Nuestra empresa en el tema de la seguridad, se basara en el sistema CIDAN, que se define por los 5 principales valores:

- **Confidencialidad** → Prohibir a cualquiera que no tenga acceso a la información, pueda interpretarla.
- **Integridad** → Garantizar que no se altere la información.
- **Disponibilidad** → Mantener operativo los sistemas todo el tiempo sin que se produzca ningún corte o caída.
- **Autenticidad** → Comprobar que quien accede a nuestros recursos este habilitado para ello.
- **No repudio** → Autentificar que la autoría de la información es correcta y no se pueda negar.

CONFIDENCIALIDAD

INTEGRIDAD

DISPOBINILIDAD

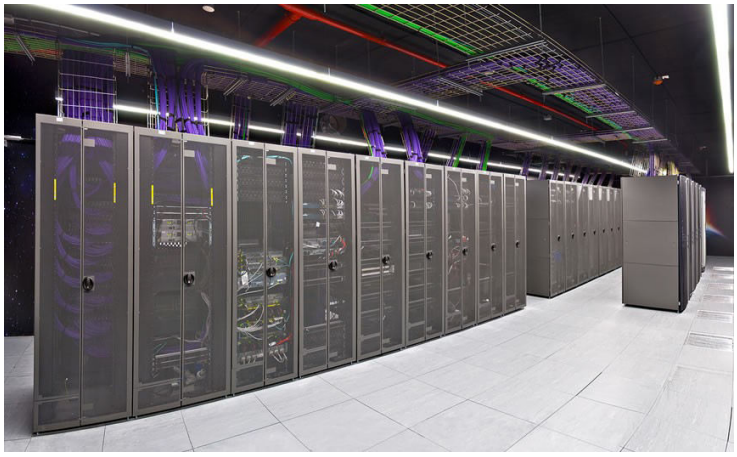
AUTENTICIDAD

NO REPUDIO

Una vez que hemos enfocado que sistema vamos a utilizar, lo siguiente sera clasificar los distintos medios que se van a utilizar.
Para ello diferenciaremos entre los dos tipos de seguridad : Seguridad Física y Seguridad Lógica.

Prohibiremos o denegaremos cualquier acceso a nuestras instalaciones, a nuestros servicios o procedimientos que ponga en riesgo a nuestra empresa.
Algunos de los medios posibles que podemos usar para proteger todo lo mencionado anteriormente pueden ser:

- Uso de guardias de seguridad para controlar el acceso a las instalaciones.
- Uso de sistemas biometricos para el acceso a lugares con contenido altamente privado(VER ANEXO SISTEMAS BIOMETRICOS).
- Centro de procesado de datos para localizar toda la información en un único punto(VER ANEXO CENTRO PROCESADO DATOS).
- Sistemas de aislamiento de los datos, bien sean SAIS o jaulas de Faraday, para que en caso de una caída de tensión o cualquier desastre natural que pase, pueda seguir funcionando como sistema secundario.



CENTRO PROCESADO DATOS

MODELOS SAIS

Seguridad Lógica

Serán el conjunto de medidas destinadas a la protección del acceso a los datos y aplicaciones informáticas, así como a garantizar el acceso a la información.
Algunos de los medios posibles que podemos usar para proteger todo lo mencionado anteriormente pueden ser:

- Políticas de contraseñas
- Políticas de almacenamiento
- Copias de seguridad
- Medios de almacenamiento

POLÍTICAS DE CONTRASEÑAS

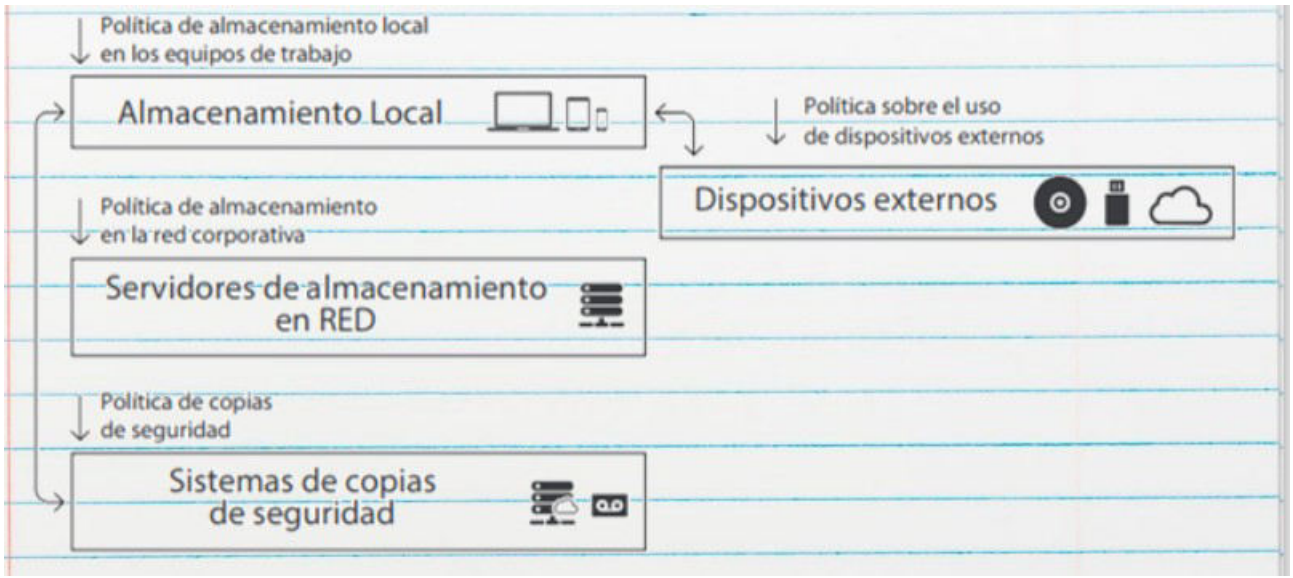
Todos nuestros equipos estarán protegidos con contraseñas altamente sofisticadas, estas seguirán el siguiente esquema:

1) Utilizar al menos 8 caracteres para crear la clave.
2) Utilizar en una misma contraseña dígitos, letras y caracteres especiales.
3) Que las letras alternen aleatoriamente mayúsculas y minúsculas.
4) Que pueda recordarse fácilmente y que pueda escribirse rápidamente.
5) Cambiarlas con una cierta regularidad.

Ademas en los equipos altamente sensibles añadiremos una capa extra mas, la cual dependerá del sistema operativo que estemos usando por ello podrá ser una contraseña en la BIOS (Sistemas Windows) o en el gestor de arranque (Sistemas GNU/Linux). (VER ANEXOS BIOS Y GRUB)

POLÍTICAS DE ALMACENAMIENTO

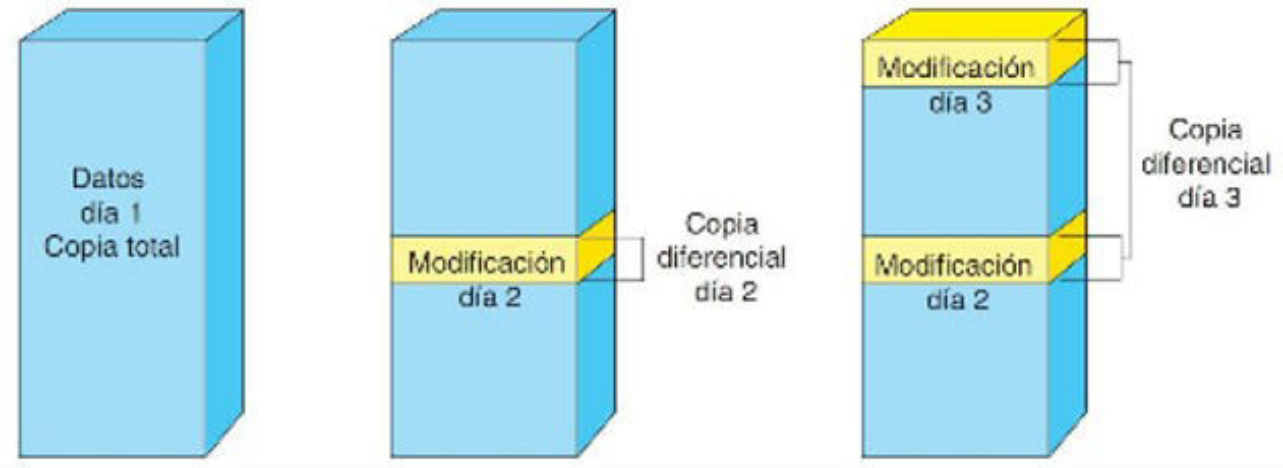
Seguiremos la siguiente normativa para saber donde se debe guardar la información:



Para darle mas seguridad a la información que almacenamos en ciertos lugares, bien sean carpetas o archivos, podemos realizar el método de encriptacion de los datos. (VER ANEXO CIFRADO)

COPIAS DE SEGURIDAD

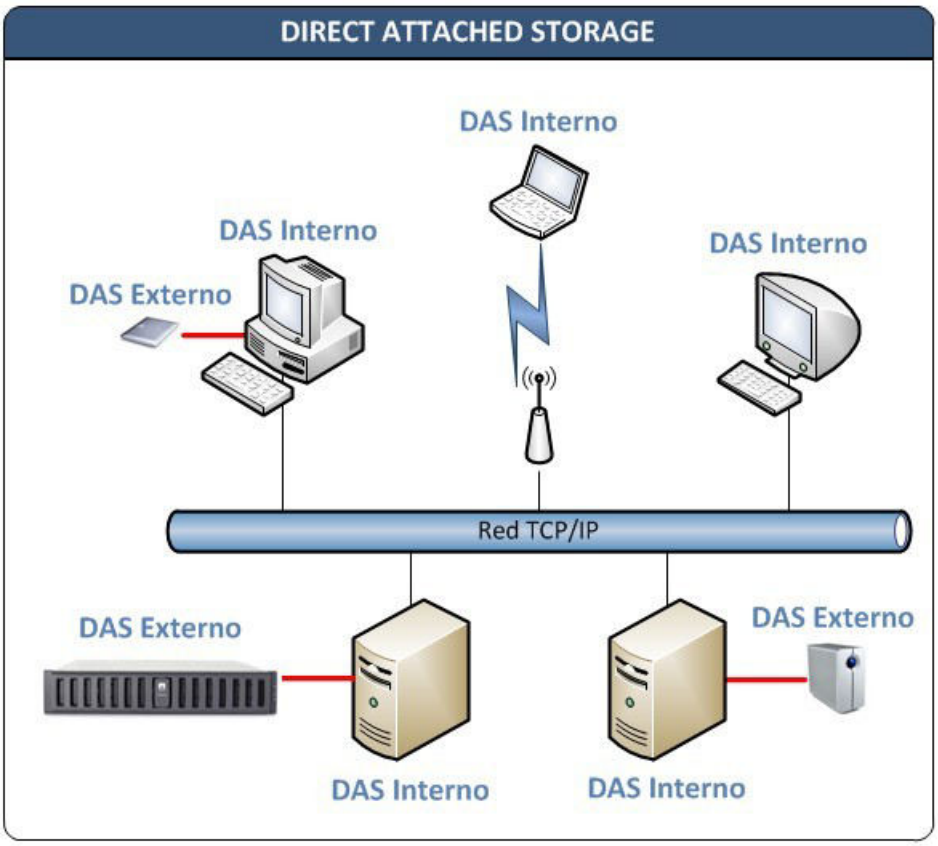
Al manipular una cantidad masiva de datos, necesitaremos realizar en periodos cortos de tiempo copias de seguridad para no perder dicha información, por ello necesitaremos un sistema basado en ello.
Utilizaremos el modelo incremental basado en copiar unicamente lo modificado desde la ultima copia de seguridad, para que a su vez, no haya una duplicación de los datos.



Para ello todos los días en una hora concreta que sera a las 23:00 se programara la copia de seguridad. (VER ANEXO COPIA SEGURIDAD WINDOWS Y ANEXO COPIA SEGURIDAD EN LINUX PARA VER EN LOS DIFERENTES SISTEMAS OPERATIVOS)

MEDIOS DE ALMACENAMIENTO

Optaremos por medios comunes, discos duros conectados a los servidores en nuestro centro de procesado de datos, por lo que usaremos el sistema DAS. El cual es la arquitectura mas tradicional de conexión entre los discos; y las ventajas mas notables son : mas barata y sencilla respecto a resto.



Una vez mencionado como vamos a trabajar, en materia de los distintos tipos de seguridad, nos enfocaremos en mecanismos que utilizaremos dentro de nuestra empresa; tales sean desde la utilización de VPN, sistemas Proxie, Firewall o el cifrado asimétrico de los datos.

Para ello nos enfocaremos en cada uno de estos aspectos, siendo fundamentales para la protección de datos personales de nuestra empresa, para actuar como primera linea de defensa frente cualquier imprevisto o ciberataque que podamos sufrir.

VPN

Denominada como Red Privada Virtual, nos permitirá a partir de una red local, propia de la empresa, extendernos a una red pública como Internet de forma segura. Siendo así que nuestros trabajadores o cualquier equipo que este conectado a ella pueda acceder sin problemas.

Lo principal que tenemos que tener en cuenta es lo siguiente:

- Todos los equipos que utilizaremos para acceder, tienen que tener acceso a cliente de la VPN.

- Solo pueden acceder los equipos dado de alta en dicha Red (Usuario y Contraseña) .

- Podemos utilizar distintos sistemas de VPN como: Punto a Punto o Remota; todo ello dependiendo de donde se utilizara el equipo.

Para adaptar este sistema nosotros lo aplicaremos tal y como se muestra en el Anexo Configuración VPN donde mostraremos como se hace paso a paso en un equipo.

PROXIE

Este software lo complementaremos con la VPN, ya que su función sera la de interceptar o bloquear ciertas direcciones URL, previamente configuradas por nosotros , que puedan impedir el acceso a sitios maliciosos o infectados. Aunque también lo podremos utilizar como un medio mas seguro de acceder a Internet, ya que nos provee un anonimato a las paginas web.

Al igual que la VPN deberemos tener en cuenta ciertos aspectos:

- Deberemos disponer de un servidor Proxie para los equipos que dispongan del Cliente Proxie.

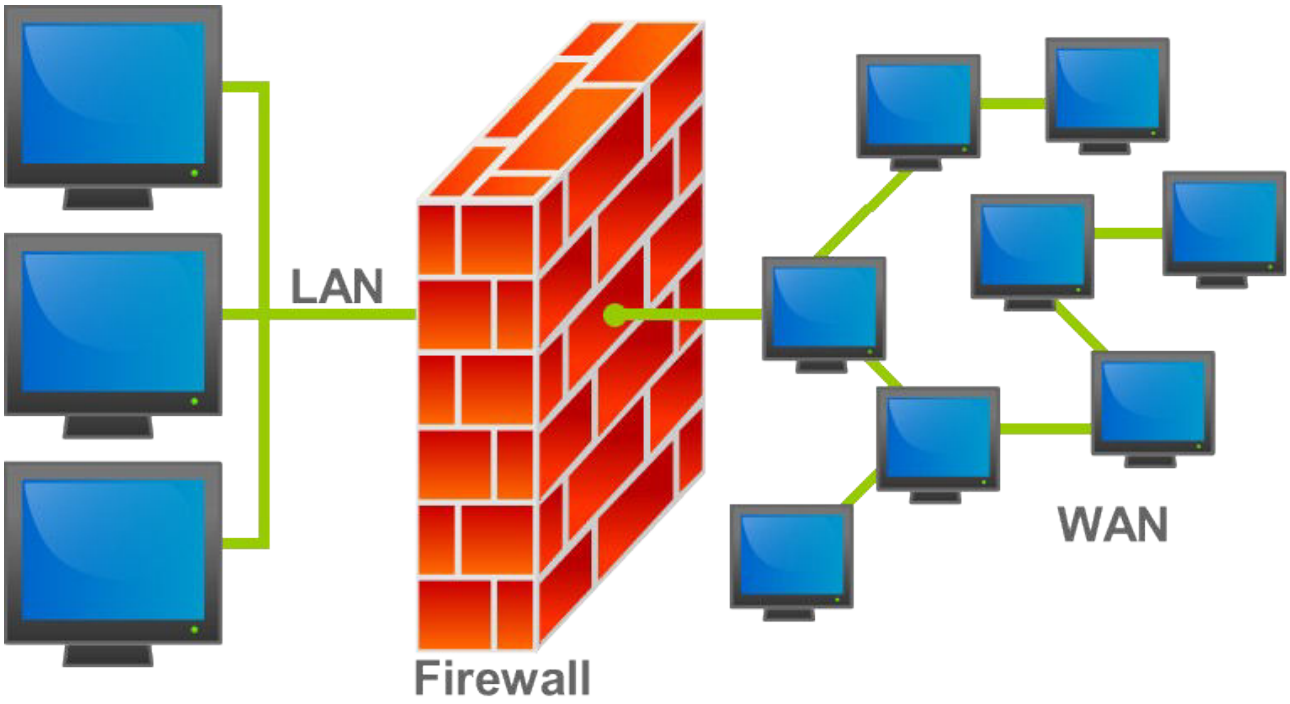
- Es muy complejo para instalar al tener que disponer de cada una de las IP de cada equipo para instalar.

Ver Anexo Proxie para ver la instalación y su configuración.

FIREWALL

Sera la aplicación que utilicemos para bloquear el acceso a las comunicaciones que no estén autorizadas; es muy parecido al Proxie salvo que su mayor diferencia es bloquear una dirección concreta, mientras que el Proxie solo era un URL, esto provoca que solo los paquetes que se acepten de dichas direcciones nos lleguen. Siendo muy útil para proteger nuestra VPN que previamente hemos mencionado.

Siendo así, que funcione como un muro para nuestra empresa frente a Internet.



Sus diferentes usos se explican en el Anexo Firewall.

CIFRADO

Este método de seguridad lo usaremos para saber que enviamos o recibimos, es tal y como fue mandado y que por el camino no haya sido modificado. Para ello utilizaremos el cifrado asimétrico que es el encargado de hacer este proceso.

Podemos usar varias herramientas de encriptacion para generar nuestras claves, ya que cada método lo hará de una forma distinta. (Ver ANEXO CRIPTOL)

El cifrado asimétrico funciona de una forma muy simple, nosotros crearemos una clave que puede ser un mensaje normal y corriente, un documento o una imagen; después esa clave se cifra y para descifrarla necesitaremos una clave privada que previamente nosotros poseeremos y así poder descifrar el mensaje que nos ha llegado. (VER ANEXOS MAILVELOPE Y CIFRADO ASIMETRICO)