

**Seminario final de redes y seguridad informática.**

**Diseño de la Red y Planificación de un SGSI para la empresa CENED**

**Autores:**

Amanda Heredia Fernández

Melisa Maura

Naomi

Yoangel Sabón

Kevin Peña

**Facultad:** Facultad Tecnologías Iterativas.

**Grupo:** 4303

**Introducción**

En el ámbito de la educación a distancia, la seguridad de la información y la gestión eficiente de los sistemas tecnológicos son esenciales. Este trabajo se enfoca en el diseño de la red y la planificación de un sistema de gestión de seguridad informática para CENED, un centro especializado en la educación a distancia. La importancia de establecer una infraestructura de red sólida y segura es crucial; no solo protege la integridad y confidencialidad de los datos académicos y administrativos, sino que también garantiza un servicio continuo y confiable para estudiantes, docentes y personal administrativo.

Un sistema de gestión de seguridad robusto ofrece múltiples beneficios específicos para CENED. Además de proteger contra amenazas internas y externas, este sistema asegura el cumplimiento de normativas y estándares tecnológicos, lo que refuerza la credibilidad del centro y fomenta la confianza de los usuarios en sus servicios educativos.

A lo largo de este documento, se explorarán los elementos clave que deben considerarse en el diseño de la red y en la planificación de la seguridad informática. Se empleará terminología técnica adecuada para proporcionar una visión completa y detallada, sin perder de vista la relevancia práctica que estos conceptos tienen en el funcionamiento diario de CENED.

## Desarrollo

Identificar la entidad organizativa que se pretende proteger:

### Caracterización del proyecto

El Centro Nacional de Educación a Distancia (CENED) en Cuba es una institución innovadora que se dedica a la promoción y mejora de la educación a distancia y semipresencial en el país. Desde su creación, CENED ha establecido un enfoque integral hacia la formación académica, utilizando tecnologías de la información y la comunicación (TIC) para facilitar el aprendizaje. CENED juega un papel crucial en el sistema educativo cubano al permitir el acceso a la educación superior a un mayor número de estudiantes. Su enfoque en la flexibilidad y la adaptación tecnológica no solo mejora la calidad educativa, sino que también responde a las demandas del mercado laboral actual. A medida que el mundo avanza hacia modelos educativos más digitales, CENED se posiciona como un líder en esta transformación, contribuyendo al desarrollo social y económico del país. En su plan de expansión, CENED busca incorporar nuevas tecnologías y metodologías que amplíen su oferta educativa. Esto incluye el desarrollo de un sistema más robusto para la gestión académica y administrativa, así como mejoras en las plataformas tecnológicas utilizadas para facilitar el aprendizaje. De esta manera, CENED se compromete a seguir innovando en el ámbito educativo, garantizando la seguridad y eficiencia en la gestión de datos críticos para su funcionamiento.

* Ubicación del local

El centro es ocupado por las áreas de Dirección, Asistente de Control, Profesores, Salón y Laboratorio del Centro Nacional de Educación a Distancia (CENED) que se encuentra en Carretera de San Antonio de los Baños, Km 2, Torrens, La Habana.

* Nombres y apellidos de los responsables al frente de la entidad

Director: Iván Pérez Mayea

Tecnólogo: Dalia Campos

Comunicador: Yisel Arias

* Descripción técnica de la red

Los locales comprendidos en el Plan de Seguridad Informática del CENED son cinco: La Dirección, Asistente de control, Profesores, Salón y Laboratorio. Todos están ubicados en el bloque de oficinas del Docente 3 y la única subred existente en el área es la 10.33.33.0/24.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Nombre | Tipo | Clasificación | Ubicación | Descripción |
| 1 | Laptop MB Directora | HW | Esencia | Dirección |  |
| 2 | Estación de trabajo | HW | Esencia | Asistente de control |  |
| 3 | Impresora | HW | Periférico | Dirección y Asistente de contro |  |
| 4 | Teléfono | HW | Comunicación | Dirección y Asistente de contro |  |
| 5 | Backups | HW | Respaldo | Dirección, Salón y Laboratorio |  |
| 7 | Cable Coaxial para TV | HW | Conexión | Salón y Laboratorio |  |
| 8 | Switch Capa-2 | HW | Red | Laboratorio |  |
| 9 | SO. Linux | SW | Sistema Operativo | Dirección, Salón y Laboratorio |  |
| 10 | Herramientas de Edición de imágenes, audio y video | SW | Software Creativo | Profesores, Salón y Laboratorio |  |
| 11 | Wine | SW | Compatibilidad | Salón y Laboratorio |  |
| 12 | Documentación de programas | D | Información Técnica |  |  |
|  | TV | HW | Multimedia | Salón y Laboratorio | Pantallas para presentaciones o clases |
| 14 | Documentación de sistemas | D | Información Técnica | Dirección, Salón y Laboratorio | Manuales sobre la configuración del sistema |
| 15 | Laptop MB Jefe de Departamento Tecnologías | HW | Esencial   Laboratorio Equipo portátil del jefe del departamento | Dirección, Salón y Laboratorio | Laptop asignada al jefe del Departamento de Tecnologías |
| 16 | Laptop MB Jefe de Departamento Gestión HW Esencial Profesores Equipo portátil del jefe del departamento | HW | esencial | Profesores | Laptop asignada al jefe del Departamento de Gestión |
| 17 | Cable fibra óptica HW Conexión General Cableado para transmisión de datos | HW | esencial | Genera | Cableado para transmisión rápida de datos en la red local |

* Políticas de Seguridad Informática

Las Políticas de Seguridad Informática se trazan atendiendo a la importancia de la información que se maneja en cada local, de los activos informáticos presentes y de la necesidad de preservar la integridad, confidencialidad y disponibilidad de la información. Las mismas deben ser de obligatorio cumplimiento por todo el personal con acceso a las áreas involucradas en este plan.

1- Todas las estaciones de trabajo deben estar en el dominio UCI.

2- En cada estación de trabajo solo existirán dos cuentas de usuario: La de administración y una cuenta de usuario con permisos estándares, en el caso del Salón y Laboratorio esta debe ser profesor.

3- El Asesor de Seguridad Informática del centro debe conocer la contraseña de administración de cada puesto de trabajo.

4- De existir carpetas compartidas, deben estar autorizadas por la Directora del Centro y el Asesor de Seguridad Informática, protegidas por contraseña y deben estar bien definidos los usuarios con acceso a estas.

5- No existirán en las estaciones de trabajo contraseñas guardadas.

6- Las computadoras personales que se encuentren en las áreas del Centro deben cumplir las Políticas de Seguridad Informática establecidas para el Centro.

4.1. Adquisición, uso, mantenimiento y traslado de las tecnologías de información de la entidad

* La adquisición de nuevas tecnologías informáticas y de las comunicaciones para el centro la efectuara el área de la dirección de la UCI encargada de esta tarea.
* Las reparaciones y mantenimientos necesarios a todo el equipamiento instalado serán llevadas a cabo por COPEXTEL o las personas autorizadas a ello, para garantizar así su eficiente funcionamiento.
* El traslado interno o externo de las tecnologías debe ser previamente autorizado por la dirección del centro. Debe llenarse además el modelo establecido para dicho traslado.
* El personal que utilice en las áreas equipamiento de su propiedad, deberá garantizar en los mismos todos los requerimientos de seguridad establecidos para la tecnología del centro.

4.2. Gestión para la implantación de nuevas versiones de sistemas y aplicaciones

* Mantener actualizados todos los Sistemas Operativos.
* Todas las estaciones de trabajo deben estar migradas a software libre. Solo las autorizadas podrán tener dos SO (Linux/Windows) siendo Linux el de booteo por defecto.
* Las estaciones de trabajo que posean distribuciones GNU/Linux deben ser estables y estar actualizadas desde los repositorios centrales de la UCI. Por otra parte, las estaciones de trabajo con SO Windows deben tener Windows 7 o superior.

4.3. Protección contra programas malignos

* Queda prohibido el diseño, la distribución o intercambio de códigos de virus informático u otros programas malignos entre personas naturales o jurídicas.
* Es de carácter obligatorio tener instalado en todas las estaciones de trabajo el antivirus informático SAV de Segurmática Antivirus o Kaspersky Antivirus, configurado para actualizaciones diarias y escaneos semanales.
* Antes de la utilización de soportes magneto-ópticos, estos deben ser escaneados y las amenazas detectadas deben ser debidamente atendidas.
* Ante indicios de contaminación por un virus informático nuevo o desconocido, asilarlo o apagar el equipo, preservar la estación de trabajo infectada y comunicarse de inmediato con el Asesor de Seguridad Informática del área.

4.4. Preparación y realización de auditorías

* Se realizarán auditorias y controles internos para conocer el cumplimiento del Plan de Seguridad Informática y la preparación de los trabajadores implicados. Estas se efectuarán en el periodo que se estime conveniente pero nunca mayor a tres meses, pueden ser avisadas, al menos, con tres días de antelación o auditorías sin previo aviso.

Riesgo

Análisis de riesgos

Valoración de la importancia por cada activo y cálculo de la importancia

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Importancia | | | | | |
| No | Nombre | Dominio | Func. | Costo | Imagen | Conf. | integ | disp | Valor |
| 1 | Laptop MB Directora | Dominio 1 | 9 | 7 | 9 | 9 | 9 | 8 | 8.33 |
| 2 | Estación de trabajo | Dominio 1 | 8 | 6 | 8 | 8 | 8 | 7 | 7.67 |
| 3 | Impresoras | Dominio 1 | 6 | 5 | 6 | 6 | 6 | 5 | 5.33 |
| 4 | Teléfonos | Dominio 1 | 6 | 5 | 6 | 6 | 6 | 5 | 5.33 |
| 5 | Backups | Dominio 1 | 10 | 8 | 9 | 10 | 10 | 9 | 9.00 |
| 6 | Teléfonos (Salón y Laboratorio) | Dominio 1 | 5 | 4 | 5 | 5 | 5 | 4 | 4.33 |
| 7 | TV | Dominio 1 | 4 | 3 | 4 | 4 | 4 | 3 | 3.33 |
| 8 | Cable Coaxial para TV | Dominio 1 | 3 | 2 | 3 | 3 | 3 | 2 | 2.50 |
| 9 | Switch Capa-2 | Dominio 1 | 7 | 6 | 7 | 7 | 7 | 6 | 6.33 |
| 10 | SO. Linux | Dominio 1 | 9 | 7 | 8 | 9 | 9 | 8 | 8.33 |
| 11 | Herramientas de Edición de imágenes, audio y video | Dominio 1 | 8 | 6 | 8 | 9 | 8 | 7 | 7.67 |
| 12 | Wine | Dominio 1 | 8 | 6 | 7 | 8 | 7 | 7 | 7.00 |
| 13 | Laptop MB Jefe de Departamento Tecnologías | Dominio 1 | 9 | 7 | 9 | 9 | 9 | 8 | 8.33 |
| 14 | Laptop MB Jefe de Departamento Gestión | Dominio 1 | 9 | 7 | 9 | 9 | 9 | 8 | 8.33 |
| 15 | Documentación de programas | Dominio 1 | 6 | 4 | 5 | 5 | 5 | 5 | 4.00 |
| 16 | Documentación de sistema | Dominio 1 | 6 | 4 | 5 | 5 | 5 | 5 | 4.00 |
| 17 | Cable fibra óptica | Dominio 1 | 3 | 2 | 3 | 3 | 3 | 2 | 2.50 |

### Listado de amenazas y análisis cruzado

|  |  |
| --- | --- |
| Amenazas | Activos Afectados |
| Fuego | HW, AUX, L |
| Inundaciones | HW, AUX, L |
| Corte del suministro eléctrico | [HW] |
| Errores de Usuario | D, S, SW |
| Errores de Administradores | D, S, SW, HW, COM |
| Software Dañino | SW |

### Estimación del riesgo

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Activo | Fuego (P/I) | Inundaciones (P/I) | Corte del suministro eléctrico (P/I) | Errores de Usuario (P/I) | | Errores de Administradores (P/I) | Software Dañino (P/I) | Ri | 𝜔𝑖 | Ri  \*𝜔𝑖 |
| 1 | 2/5 | 1/4 | 3/4 | | 4/5 | 4/5 | 3/5 | 19 | 9.67 | 183.73 |
| 2 | 2/4 | 1/3 | 3/4 | | 4/4 | 3/4 | 3/4 | 16 | 8.17 | 130.72 |
| 3 | 2/4 | 1/3 | 3/4 | | 4/4 | 3/4 | 3/4 | 16 | 8.33 | 133.28 |
| 4 | 2/3 | 1/2 | 3/3 | | 4/4 | 3/3 | 3/3 | 14 | 7.67 | 107.38 |
| 5 | 3/4 | 2/3 | 4/4 | | 3/3 | 3/3 | 2/3 | 15 | 6.67 | 100.05 |
| 6 | 3/4 | 2/3 | 4/4 | | 3/3 | 3/3 | 2/3 | 15 | 6.67 | 100.05 |
| 7 | 2/5 | 1/4 | 3/4 | | 4/5 | 4/5 | 3/5 | 19 | 9.67 | 183.73 |
| 8 | 2/4 | 1/3 | 3/4 | | 4/4 | 3/4 | 3/4 | 16 | 8.83 | 141.28 |
| 9 | 2/3 | 1/2 | 3/3 | | 4/3 | 3/3 | 3/3 | 14 | 7.50 | 105.00 |
| 10 | 3/3 | 2/2 | 4/3 | | 3/2 | 3/2 | 2/2 | 14 | 5.17 | 72.38 |
| 11 | 3/3 | 2/2 | 4/3 | | 3/2 | 3/2 | 2/2 | 14 | 5.17 | 72.38 |
| 12 | 3/4 | 2/3 | 4/3 | | 3/3 | 3/3 | 2/3 | 15 | 6.17 | 92.55 |
| 13 | 2/4 | 1/3 | 3/4 | | 4/4 | 3/4 | 3/4 | 16 | 8.33 | 133.28 |
| 14 | 3/3 | 2/2 | 4/3 | | 3/2 | 3/2 | 2/2 | 14 | 5.17 | 72.38 |
| 15 | 3/2 | 2/1 | 4/2 | | 3/1 | 3/1 | 2/1 | 11 | 4.17 | 45.87 |
| 16 | 2/4 | 1/3 | 3/3 | | 4/4 | 3/3 | 3/3 | 16 | 7.33 | 117.28 |
| 17 | 2/5 | 1/4 | 3/4 | | 4/5 | 4/5 | 3/5 | 20 | 8.83 | 176.60 |

Las áreas sometidas a un mayor peso de riesgo y las amenazas que lo motivan son:

• La Dirección (Las averías de origen físico, errores de usuarios y fallo de servicios de comunicaciones).

• La Asistente de Control (Las averías de origen físico, errores de usuarios y fallo de servicios de comunicaciones).

• Profesores (Las averías de origen físico y errores de usuarios).

• Salón (Las averías de origen físico, fallo de servicios de comunicaciones).

• Laboratorio (Las averías de origen físico, errores de usuarios, fallo de servicios de comunicaciones y errores de mantenimiento / actualización de programas).

### Selección de controles

Amenaza: Fuego, Inundaciones, Terremotos

Control: Se debiera asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión y otras formas de desastres naturales o causados por el hombre.

La ISO establece:

Se debieran considerar los siguientes lineamientos para evitar el daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre:

a) los materiales peligrosos o combustibles debieran ser almacenados a una distancia segura del área asegurada. Los suministros a granel como papelería no deben almacenarse en el área asegurada;

b) el equipo de reemplazo y los medios de respaldo debieran ubicarse a una distancia segura para evitar el daño de un desastre que afecte el local principal;

c) se debiera proporcionar equipo contra-incendios ubicado adecuadamente.

Riesgo: Fuego

Salvaguarda:

• Instalación de Alarmas

• Mantenimiento de Extintores

• Almacenar Backus en local diferente al servidor

d) Realizar inspecciones periódicas de la integridad estructural del edificio para identificar y reparar posibles debilidades.

e) Desarrollar y mantener un plan de respuesta a emergencias, incluyendo procedimientos de evacuación y primeros auxilios.

f) Utilizar tecnologías de redundancia para asegurar la continuidad operativa de los sistemas críticos.

g) Realizar evaluaciones periódicas de riesgos para identificar nuevas amenazas y evaluar la efectividad de los controles existentes.

h) Establecer canales de comunicación de emergencia para coordinar respuestas rápidas y eficaces en caso de desastres.

## Recuperación ante desastre

El Plan de Recuperación ante Desastres (PRD), tiene como objetivo detectar los riesgos presentes en el entorno, analizar su probabilidad de ocurrencia, establecer su criticidad según cómo afectan la continuidad del negocio, y finalmente proponer un plan que logre mitigar en cierta medida estos riesgos, y que permita la recuperación de la disponibilidad de los recursos lógicos, físicos y humanos ante situaciones de contingencia(F. Tipton, s. f.).

### Definición de los tipos de operación en una contingencia

Para elaborar el Plan de Recuperación ante Desastres (PRD), se consideran distintos estados de situación, que se definen a continuación, para establecer un marco claro que identifique y enumere las distintas instancias por las que puede atravesar el centro de cómputos de Desoft antes, durante y después de una contingencia.

Contingencia: Ataque de Programas Malignos en el Código Fuente de Soluciones

Selección de controles

Los medios técnicos utilizados en función de garantizar niveles de seguridad adecuados, tanto a nivel de software como de hardware, así como la configuración de los mismos, consisten en:

1. Sistemas Operativos y Aplicaciones: Las actualizaciones de los Sistemas Operativos en Windows se harán automáticamente. Las estaciones de trabajo se actualizan desde el servidor central. No se debe tener instalado Sistemas Operativos Obsoletos, a excepción de algunas áreas, las cuales deben tener una carta de autorización de la Dirección de Seguridad Informática (DSI) que los autorice a tener este tipo de Sistema Operativo. El firewall del sistema o del antivirus debe estar activado.

En el caso del sistema operativo Linux se mantienen constantemente actualizados en el servidor de la universidad (http://ucistore.uci.cu) los repositorios de las distribuciones: Debian (http://debian.uci.cu), Ubuntu (http://ubuntu.uci.cu), CentOS (http://centos.uci.cu) y NOVA (http://novarepo.uci.cu). El firewall debe estar activado. 2- Antivirus: Para la protección contra programas malignos se utiliza el antivirus Kaspersky o el Segurmática Antivirus. Las actualizaciones se encuentran disponible en http://kavupdates.uci.cu y http://savunixupdate.uci.cu respectivamente, los cuales se actualizan diariamente.

1. Cliente GRHS: Todas las máquinas deben tener instalado el cliente GRHS disponible en ftp://10.0.0.22/software/Tools/Security/ClienteGRHS/. El asesor de seguridad es responsable de mantener actualizado la información de su área en <https://grhs.uci.cu>.
2. 4- Servidores de uso interno: No se debe tener servidores locales, en casos excepcionales debe contar con carta de una autorización de la Dirección de Seguridad Informática (DSI) que autoriza por un tiempo determinado.
3. 5- Sistema OTRS: Para la gestión de incidentes de seguridad informática se utiliza el sistema OTRS. Este sistema permite facilitar el reporte de los incidentes de seguridad y gestionar de una manera eficiente los Centro Nacional de Educación a Distancia. mismos, donde se realiza un seguimiento completo desde el reporte hasta la solución de los incidentes.
4. Los incidentes de seguridad pueden ser reportados usando cualquiera de las vías siguientes:

• Mediante la página web: <http://reportesdrsi.uci.cu>

• Escribir un correo electrónico a las direcciones: seguridad.informática@uci.cu ó [reportesdrsi@uci.cu](mailto:reportesdrsi@uci.cu)

1. Sitio web de seguridad informática:

El sitio Web de la Dirección de Seguridad Informática se encuentra hospedado en la siguiente dirección https://seguridad.uci.cu, y su objetivo es:

• Mantener informado a la comunidad universitaria sobre las noticias más recientes en el ámbito de la seguridad tanto a nivel interno como en el ámbito internacional.

• Servir como referencia de consulta de las regulaciones, normas y políticas que se aplican en la entidad.

• Fomentar la discusión sobre temas de seguridad mediante la implementación de un foro de discusión accesible a todos los usuarios de la universidad.

• Proveer de documentación y manuales de seguridad que ayuden a los usuarios a enriquecer sus conocimientos.

1. Medios físicos:

• Todas las estaciones de trabajo deben contar con Backups como respaldo eléctrico antes fallas de electricidad.

• Todas las computadoras contarán con sellos de seguridad visible a todos los usuarios.

• Al terminar la jornada laboral se activará la alarma, en caso de que exista.

• Los aires acondicionados deben permanecer encendidos en el horario laboral, en las áreas donde existan. Centro Nacional de Educación a Distancia.

5.3. Procedimientos de Seguridad. A continuación, se describen los procedimientos relacionados con: El Proceso de salva de la información.

• Se deben realizar salvas de la información relacionada con los procesos medulares del Centro (dígase documentación u otros) de forma periódica.

• La salva de las plataformas Moodle se realizan dos veces al año coincidiendo con los cambios de semestre y almacenadas localmente en una PC del laboratorio.

• Los privilegios de acceso a la información de cada área deben estar de acuerdo a los roles que desempeña el personal.

Nota: En el centro existe un disco duro externo con el que se realiza la salva de información del centro dos veces al año. El proceso de gestión de los incidentes detectados del área.

Ante cualquier incidente o violación de la seguridad que pueda producirse se garantizará la continuidad, el restablecimiento y la recuperación de los procesos informáticos críticos. La recuperación se organizará teniendo en cuenta las acciones de respuesta a realizar, la determinación de los responsables de su cumplimiento y los recursos necesarios en cada caso. Ante cualquier incidente que afecte la Seguridad Informática se designará por la Dirección del Centro una comisión presidida por un miembro del Consejo de Dirección e integrada por especialistas no comprometidos directamente con el incidente, que realizará las investigaciones necesarias con el fin de esclarecer lo ocurrido, determinar el impacto, precisar los responsables y proponer la conducta a seguir.

La Dirección garantizará que, al producirse un incidente o violación de la SI, este acontecimiento se reporte inmediatamente a la Dirección de Seguridad Informática de la universidad. Este reporte incluirá como mínimo:

a) En qué consistió el incidente o violación.

b) Fecha y hora de comienzo del incidente y de su detección.

c) Implicaciones y daños para la entidad y para terceros.

d) Acciones iniciales tomadas.

e) Evaluación preliminar.

El asesor de Seguridad Informática habilitará un registro de incidencias para reflejar posibles violaciones con respecto a lo establecido en este Plan. Tratamiento de las laptops personales.

• Deben poseer el documento que autoriza la tenencia del medio tecnológico.

• Deben cumplir con todas las políticas de seguridad informática establecida por la universidad y el centro. Las Auditorías Internas.

• Se realizan trimestralmente.

• Se genera un informe que se presenta en el Consejo de Dirección del Centro.

• Se toman medidas (En el caso de detectarse alguna incidencia se hace un llamado de atención al trabajador, si reincide se aplican medidas más rigurosas, determinadas por la dirección del centro).

### Establecimiento de Criticidades

La idea ante determinar la criticidad de los activos es que en esta etapa se establezca la criticidad de las aplicaciones, de los equipos y los servicios que sostienen al negocio(Stallings, s. f.-a). En función del impacto producido por la suspensión de las prestaciones del entorno informatizado, se determina la criticidad y el tiempo máximo de tolerancia de corte de las mismas.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | Activo | Función | SO | Criticidad | Tolerancia | Impacto |
| 14 | Estaciones de trabajo | Utilizadas por profesores y personal administrativo para gestión académica | Linux/Windows | Media | 2 Días | Retrasos en la gestión académica y administrativa |

Inventario de activos informáticos a proteger

1. Hardware (HW):

* Laptop Medio Básico. - Laptop MB de la directora del Centro.
* - Laptop MB de la jefa del Departamento de Gestión de la Formación a Distancia.
* - Laptop MB del jefe del Departamento de Tecnologías para el Aprendizaje

2- Estaciones de Trabajo.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Dirección | Asistente de Control | Profesores | Salón | Laboratorio | Total |
| 1 | 1 | 7 | 1 | 21 | 31 |

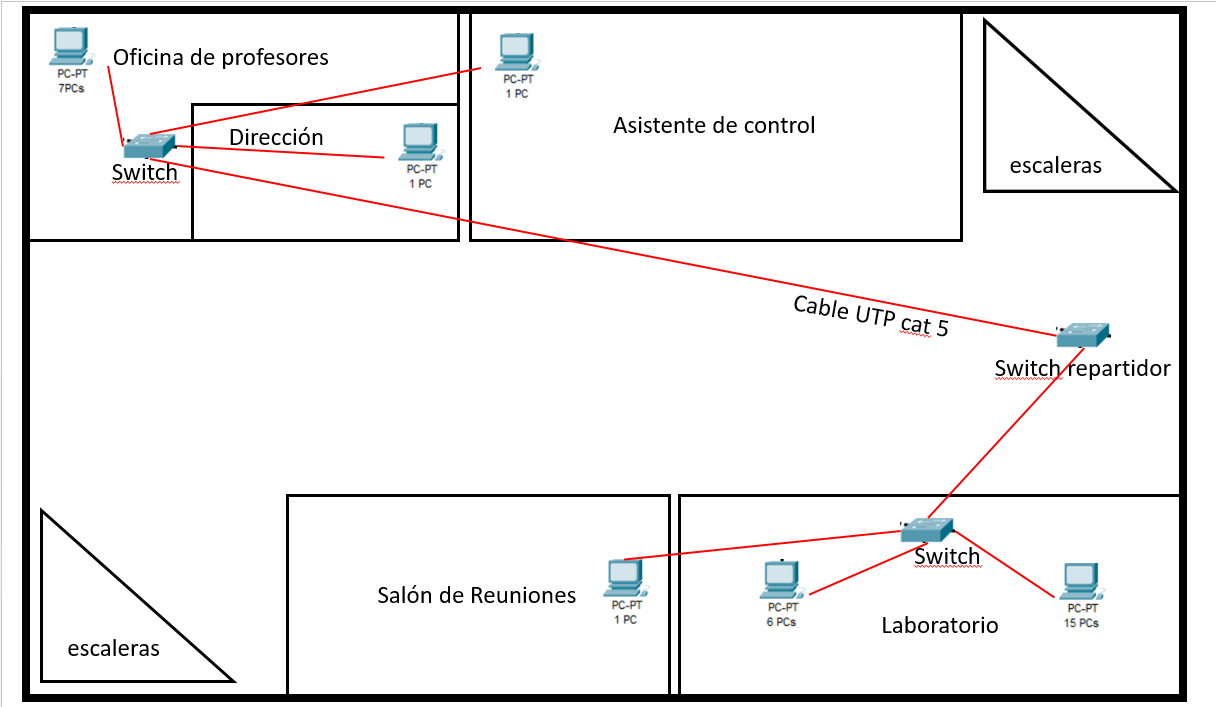
Tabla 1: Distribución de las estaciones de trabajo del centro por locales.

Nota: De las 31 estaciones de trabajo solo una está rota, las demás, están en perfecto estado técnico. De las 30 en buen estado, 29 poseen el sistema operativo Linux y una tiene tanto el Sistema operativo Linux como SO Windows, con la autorización de la Directora del Centro y el Asesor de Seguridad Informática, debido a que es la estación de trabajo de una profesora de la Disciplina de Idiomas Extranjeros y Jefa del Tribunal para examen de mínimo de doctorado y ejercicio de idioma para cambio de categoría docente y requiere de aplicaciones que solo corren en SO Windows.

3- Líneas de Comunicación.

El cableado troncal vertical conecta diferentes pisos o áreas del edificio. Ventajas: Asegura que todas las secciones de CENED estén interconectadas de manera óptima y permite una gestión centralizada de la red. Desventajas: La instalación puede ser más compleja y costosa debido a la necesidad de atravesar múltiples pisos. Medidas a tomar: Es importante considerar la estructura del edificio y utilizar materiales de alta calidad para evitar problemas futuros, además de implementar protecciones contra incendios y otras emergencias.

Para ambos sistemas de cableado, se ha seleccionado el cable UTP (Unshielded Twisted Pair) categoría 5e por sus excelentes prestaciones en términos de velocidad y fiabilidad. Este tipo de cable, combinado con la interfaz RJ45, garantiza conexiones estables y de alta calidad en toda la red de CENED.



4- Dispositivos de interconexión.

* Un Switch repetidor que se conectan con el switch del laboratorio, y el switch de las oficinas

Direccionamiento

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Subred | Ci | #Bit | Network | Broadcast | Gateway | Masc |
| Laboratorio | 24 | 5 | 10.33.33.0 | 10.33.33.31 | 10.33.33.1 | 255.255.255.224 |
| Profesores | 10 | 4 | 10.33.33.32 | 10.33.33.63 | 10.33.33.33 | 255.255.255.224 |
| Dirección | 4 | 2 | 10.33.33.64 | 10.33.33.95 | 10.33.33.65 | 255.255.255.224 |
| Salón | 4 | 2 | 10.33.33.96 | 10.33.33.127 | 10.33.33.97 | 255.255.255.224 |
| Asistente de control | 4 | 2 | 10.33.33.128 | 10.33.33.159 | 10.33.33.129 | 255.255.255.224 |

## Muro de seguridad o firewall

Se propone como arquitectura de firewall para proteger el servidor de uso compartido: Screening router. Para lo que será necesario habilitar el filtrado a nivel de red en un choke empleando reglas iptables en el propio servidor.

#!/bin/bash

# Limpiar reglas existentes

iptables -F

iptables -X

iptables -Z

# Establecer políticas predeterminadas

iptables -P INPUT DROP

iptables -P FORWARD DROP

iptables -P OUTPUT ACCEPT

# Permitir tráfico en loopback (localhost)

iptables -A INPUT -i lo -j ACCEPT

# Permitir conexiones establecidas y relacionadas

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Permitir tráfico HTTP (puerto 80) para servidores web

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

# Permitir tráfico HTTPS (puerto 443) para servidores web seguros

iptables -A INPUT -p tcp --dport 443 -j ACCEPT

# Permitir tráfico SSH (puerto 22) para administración remota (recomendado cambiar el puerto)

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

# Bloquear todo el tráfico ICMP (ping) para evitar ataques de descubrimiento de red (opcional)

# iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

# Registrar intentos de acceso no autorizados (opcional, para análisis de seguridad)

iptables -A INPUT -j LOG --log-prefix "IPTables-Dropped: " --log-level 4

# Bloquear todo el resto del tráfico no permitido explícitamente

iptables -A INPUT -j DROP

# Guardar las reglas para que persistan después del reinicio

# Para sistemas basados en Debian/Ubuntu:

iptables-save > /etc/iptables/rules.v4

# Para sistemas basados en RedHat/CentOS:

# service iptables save

echo "Firewall configurado correctamente."

Conclusiones

En el desarrollo de este trabajo, se ha evidenciado la relevancia de contar con una infraestructura de red bien estructurada y un sistema de gestión de seguridad informática sólido para el Centro Nacional de Educación a Distancia (CENED). La implementación de estas medidas no solo protege la información sensible y garantiza la continuidad de las operaciones educativas, sino que también optimiza la eficiencia y confiabilidad del entorno virtual de aprendizaje. A través del uso de tecnologías avanzadas y buenas prácticas, el CENED se encuentra mejor preparado para enfrentar las amenazas y desafíos del entorno digital actual. Entre las lecciones aprendidas, se destaca la importancia de una planificación detallada y una ejecución precisa en cada fase del diseño y configuración de la red y los sistemas de seguridad. La selección adecuada de tecnologías y la correcta configuración de los servicios son fundamentales para maximizar tanto el rendimiento como la seguridad. Además, el mantenimiento regular y la actualización constante de los sistemas son esenciales para asegurar que el CENED continúe operando de manera eficiente y segura en el futuro. La planificación del diseño de la red y la gestión de seguridad informática para el CENED han demostrado ser pilares fundamentales para su éxito operativo. Una infraestructura bien diseñada no solo proporciona al CENED una ventaja competitiva en el ámbito educativo, sino que también refuerza su compromiso con la calidad y seguridad en la educación a distancia. Estas conclusiones subrayan la necesidad de seguir invirtiendo en medidas de seguridad y optimización de la red para mantener la posición destacada del CENED en el sector educativo.