Universidad de Costa Rica

Escuela de la Ciencias de la Computación y la Informática

II Semestre 2021

CI-0144 Diseño y Oper. de Servicios de Infraestructura

Prof. Ricardo Villalón F

Análisis de seguridad de los centros de datos

Stephanie Maria Leiton Ramírez B74106

Jorge Mario Trejos Barquero B77676

San Pedro, Montes de Oca

Tabla de contenidos

Resumen

En este documento se presenta un análisis de seguridad del servicio alrededor de la red social de los centros de datos.

Análisis de seguridad

1. Identificación

Personajes, equipos, sistemas, información o cualquier otro elemento del sistema para los cuales pudiera ser interesante hacer un análisis de seguridad. .

1. Hipervisor para el centro de datos: infraestructura de nube en la que están las máquinas del sistema.
2. Máquinas del centro de datos: futuras máquinas que se utilizan para que se realice el servicio.
3. Máquinas de gestión: es por donde se puede realizar la gestión a las máquinas de los centros de datos.
4. Comunicación entre las máquinas de un centro de datos: porque se quiere mantener la comunicación de forma segura.
5. Comunicación entre centros de datos: es importante que la comunicación entre ambos centros de datos sea de manera segura.
6. Comunicación gestión-centro de datos: para asegurar el ingreso a las máquinas del centro de datos para su gestión.
7. Comunicación usuario-centro de datos: se desea que la comunicación entre el usuario y el centro de datos sea de manera segura.
8. Servidor DNS: Servidor encargado de relacionar nombres y direcciones IP's, además de dar organización a las máquinas virtuales.
9. Servidor DHCP: Servidor encargado de proporcionar una configuración completa para conexión a internet a las nuevas máquinas virtuales que se crean.
10. FreeIPA: Servidor que provee un servicio de identidad, autenticación de usuarios y autenticación y autorización de recursos, para la gestión de una infraestructura de TI.
11. Servidor OSSN: Servidor que provee el servicio de la Red Social de Open Source Social Network.
12. Servidor de base de datos: base de datos que contiene la información de la Red Social.

Sistema a analizar: Mini centro de datos virtual

Árbol del todo y las partes del sistema

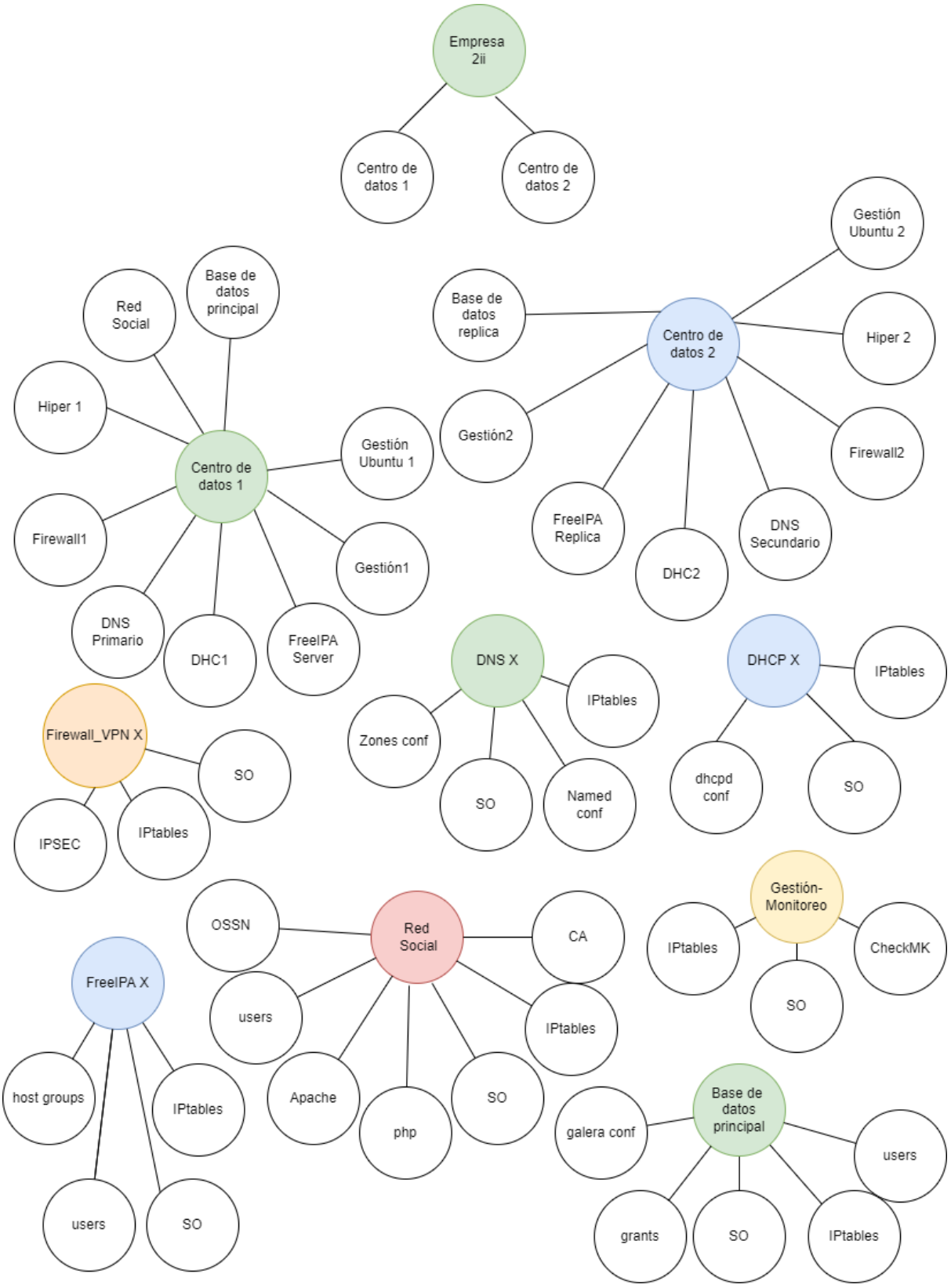

Imagen 1 Árbol del todo y las partes

En la imagen 1 se puede ver el árbol del todo y las partes de la infraestructura que se está realizando.

2. Objetivos de seguridad

Para alguno de los elementos identificados en el punto anterior, se establecen una lista de objetivos de seguridad que sirvan como referencia para el análisis.

1. Mantener la integridad de la información transmitida entre los centros de datos.
2. Requerir autenticación para asegurarse de que quien transmite la información entre centro de datos es de quien dice ser.
3. Mantener la confidencialidad de la información transmitida entre los dos centros de datos.
4. Mantener la integridad de la información transmitida entre el sistema de centro de datos y el usuario.
5. Mantener la confidencialidad de la información transmitida entre el sistema de centros de datos y el usuario.
6. Mantener la confidencialidad de la información transmitida entre las máquinas virtuales de un centro de datos.
7. Mantener la integridad del hipervisor y su información ante accidentes e intentos maliciosos de acceso.
8. Mantener la integridad de las máquinas virtuales ante accidentes e intentos maliciosos de acceso.
9. Requerir autenticación para el ingreso a la gestión de las máquinas un centro de datos.
10. Requerir autenticación para el ingreso a la máquina de gestión de un centro de datos.
11. Mantener confidenciales las IP's de las máquinas virtuales del servicio para los clientes.
12. Mantener un manejo responsable y autorizado de las direcciones IP asignadas a las máquinas virtuales del servicio.
13. Procurar mantener la disponibilidad del servicio en relación con las direcciones IP de las máquinas servicio.
14. Requerir autorización para identificar los usuarios al ingreso a los servicios básicos.
15. Mantener disponibilidad en el tráfico de red para gestionar los servicios básicos.
16. Mantener la integridad de la información transmitida entre las máquinas virtuales de un centro de datos.
17. Mantener la confidencialidad de la información entre la máquina de gestión interna y la máquina de gestión externa.
18. Mantener disponibilidad en el servicio de la Red Social.

3. Diagrama de interacción entre los componentes componentes

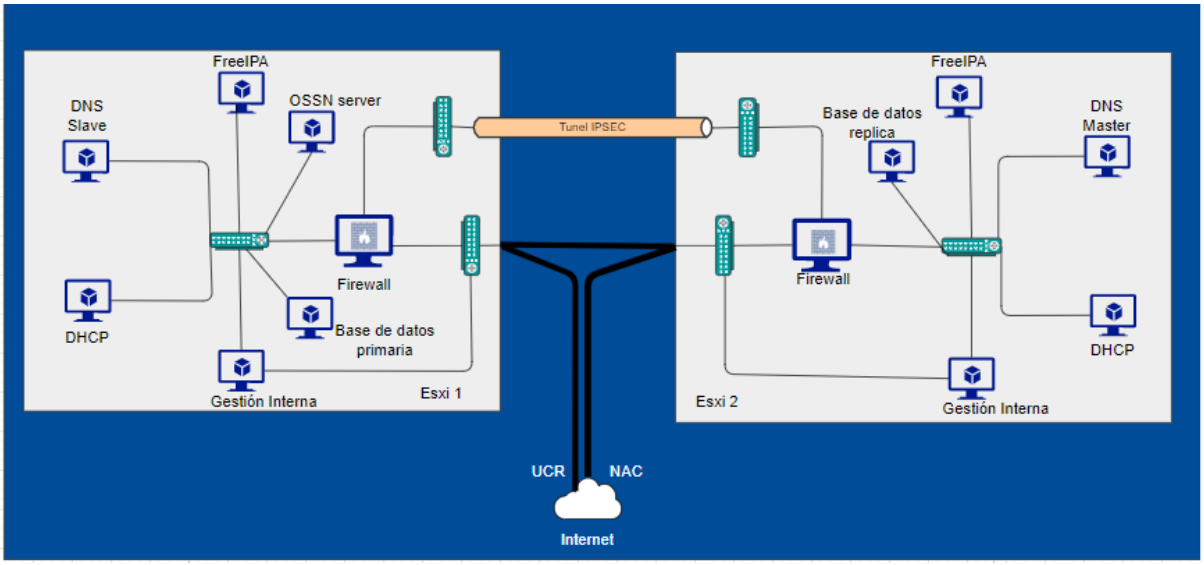

Imagen 2 Diagrama de interacción entre los componentes

Reglas de firewall

Estas son las reglas que restringen la interacción entre los centros de datos y el exterior.

1. Permite la comunicación entre los centros de datos mediante el IPsec para FreeIPA y DNS y las bases de datos de la red social.
2. Permite la salida la internet para todas las máquinas de la red interna.
3. Permite que DNS sea visible desde la red de la NAC.
4. Permite que la Red Social sea visible desde la NAC.
5. Prohíba el acceso para toda entrada externa que no esté especificada anteriormente.

4. Riesgos y evaluación preliminar

4.1. Riesgos

Con la información del punto anterior, se hace una identificación de riesgos de los elementos seleccionados y tomando como referencia los objetivos establecidos.

Objetivo 1: Mantener la integridad de la información transmitida entre los centros de datos.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Paquete de información	• Que el paquete pueda ser alterado o reemplazado	- Que alguien logre acceder al paquete	- Que alguien cambie información de un paquete Nivel de impacto: alto - Que alguien cambie el paquete por otro Nivel de impacto: alto

Objetivo 2: Requerir autenticación para asegurarse de que quien transmite la información entre centro de datos es de

quien dice ser.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Maquina fuente	● Quien envía el paquete no sea el esperado	- Que alguien logre falsificarse como la fuente de información	- Que se cambie el origen de información y el destino no se de cuenta Nivel de impacto: alto
Máquina destino	● Quien recibe el paquete no sea el esperado	- Que alguien logre falsificarse como la destino de información	- Que se cambie el destino de la información y se acepté la información Nivel de impacto: alto - Que se cambie el destino de la información y no se de cuenta de que recibió información no esperada Nivel de impacto: alto

Objetivo 3: Mantener la confidencialidad de la información transmitida entre los dos centros de datos.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Paquete de información	● Que el paquete sea de información legible durante la comunicación	- Que un tercero intercepte la información del paquete.	- Que alguien pueda leer e interpretar el contenido del paquete. Nivel de impacto: medio-alto

Objetivo 4: Mantener la integridad de la información transmitida entre el sistema de centro de datos y el usuario.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Paquete de información	● Que el paquete pueda ser alterado o reemplazado	- Que alguien logre acceder al paquete - Que se produzca una falla en la red	- Que un atacante pueda cambiar información de un paquete Nivel de impacto: alto - Que un atacante pueda cambiar el paquete por otro Nivel de impacto: alto - Que se cambie un paquete durante transmisión Nivel de impacto: alto

Objetivo 5: Mantener la confidencialidad de la información transmitida entre el sistema de centros de datos y el usuario.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Paquete de información	● Que el paquete sea de información legible durante la comunicación	- Que un tercero intercepte la información del paquete.	- Que alguien pueda leer e interpretar el contenido del paquete. Nivel de impacto: medio-alto

Objetivo 6: Mantener la confidencialidad de la información transmitida entre las máquinas virtuales de un centro de datos.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Paquete de información	● Que el paquete de información sea legible durante la comunicación	- Que un tercero intercepte la información del paquete.	- Que alguien pueda leer e interpretar el contenido del paquete. Nivel de impacto: medio-alto

Objetivo 7: Mantener la integridad del hipervisor y su información ante accidentes e intentos maliciosos de acceso.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Hipervisor	● Fallas en el ingreso al hipervisor	- Que alguien no autorizado ingrese al hipervisor	- Que alguien altere cualquier componente del sistema. Nivel de impacto: alto

Objetivo 8: Mantener la integridad de las máquinas virtuales ante accidentes e intentos maliciosos de acceso.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Sistema operativo	● Fallas en el ingreso a la MV	- Que un tercero ingrese a la MV	- Que alguien altere cualquier componente del sistema operativo. Nivel de impacto: medio-bajo
Servicios	● Débil configuración de seguridad de los servicios	- Que alguien acceda a información sensible la MV. - Que alguien logre acceder a la MV.	- Que alguien altere archivos de configuración del servicio. - Que alguien altere cualquier componente de la MV. Nivel de impacto: medio

Objetivo 9: Requerir autenticación para el ingreso a la gestión de las máquinas un centro de datos.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Administración de Usuarios	● Débiles o nulos componentes de la autenticación ● No limitar el acceso a la autenticación	- Que se logre descifrar los componentes de la autenticación - Que se pueda intentar autenticar desde cualquier máquina.	- Que alguien altere archivos de configuración del servicio. Nivel de impacto: alto - Que alguien altere cualquier componente de la MV. Nivel de impacto: alto

Objetivo 10: Requerir autenticación para el ingreso a la máquina de gestión de un centro de datos.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Administración de usuarios	● Débiles o nulos componentes de la autenticación ● No limitar el acceso a la autenticación	- Que se logre descifrar los componentes de la autenticación - Que alguien se pueda intentar autenticar desde cualquier máquina.	- Que alguien descifre los componentes de la autenticación como una máquina o una contraseña y altere cualquier componente de la MV de gestión. Nivel de impacto: alto - Que alguien se pueda intentar autenticar desde cualquier máquina y luego altere cualquier componente de la MV de gestión al no tener un límite desde donde se puede intentar autenticar. Nivel de impacto:alto
IP	● Que la IP para ingresar a la maquina de gestión pueda ser utilizada por otra máquina	- Que alguien malintencionado asigne la IP a otra máquina - Que a otra máquina se le asigne la misma IP	- Que alguien malintencionado utilice la IP en otra máquina y pueda tener contacto con la máquina de gestión. Nivel de impacto:alto

Objetivo 11: Mantener confidenciales las IP's de las máquinas virtuales del servicio para los clientes.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
IP's	● Fácil visibilidad la IP de las máquinas de los servicios	- Un atacante conozca fácilmente la ip del servidor que lo atiende	- Un atacante conoce fácilmente la ip del servidor que lo atiende y pueda aprovecharse de ello para realizar un ataque. Nivel de impacto: alto

Objetivo 12: Mantener un manejo responsable y autorizado de las direcciones IP asignadas a las máquinas virtuales del servicio.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
IP's	● Fácil y no administrada asignación de IP's a las máquinas del servicio	- Un atacante pueda acceder y cambiar las redes de una MV	- Un atacante puede asignar direcciones indebidas a MV para generar daño o extraer información Nivel de impacto: alto

Objetivo 13: Procurar mantener la disponibilidad del servicio en relación con las direcciones IP de las máquinas servicio.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
IP's	● Compleja configuración de los servicios en relación con de direcciones IP	- Pérdida de disponibilidad - Configuraciones irrecuperables - Cambios drásticos en el servicio - Atacantes malintencionados	- Pérdida de mucha disponibilidad por los largos tiempos de configuración de los servicios en relación con las IP Nivel de impacto: alto - Configuraciones irrecuperables debido a que la configuración es compleja y larga y no se puede replicar. Nivel de impacto: alto - Cambios drásticos de un servicio complejo pueden causar una larga pérdida de disponibilidad. Nivel de impacto: alto - Atacantes malintencionados aprovechan puede atacar los servicios de IP y por la complejidad de restablecer para afecta la disponibilidad Nivel de impacto: alto

Objetivo 14: Requerir autorización para identificar los usuarios al ingreso a los servicios básicos			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Sistema operativo	● Débiles o nulos componentes de la autenticación ● No limitar el acceso a la autenticación ● No tener niveles de privilegios	- Que se logre descifrar los componentes de la autenticación - Posibilidad de realizar escalamiento de privilegios - Que alguien tenga permisos para realizar acciones que no debería tener	- Que alguien logre descifrar la autenticación y altere archivos de configuración del servicio. Nivel de impacto: alto - Que alguien altere cualquier componente de la MV y logre realizar un escalamiento de privilegios hasta el administrador de la máquina. Nivel de impacto: alto - Que un usuario tenga más permisos de los que debería tener y altere archivos de configuración del servicio. Nivel de impacto: alto

Objetivo 15: Mantener disponibilidad en el tráfico de red para gestionar los servicios básicos.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**

Red	● Imposibilidad del paso del tráfico entre los servicios.	- Recepción de paquetes malintencionados - Recepción de grandes cantidades paquetes	- Paquetes que realicen una denegación del servicio de red y se detenga el tráfico de la red Nivel de impacto: alto

Objetivo 16: Mantener la integridad de la información transmitida entre las máquinas virtuales de un centro de datos			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Paquete de información	● Que el paquete pueda ser alterado o reemplazado	- Que alguien logre acceder al paquete - Que se de una falla en la red	- Que un atacante pueda cambiar información de un paquete Nivel de impacto: alto - Que un atacante pueda cambiar el paquete por otro Nivel de impacto: alto - Que se cambie un paquete durante transmisión Nivel de impacto: alto

Objetivo 17: Mantener la confidencialidad de la información entre la máquina de gestión interna y la máquina de gestión externa.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Paquete de información	● Que el paquete de información sea legible durante la comunicación	- Que un tercero intercepte la información del paquete.	- Que alguien pueda leer e interpretar el contenido del paquete. Nivel de impacto: medio-alto

Objetivo 19: Mantener disponibilidad en el servicio de la Red Social.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Servidor de red social	● Que el servidor no tenga un respaldo ante una eventualidad en el servidor de la red social.	- Que el servidor no dé abasto a las solicitudes de información. - Que alguien malintencionado ataque el servidor. - Que se produzca y una falla en el servidor.	- Que el servidor se caiga y rechace las solicitudes porque no da abasto a las solicitudes de información . Nivel de impacto: Alto ● Que alguien malintencionado ataque el servidor y este se caiga o se sature. Nivel de impacto: Alto ● Que alguien malintencionado ataque el servidor y modifique el servidor.

			Nivel de impacto: medio-alto ● Que se produzca y una falla en el servidor y no quede disponible. Nivel de impacto: Alto
Servicio de red social	● Que la red social no cuente o sea deficiente en términos de alta disponibilidad y tolerancia a fallas. ● Que los desarrolladores no previeron o no tomaron en cuenta características de alta disponibilidad y tolerancia a fallos. ● Que el servicio tolere una baja cantidad de solicitudes de usuarios.	● Que la información de la red social no pueda ser replicada. ● Que el servicio no pueda ser replicado. ● Que la replicación sea ineficiente. ● Que las solicitudes sobrecarguen el servicio.	● Que la información de la red social no pueda ser replicada y se pierda ante una eventualidad. Nivel de impacto: Alto ● Que el servicio no pueda ser replicado y el servicio no esté disponible. Nivel de impacto: Alto ● Que la replicación sea ineficiente y no sea suficiente para mantener el servicio. Nivel de impacto: Alto ● Que las solicitudes sobrecarguen el servicio y que el servicio de caída o se sature el servicio. Nivel de impacto: Alto

Análisis de seguridad con base en los riesgos

Esta sección de la seguridad, posterior a la identificación del elemento analizado y los objetivos de seguridad, presenta los riesgos identificados y el análisis de seguridad con base en los riesgos donde se describen las políticas y controles a implementar.

Políticas de seguridad

1. Implementar un software que permita la transferencia de información entre los centros de datos de manera confidencial, íntegra y con características de no replay.
2. Implementar un software que permita la transferencia segura de los datos desde internet hacia la red interna, además de proveer seguridad a la infraestructura.
3. Utilizar mecanismos de autenticación para el ingreso a la gestión de las máquinas un centro de datos.
4. Utilizar mecanismos de autenticación para el ingreso a la máquina de gestión de un centro de datos.
5. Implementar un mecanismo para mantener la confidencialidad de la información transmitida entre las máquinas virtuales de un centro de datos.
6. Implementar un mecanismo para mantener la confidencialidad de los datos transmitida desde los usuarios hasta el hipervisor.
7. Implementar una herramienta que permita tener un alto grado de confidencialidad de las IP’s de las máquinas virtuales del servicio para los clientes y que también permite

poder gestionar las IP's para brindar alta disponibilidad del servicio en relación con las direcciones.
8. Usar las versiones más recientes del software que se utilice para mantener el sistema actualizado, dichas actualizaciones deben darse únicamente en tiempo donde se pueda dar esta clase de gestión, no cuando el sistema está en uso normal.
9. Implementar un software que automatice el proceso de entrega de una configuración de red a las máquinas que la necesiten, manteniendo el cuidado de no salirse de un rango establecido de direcciones ni de direcciones.
10. Implementar un software que permita la gestión centralizada de la infraestructura, además de autenticación y autorización.
11. Implementar un mecanismo para mantener la confidencialidad de la información transmitida entre las máquinas de gestión interna y externa.
12. Implementar mecanismos para proporcionar una alta disponibilidad en el servicio de la red social.
13. Implementar un mecanismo para mantener la confidencialidad e integridad de los datos transmitida desde los usuarios hasta el hipervisor.

Controles de seguridad

1. IPsec

Objetivo 1: Mantener la integridad de la información transmitida entre los centros de datos.
Riesgos:

- Que alguien cambie información de un paquete: Nivel de impacto: alto
- Que alguien cambie el paquete por otro : Nivel de impacto: alto

Objetivo 2: Requerir autenticación para asegurarse de que quien transmite la información entre centro de datos es de quien dice ser.
Riesgos:

- Que se cambie el origen de información y el destino no se de cuenta. Nivel de impacto: alto
- Que se cambie el destino de la información y se acepté la información. Nivel de impacto: alto
- Que se cambie el destino de la información y no se de cuenta de que recibió información no esperada. Nivel de impacto: alto

Objetivo 3: Mantener la confidencialidad de la información transmitida entre los dos centros de datos.
Riesgos:

- Que alguien pueda leer e interpretar el contenido del paquete. Nivel de impacto: medio-alto

Herramienta de control para la política 1
Con IPsec podemos evitar cualquiera de estos riesgos que aparecen asociados a los objetivos de seguridad ya que IPsec provee de integridad, confidencialidad y autenticación. IPsec está configurado para comunicar a los dos centros de datos por medio de un túnel el cual lleva datos encriptados desde el origen hasta el destino de manera segura, evitando cualquiera de los riesgos previamente mencionados.

2. Firewall

Objetivo 6: Mantener la confidencialidad de la información transmitida entre las máquinas virtuales de un centro de datos.
Riesgo:

- Que alguien pueda leer e interpretar el contenido del paquete. Nivel de impacto: medio-alto

Objetivo 8: Mantener la integridad de las máquinas virtuales ante accidentes e intentos maliciosos de acceso.
Riesgos:

- Que alguien altere cualquier componente del sistema operativo.
- Que alguien altere archivos de configuración del servicio.
- Que alguien altere cualquier componente de la MV.

Herramienta de control para la política 2
Gracias a una máquina que hace función de firewall se pueden evitar estos riesgos, dicha máquina está colocada en la entrada a la red interna del ESXi y solo se puede acceder a esta red de esta manera, por lo que no es posible que alguien pueda interceptar o alterar los paquetes que anden por esta red. Este firewall hace que la red interna al ESXi quede aislada de manera que nada de lo que esté dentro de esta red pueda ser interceptado por un tercero.

3. Firewall de gestión

Objetivo 9: Requerir autenticación para el ingreso a la gestión de las máquinas un centro de datos.
Riesgos:

- Que alguien altere archivos de configuración del servicio.
- Que alguien altere cualquier componente de la MV.

Objetivo 10: Requerir autenticación para el ingreso a la máquina de gestión de un centro de datos.
Riesgos:

- Que alguien descifre los componentes de la autenticación como la máquina o la contraseña y altere cualquier componente de la MV de gestión.
- Que alguien se pueda intentar autenticar desde cualquier máquina y luego altere cualquier componente de la MV de gestión al no tener un límite desde donde se puede intentar autenticar.

Objetivo 17: Mantener la confidencialidad de la información entre la máquina de gestión interna y la máquina de gestión externa.
Riesgos:

- Que alguien pueda leer e interpretar el contenido del paquete.

Herramienta de control para las políticas 3 y 4

Se usa un firewall en la máquina de gestión ya que esta máquina funciona como entrada alternativa al sistema, esto sirve en caso de que pase algo con la entrada principal (el firewall mencionado en el punto 2) entonces tenemos una entrada diferente para poder revisar qué está pasando en el sistema. De igual manera esta máquina de gestión tiene que estar asegurada para que nadie pueda entrar, es por esto que tiene un firewall con iptables el cual

solo permite conexiones desde unas ciertas IP's. Además, esta máquina es la única con capacidad de hacer ssh con las demás máquinas del sistema para poder entrar a gestionarlas, por lo que las demás máquinas están protegidas de que se intente acceder a estas desde otras máquinas. Finalmente, este firewall de gestión está en una red diferente por la cual trabaja el sistema, se podría decir que es una red dedicada específicamente a la gestión.

Herramienta de control para la política 11

Mediante un secure shell (ssh) se puede lograr tener control de la confidencialidad entre las comunicaciones de dos máquinas. En la máquina de gestión interna del centro de datos se agregan reglas de firewall para que únicamente una máquina de gestión externa al centro de datos pueda acceder remotamente a ella. La única máquina que puede lograr autenticarse mediante ssh es la máquina de gestión externa porque su dirección IP está establecida en el firewall como el único punto de acceso externo.

La máquina de gestión externa no se puede asegurar, no tenemos para poder modificar y hacer administración en esa máquina. Pero si hay que lograr resguardar el usuario y la contraseña para que ningúna persona malintencionada tenga acceso a ella.

Riesgo asumido:

El riesgo de que una persona malintencionada utilice la IP para intentar el ingreso a la máquina de gestión, es un riesgo que se va a aceptar ya que la probabilidad de ocurrencia no es muy alta.

4. Comunicación con rangos de redes

Objetivo 6: Mantener la confidencialidad de la información transmitida entre las máquinas virtuales de un centro de datos.
Riesgo:

- Que alguien pueda leer e interpretar el contenido del paquete. Nivel de impacto: medio-alto

Herramienta de control para la política 5

Red interna del hipervisor

Las máquinas virtuales dentro de los centros de datos utilizarán un rango en direcciones IP en una red específica la cual solo puede ser accedida dentro del hipervisor donde se encuentran. Ningún elemento ajeno al hipervisor podrá tener acceso a los paquetes enviados por esta red.

Objetivo 6: Mantener la confidencialidad de la información transmitida entre las máquinas virtuales de un centro de datos.
Riesgo:

- Que alguien pueda leer e interpretar el contenido del paquete. Nivel de impacto: medio-alto

Herramienta de control para la política 5

Red interna de la Nube académica

Las máquinas virtuales de firewall dentro de los centros de datos utilizarán un rango en direcciones IP en una red específica la cual solo puede ser accedida entre los Blade de la NAC o dentro de cada hipervisor. Ningún elemento ajeno a la NAC podrá tener acceso a los paquetes enviados por esta red.

Objetivo 10: Requerir autenticación para el ingreso a la máquina de gestión de un centro de datos.
Riesgos:

- Que alguien se pueda intentar autenticar desde cualquier máquina y luego altere cualquier componente de la MV.

Herramienta de control para la política 5

Red interna a UCR

Las máquinas virtuales de gestión dentro de los centros de datos utilizarán un rango en direcciones IP en una red específica la cual solo puede ser accedida si se está conectado a esta red de la UCR. Ningún elemento ajeno a la red de la UCR podrá tener acceso a los paquetes enviados por esta red.

5. Actualizaciones

Objetivo 7: Mantener la integridad del hipervisor y su información ante accidentes e intentos maliciosos de acceso.
Riesgo:

- Que alguien altere cualquier componente del sistema.

Objetivo 8: Mantener la integridad de las máquinas virtuales ante accidentes e intentos maliciosos de acceso.

Riesgos:

- Que alguien altere cualquier componente del sistema operativo.
- Que alguien altere archivos de configuración del servicio.
- Que alguien altere cualquier componente de las MV.

Herramientas de control para la política 6

Actualizar los hipervisores para que se puedan corregir los parches de seguridad que se han detectado por el proveedor.

6. Objetivo 4

Para el objetivos 5 que tratan de mantener la integridad y confidencialidad de los paquetes que viajan entre el usuario y el centro de datos aún no se a tomado la decisión de cómo se van a lograr estos objetivos, se tienen ideas de como poder lograrlas pero hasta no consultar sobre la efectividad de estas soluciones es mejor no tomar decisiones precipitadas, pero si se tiene en cuenta que estos objetivos son de gran importancia y no los podemos asumir, se tienen que cumplir de alguna manera.

La política 7 y 13 corresponden a este objetivo pero aún no tiene una herramienta de control implementada.

7. DNS

Objetivo 11: Mantener confidenciales las IP's de las máquinas virtuales del servicio para los clientes.
Riesgo.

- Un atacante conoce fácilmente la ip del servidor que lo atiende y pueda aprovecharse de ello para realizar un ataque.

Objetivo 13: Procurar mantener la disponibilidad del servicio en relación con las direcciones.
Riesgos

- Pérdida de mucha disponibilidad por los largos tiempos de configuración de los servicios en relación con las IP
- Configuraciones irrecuperables debido a que la configuración es compleja y larga y no se puede replicar.
- Cambios drásticos de un servicio complejo pueden causar una larga pérdida de disponibilidad.
- Atacantes malintencionados aprovechan puede atacar los servicios de IP y por la complejidad de restablecer para afecta la disponibilidad

Herramientas de control para la política 8
Se implementará un DNS para asociar direcciones ip de máquinas, servidores y nombres de dominios para atender las solicitudes de los clientes y usuarios. Además, el enmascaramiento de las direcciones IP con un nombre es un beneficio de mayor seguridad para el servicio así como una herramienta que ayuda a gestionar más fácilmente el servicio y en caso de una eventualidad ayuda a reducir configuraciones complejas en beneficio de la disponibilidad del servicio.
Sirve como herramienta de control para mantener realizar la conversión entre los nombres del dominio e IP's, la cual se va a utilizar como un DNS externo como primera capa de interacciones entre los usuarios y los servicios.

8. DHCP

Objetivo 12: Mantener un manejo responsable y autorizado de las direcciones IP asignadas a las máquinas virtuales del servicio.
Riesgo:

- Un atacante puede asignar direcciones indebidas a MV para generar daño o extraer información

Herramientas de control para la política 9
Se implementará un dhcp para administrar y asignar de una mejor manera y centralizada la asignación de direcciones IP a las máquinas virtuales del servicio.

9. FreeIPA

Objetivo 14: Requerir autorización para identificar los usuarios al ingreso a los servicios básicos
Riesgos:

- Que alguien logre descifrar la autenticación y altere archivos de configuración del servicio.
- Que alguien altere cualquier componente de la MV y logre realizar un escalamiento de privilegios hasta el administrador de la máquina.

- Que un usuario tenga más permisos de los que debería tener y altere archivos de configuración del servicio.

Objetivo 15: Mantener disponibilidad en el tráfico de red para gestionar los servicios básicos.
Riesgo:

- Paquetes que realicen una denegación del servicio de red y se detenga el tráfico de la red.

Objetivo 16: Mantener la integridad de la información transmitida entre las máquinas virtuales de un centro de datos
Riesgos:

- Que un atacante pueda cambiar información de un paquete
- Que un atacante pueda cambiar el paquete por otro
- Que se cambie un paquete durante transmisión

Herramientas de control para la política 10
Servidor que provee un servicio de identidad y autenticación de usuarios, integrado con servicios adicionales de identidad, autenticación y autorización de recursos, para la gestión de una infraestructura de TI mediante un dominio interno de la red. El DNS anteriormente mencionado es el responsable de la atención de clientes y usuarios.
También sirve esta herramienta es un control de seguridad como una capa más para acceder a servicios básicos del los centros de datos porque si ocurre algún problema en cuanto a la disponibilidad del DNS externo, siendo una segunda capa, en la cual como es interno pueda permitir continuidad de los servicios a lo interno del centro de datos ante una eventualidad.

10. Cluster de Galera

Objetivo 19: Mantener disponibilidad en el servicio de la Red Social
Riesgos:

- Que la información de la red social no pueda ser replicada y se pierda ante una eventualidad.
- Que el servicio no pueda ser replicado y el servicio no esté disponible.
- Que la replicación sea ineficiente y no sea suficiente para mantener el servicio.
- Que las solicitudes sobrecarguen el servicio y que el servicio de caída o se sature el servicio.

Herramienta de control política 12
Mediante el clúster de galera, se puede tener redundancia de información y tener varias bases de datos(en nuestro caso 2) para ello. Además permite tener mayor disponibilidad en el caso de que un servidor de base de datos falle porque se tiene en un segundo lugar toda la información ya que están sincronizadas. Esto fue posible luego de alterar la configuración inicial del software de la red social.

11. Redundancia de servidores OSSN

Objetivo 19: Mantener disponibilidad en el servicio de la Red Social
Riesgos:

- Que el servidor se caiga y rechace las solicitudes porque no da abasto a las solicitudes de información .
- Que alguien malintencionado ataque el servidor y este se caiga o se sature.
- Que alguien malintencionado ataque el servidor y modifique el servidor.
- Que se produzca y una falla en el servidor y no quede disponible.

Herramienta de control política 12
No se pudo configurar una herramienta control para estos riesgos debido a la implementación de la red social como la desarrollaron y las limitaciones visibles de concurrencia que encontramos. Aún no se ha podido encontrar una solución por falta de tiempo.

12. Certificado digital

Objetivo 5: Mantener la integridad de la información transmitida entre el sistema de centro de datos y el usuario.

- Que un atacante pueda cambiar información de un paquete
- Que un atacante pueda cambiar el paquete por otro
- Que se cambie un paquete durante transmisión

Herramienta de control para política 6

La herramienta de control para esto es tener implementado un certificado digital para el sitio web de la red social y así establecer conexiones seguras entre los usuarios y la página hospedada en los centros de datos. Por falta de tiempo no se pudo intentar implementar este control.