también a la ISO 15408 la cual nos habla acerca de criterios de evaluación de las propiedades de seguridad de un sistema de la información, mencionadas las dos normas anteriores y al complementarse crean un esquema robusto que garantiza la seguridad de la información, las normas mencionadas anteriormente pueden ser accedidas desde los siguientes enlaces.

ISO 27000:

Para saber más sobre esta norma y desarrollo consulte el siguiente enlace: ***(ISO 15408):*** https://www.iso.org/standard/50341.html

Seguridad Física: Para saber más sobre esta norma y desarrollo consulte el siguiente enlace ***(ISO 18000):***

https://www.iso.org/standard/46149.html

C.Gestión de Proyectos

Para la definición de la gestión de proyectos se contempla la ISO 21500 dado que esta norma le proporciona a una organización herramientas y metodologías que orientan la gestión de proyectos importantes de la mejor manera además de definir un conjunto de operaciones para cumplir con el objetivo según la lógica del negocio.

Considerando lo anterior y al adaptarlo al CPD de Colombia Científica se puede crear un conjunto de metodologías para dirigir, controlar y evaluar los proyectos en curso o que se generen a partir de la información contenida en el mismo, el objetivo de la gestión de proyectos es alcanzar los objetivos preestablecidos de la organización y así beneficiarla a ella al llevar un control de este teniendo buenos resultados sin consecuencias además de aumentar la calidad en servicios y demás.

Para saber más sobre esta norma y desarrollo consulte el siguiente enlace ***(ISO 215000):*** https://www.iso.org/obp/ui#iso:std:iso:21500:ed-1:v1:es

D.Gestión de infraestructura

La gestión de la infraestructura en CPD está regido por diferentes normas y estándares como el TIA-EIA 942, ANSI - BICSI 002 o la ISO 24762, todas ellas proveen una guía de buenas prácticas a seguir para la instalación de los elementos de un centro de datos en su fase de diseño. A continuación .

Usualmente en la empresas u organizaciones grandes gastan grandes sumas de dinero en compras de elementos físicos y reparaciones, la gestión de la infraestructura implementada en un CPD en este caso en el de Colombia Científica, cra parámetros sobre las funciones de tecnologías de información que provee además de los edificios e instalación,

como objetivo final esta gestión provee un rendimiento integra en control de energía, equipo y el espacio, garantizando que se use todo de la manera más eficiente.

Para saber más sobre esta norma y desarrollo consulte el siguiente enlace **(TIA-EIA 942):** https://tiaonline.org/

Para saber más sobre esta norma y desarrollo consulte el siguiente enlace **(ANSI - BICSI 002):** https://www.bicsi.org/docs/default-source/publications/bicsi_002_esp_sample.pdf?sfvrsn=f4bce3b9_0

Para saber más sobre esta norma y desarrollo consulte el siguiente enlace **(ISO 24762):** https://www.iso.org/standard/41532.html

dentro del marco de la infraestructura encontramos enmarcados ciertos elementos físicos y lógicos que se deben tener en consideración con sus respectivas normas que los rigen:

- Red

  *https://iie.fing.edu.uy/ense/asign/ccu/material/docs/Cableado%20Estructurado.pdf
  *https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/N0041470

- Espacio y canalizaciones

  *https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=75

- Prevención de incendios

  *https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0057559

- Electricidad

  TIA 607
  *https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0057559

- Temperatura y humedad

  *http://www.areadata.com.ar/pdf/El%20standard%20TIA%20942%20-vds-11-4.pdf

- Racks
  *https://www.normadoc.com/spanish/eia-eca-310-e-2005.html

  *http://www.retex.es/Downloads/TECH_ENCLOSURES_EP_2009.pdf

E.Monitoreo y control de métricas.

El monitoreo y control de las métricas, servicios y productos de un CPD está regido por la norma ISO 9001 donde se establecen ciertos criterios para convertir el sistema en un SGGI de alta calidad para una empresa y así demostrar que se tiene toda la capacidad para satisfacer las necesidades del cliente, para validar todos los aspectos y apartados de esta norma se encuentra a continuación el enlace a la página oficial.

Para saber más sobre esta norma y desarrollo consulte el siguiente enlace **(ISO9001)**: https://www.normas-iso.com/iso-9001/

Al implementar un control y monitoreo de métricas al CPD de colombia Científica se crea un SGSI en el cual le garantiza a sus usuarios la seguridad de información, al asegurar esto se debe proveer un conjunto de normas para que los usuarios no expongan la seguridad de la información además de que se establecen métricas y criterios para evaluar la

seguridad de manera periódica y dar fe del buen uso y privacidad de la información.

F.Continuidad del negocio

Para los centros de datos la continuidad del negocio es algo vital ya que se debe contemplar a futuro el servicio que se ofrece y dema, la continuidad de negocio de define como procesos y procedimientos que una empresa u organización desarrollan para que los servicios que se ofertan puedan servir después de pasar por situaciones anormales,, la continuidad del centro de datos de Colombia científico es esencial ya que al pasar el tiempo de diseño del proyecto se deben seguir proveyendo los servicios a las personas ya que el alcalde del CPD y sus servicios se proyectan a lo largo de varios años, para garantizar esta continuidad podemos considerar los siguientes apartados, estos son:

a.Gestión de BCP

El componente BCP significa planificación del negocio y como su nombre lo indica se trata de la creación de estrategias antes situaciones anormales que afecten la integridad de un centro de datos y aun así superar y seguir ofertando servicios, este apartado está regido por la ISO 24762 y la NFPA 1600,Considerando lo anterior al implementar el componente BCP al CPD de Colombia Científico se procedería a crear estrategias de respaldo para cada caso de uso que falle en operación, todo esto para poder garantizar la continuidad de los que ofertan el centro de datos sin ocasionar pérdida o corrupción de la información además de prevenir ataques si se llegan a crear vulnerabilidades mediante la situacion anormal,a continuación podemos encontrar enlaces a las respectivas normas y así expandir a detalle toda la información de ellas.

Para saber más sobre esta norma y desarrollo consulte el siguientes enlaces : *https://tiaonline.org/

*https://www.iso.org/standard/41532.html

*https://www.nfpajla.org/archivos/edicion-impresa/manejo-de-emergencias-egreso/802-nfpa-1600-una-herramienta-importante-para-la-respuesta-y-recuperacion

b.Gestión de DR(disaster recovery)

Un plan de recuperación ante desastres es un modelo que provee procesos de recuperación de datos, hardware y software de un centro de datos, para que la lógica de negocio y sus datos puedan a operar con total normalidad en dado caso que ocurra un evento inesperado, el plan de recuperación ante desastres está regido por la ISO 22301, ISO 27031, ISO 22399 y BS 2599, a continuación encontraremos enlaces a cada una de las normas para expandir los conceptos de cada una respectivamente.

G. Gobierno de IT y Gestión administrativa.

El gobierno de las tecnologías de la información se encuentra regido por la norma ISO 28500 dado que este estándar provee principios para que una organización tenga una dirección, evaluación, y gestión con respecto al uso de las tecnologías de la información, para conocer más de la norma mencionada anteriormente en el siguiente enlace se expande de manera detallada.

*https://www.iso.org/standard/62816.html

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- Sdep- 2019]

[2] S. Alestra, "5 Básicos del DataCenter", 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: DamiánFernández, 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] "¿Cuáles 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.html14[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] ISO/IEC 2701:2013 mantenimiento de un SGSI

[10] "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].

[11] "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].

[12] "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].

[13] 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].

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

[15] 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].

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

[17] 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].

[18] ISO/IEC 17799:2005 Código para la práctica de la gestión de la seguridad de la información.

[19]"AWS | Computación de alto rendimiento (HPC)", Amazon Web Services, Inc.. [Online]. Available: https://aws.amazon.com/es/hpc/. [Accessed: 07- May- 2020].

[20]C. Brown, "Beyond Fault Tolerance: Data Center Active Fault Avoidance Strategies", Uptime Institute, 2017.

[21]"Clusters de servidores - Servidores T153 UTEQ", Sites.google.com. [Online]. Available: https://sites.google.com/site/servidores153uteq/clusters-de-servidores. [Accessed: 07- May- 2020].

[22]C. Empey, "Guía básica sobre VPN: Qué son y cómo funcionan", Blog.avast.com, 2018. [Online]. Available:https://blog.avast.com/es/guia-basica-sobre-vpn-que-son-y-como-funcionan. [Accessed: 07- May- 2020].

[23]"Fallas en el data center: 95% son causadas por errores humanos - CIOAL The Standard IT", CIOAL The Standard IT. [Online]. Available: http://thestandardcio.com/2015/03/25/data-center-95-son-causadas-por-errores-humanos/. [Accessed: 07- May- 2020].

[24]"Implementación de un servidor de archivos en clúster de dos nodos", Docs.microsoft.com, 2019. [Online]. Available: https://docs.microsoft.com/es-es/windows-server/failover-clustering/deploy-two-node-clustered-file-server. [Accessed: 07- May- 2020].

[25]"ISO 17799", ISO 17799, 2005. .

].

[26]H. Toutchkov, "¿Qué es una PKI o infraestructura de clave pública?", Oodrive - ES. [Online]. Available: https://www.oodrive.es/blog/security/que-es-una-pki-o-infraestructura-de-clave-publica/. [Accessed: 07- May- 2020].

[27]"Control de acceso basado en roles (descripción general) - Guía de administración del sistema: servicios de seguridad", Docs.oracle.com, 2011. [Online]. Available:

https://docs.oracle.com/cd/E24842_01/html/E23286/rbac-1.html. [Accessed: 07- May- 2020].

[28]D. Ferraiolo and R. Kuhn, "15ª Conferencia Nacional de Seguridad Informática (NCSC)", Baltimore, Maryland, Estados Unidos, 1992.

[29]EJ Coyne, TR Weil (2013), ABAC y RBAC: Gestión de acceso escalable, flexible y auditable, IEEE IT Professional (mayo / junio de 2013).

[30]DR Kuhn, EJ Coyne, TR Weil (2010), Agregar atributos al control de acceso basado en roles, computadora IEEE (junio de 2010).

[31]"Descripción del Kerberos un servicio de autenticación para los sistemas de red abierta", Cisco, 2006. [Online]. Available: https://www.cisco.com/c/es_mx/support/docs/securit

y-vpn/kerberos/16087-1.html. [Accessed: 07- May- 2020].

[32]"Kerberos - EcuRed", Ecured.cu. [Online]. Available: https://www.ecured.cu/Kerberos. [Accessed: 07- May- 2020].

[33]"Pentest: ¿qué es y cuáles son los principales tipos? - OSTEC Blog", OSTEC Blog. [Online]. Available: https://ostec.blog/es/seguridad-perimetral/pentest-concepto-tipos. [Accessed: 30- Aug- 2020].

[33]"¿Qué es un SLA? | Definición y tipos de SLA | ServiceTonic", ServiceTonic. [Online]. Available: https://www.servicetonic.com/es/service-desk/que-es-un-sla/. [Accessed: 07- May- 2020].

[33]J. Traver, "OpenSSL/X509 - ¿Para que sirve el X509?", Spi1.nisu.org. [Online]. Available: http://spi1.nisu.org/recop/al01/pepe/X509_paraque.html. [Accessed: 07- May- 2020].

[34]J. Villegas, "¿Qué es un Sistema de Control de Acceso?", Tecnoseguro.com. [Online]. Available: https://www.tecnoseguro.com/faqs/control-de-acceso/que-es-un-control-de-acceso#:~:text=Un%20sistema%20de%20control%20de%20acceso%20es%20un%20sistema%20electr%C3%B3nico,puerta%2C%20torniquete%20o%20talanquera)%20por. [Accessed: 09- Jul- 2020].

[35]"3.2 TÉCNICAS CONTROL DE ACCESO - wiki_seguridadinformatica", Sites.google.com. [Online]. Available: https://sites.google.com/site/wikiseguridadinformatica/3-seguridad-logica/3-2-tecnicas-control-de-acceso. [Accessed: 09- Jul- 2020].

[36]"Usuario (Informática) - EcuRed", Ecured.cu. [Online]. Available: https://www.ecured.cu/Usuario_(Inform%C3%A1tica)#Cuentas_de_usuarios. [Accessed: 06- Aug- 2020].

[37]N. Peña Calvo, UF1643, Gestión y control de los sistemas de información. [Málaga]: Nuevos Negocios en la Red, 2015.

[38]A. Astorquiza, Findeter.gov.co, 2013. [Online]. Available: https://www.findeter.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=211834. [Accessed: 27- Aug- 2020

[39]"Principales riesgos y amenazas de seguridad informática", Rittal - Datacenter - Edge Computing - IoT - Industrial 4.0, 2018. [Online]. Available: https://www.rittaltic.es/principales-riesgos-y-amenazas-seguridad-it/. [Accessed: 10- Sep- 2020].

[40]M. Rouse, "¿Qué es Gestión de la infraestructura de centros de datos, DCIM? - Definición en WhatIs.com", SearchDataCenter en Español. [Online]. Available: https://searchdatacenter.techtarget.com/es/definicion/Gestion-de-la-infraestructura-de-centro-de-datos-DCIM. [Accessed: 18- Sep- 2020].

[41]"Qué es la gestión de servicios", Gestion.org. [Online]. Available: https://www.gestion.org/que-es-la-gestion-de-servicios/. [Accessed: 17- Sep- 2020].

[42]"Qué es la gestión de servicios", Gestion.org. [Online]. Available: https://www.gestion.org/que-es-la-gestion-de-servicios/. [Accessed: 17- Sep- 2020].

[43]"Gestión de proyectos: ¿Qué es y qué metodologías son las más usadas?", TIC Portal, 2018. [Online]. Available: https://www.ticportal.es/glosario-tic/gestion-proyectos. [Accessed: 17- Sep- 2020].