DISEÑO DE LA SEGURIDAD DEL SISTEMA

1. Medidas de protección contra amenazas

1.1. Amenazas externas

1.1.1. Protección contra ciberataques

- **Firewall y sistemas de detección de intrusos:** Hay que implementar una serie de firewalls y de un monitoreo constante del tráfico de la red de los servidores.
- **Autenticación multifactor:** Implementar el uso de este tipo de identificación para accesos que resulten importantes y para los trabajos administrativos.
- **Cifrado de datos:** Cifrar los datos que se transmiten entre los servidores y los mismos y los clientes.
- **Pruebas de seguridad:** Evaluar periódicamente la seguridad de todos los sistemas para poder identificar y eliminar vulnerabilidades.

1.1.2. Protección contra interrupciones de red

- **Redundancia en la conexión:** Llevar a cabo la contratación de múltiples proveedores de internet y el uso de múltiples enlaces de respaldo.
- **Balanceadores de carga:** Distribución del tráfico en la red para poder evitar posibles sobrecargas en los servidores.
- **Reducción de ataques DDoS:** Utilizar servicios especializados para poder detectar y neutralizar cualquier ataque de este tipo.

1.1.3. Protección contra intrusión física

- **Control de acceso con targetas:** Aplicar el uso de targetas de proximidad para poder acceder a las salas de los servidores y así restringir el acceso a solo el personal autorizado.
- **Instalación de cámaras:** Instalar un circuito de cámaras de vigilancia trabajando continuamente en todas las áreas del CPD.
- **Guardias de seguridad:** Asegurar que se evite el acceso de personal no autorizado mediante la contratación de guardias de seguridad.

1.1.4. Protección contra desastres naturales

- **Infraestructura resistente:** Diseñar el CPD con unos materiales que sean capaces de poder resistir a las condiciones más extremas posibles.
- **Extinción de incendios:** Instalar un sistema de extinción de incendios con el que mediante el uso de gas inerte apagar el fuego sin dañar los equipos del CPD.
- **Monitoreo del ambiente:** Utilizar sensores de temperatura, humedad y detección de humo para poder saber en todo momento el estado del ambiente del CPD.

1.1.5. Protección contra cortes de energía

- **Sistema de alimentación ininterrumpida:** Garantizar el suministro eléctrico temporal en caso de apagones.
- **Generadores de respaldo:** Usar generadores de emergencia con la capacidad suficiente para mantener el CPD activo en el caso de que los sistemas de alimentación ininterrumpida no sean capaces de ello.
- **Monitoreo de voltaje y corriente:** Prevenir los daños a los equipos que se puedan producir por fluctuaciones eléctricas.

1.2. Amenazas internas

- **Capacitación de personal:** Formar de manera continua en buenas prácticas de seguridad y manejo de datos a todos los trabajadores del CPD.
- **Gestión de acceso y privilegios:** Implementar los mínimos permisos posibles a los usuarios y monitorear los accesos al sistema.
- **Supervisión de actividad interna:** Registrar y inventariar las actividades dentro de los servidores y la base de datos.
- **Seguridad en endpoints:** Instalar antivirus en todas las estaciones de trabajo y solucionar la detección de amenazas internas.

2. Políticas de seguridad de acceso a los recursos del CPD

- Acceso remoto seguro: Utilizar una VPN con cifrado y que contenga restricciones de acceso a redes que no estén autorizadas.
- Contraseñas: Utilizar contraseñas lo más seguras posibles, con cambios periódicos obligatorios cada 3 meses.
- Permisos: Asignar los menores permisos posibles a los usuarios del CPD.