TRABAJO DE INVESTIGACIÓN: DISEÑANDO UNA RED

Trabajo de Alejandro Sainz Sainz

SISTEMAS INFORMÁTICOS 24-25

INTRODUCCIÓN 3

DESCRIPCIÓN **¡Error! Marcador no definido.**

TOPOLOGÍA HÍBRIDA **¡Error! Marcador no definido.**

VENTAJAS Y DESVENTAJAS **¡Error! Marcador no definido.**

EJEMPLOS DE USO REAL **¡Error! Marcador no definido.**

CONCLUSIÓN Y REFLEXIÓN 3

BIBLIOGRAFIA Y ENLACES 15

TABLA DE FIGURAS

[1 Tipología hibrida: Anillo más árbol **¡Error! Marcador no definido.**](#_Toc194560660)

[2 Las variables son casi ilimitadas **¡Error! Marcador no definido.**](#_Toc194560661)

# INTRODUCCIÓN

En este trabajo nos vamos a dedicar a diseñar una red, más o menos para unas 20 o 30 personas. Para realizar esto nos vamos a centrar en detallar minuciosamente y paso a paso todos los aspectos, desde el comienzo, para llevar esta empresa a buen término. Cuando me refiero a esta empresa y todos sus pasos, hablamos de la selección de servidores, protocolos, medidas de seguridad, políticas de usuarios y otra serie de aspectos que intentaré detallar lo más posible, aunque quizá en algunos de ellos pasemos un tanto por encima, ya sea porque quizá reflejen un aspecto más secundario de esta tarea o, que también es muy posible, por falta de conocimientos sobre un determinado campo o por su dificultad para reflejarlos con mis propias palabras de una forma sencilla y fácilmente entendible.

Hay que tener en cuenta que intentaremos cubrir los pasos a diseñar y crear esta red, pero al no tener determinado el sector y gremio al que va a dirigida puede que algunos aspectos sólo se refieran como posibles o dependientes de que se cumpliesen una serie de condiciones. Estas pueden ir desde trabajadores móviles o deslocalizados, a aquellos que trabajan en remoto, la necesidad o no de servicios a través de una página web o si esta está simplemente pensada para darnos a conocer. Todas esas variables hacen que, de darse o no, tuviésemos la necesidad de implementar unas soluciones u otras, teniendo que dar información del cómo, el por qué y la manera en la que podrían ser relevantes estas cuestiones.

Intentaré también, de ser posible y relevante para el tema, ir enlazando todo con algunos otros de los temas que hemos ido viendo a lo largo de nuestra andadura, ya que algunas de estas cuestiones pueden volver a resultar útiles dentro de esta práctica y creo que podrían complementarla bastante bien.

Otro de los objetivos es reflejar la importancia sobre ciertas políticas, sobre todo en temas de seguridad ya que, a nivel empresarial, se ha convertido en un aspecto de máxima importancia, eso sí, siempre y cuando estén justificadas y no supongan un gasto y un despliegue superficial y sin sentido alguno. Hay que tratar siempre que cada acción importe y sume, de que cada funcionalidad en una red tenga un propósito, ya que en sistemas que quizá puedan ser muy limitados o que se necesite que sean más escuetos, habrá funcionalidades que no aporten y que sean más un lastre o un ligero impedimento.

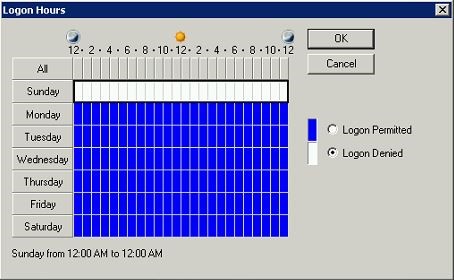
Ahora ya, sin nada más que añadir, vamos a comenzar con este trabajo.

# USUARIOS, DIRECTIVA, PERFILES Y SEGURIDAD

Lo primero que voy a comentar aquí, que me parece básico y que es lo primero a tener en cuenta, es que esta me parece la parte más frágil de la cadena y doy mis motivos.

Podemos tener la mejor seguridad del mundo, firewall y servidores cuánticos, routers con 100 capas de seguridad y políticas extremadamente seguras y complejas, que incluso con todos eso, un usuario va a conseguir, y de seguro de forma involuntaria, encontrar más vulnerabilidades y fallos que muchos técnicos en seguridad. Y eso no es de chiste, es que yo también en alguno de mis trabajos, he sido un usuario de sistema y me he tropezado con casos en los que sabiendo lo que hacía, y otros de forma involuntarias, acabas tocando algo que casca el sistema.

¿Por qué digo esto? Fácil, para justificar el motivo que me impulsa a escribir lo que viene a continuación.

Las políticas en torno a los usuarios, su interacción con el sistema y la libertad que tengan durante su uso, salvo en casos especiales que se necesite otra cosa, deben de ser lo más restrictivas posibles. [](https://www.manageengine.com/latam/active-directory-audit/kb/how-to/como-configurar-las-horas-de-inicio-de-sesion-en-active-directory.html)

GESTOR DE HORARIOS DE ACTIVE DIRECTORY

<https://www.manageengine.com/latam/active-directory-audit/kb/how-to/como-configurar-las-horas-de-inicio-de-sesion-en-active-directory.html>

A que me refiero con más restrictivas. A qué se deben de limitar lo más posible las acciones de los usuarios para evitar esos problemas que puedan surgir.

Como vemos en la imagen anterior (Gestor de horarios de conexión de Active Directory) podemos incluso limitar las horas en las que un equipo, ya sea identificado por IP o MAC, se conecta contra el servidor, es decir, comienza su sesión identificándose en el server.

Ahora bien, lo que estamos trabajando aquí es una empresa ficticia, de unas 30 personas, de la cual no sabemos su actividad ni el régimen de funcionamiento que tiene. Así que vamos a comenzar desde el principio intentando evaluar todas las opciones posibles.

Como tipos de perfil de usuario yo siempre optaría por perfiles obligatorios, que no puedan ser modificados por los usuarios. A estos se les van a asignar zonas de almacenamiento que posiblemente no estén ubicadas físicamente en su equipo, así que lo que no vamos a dejar es que modifiquen bajo ningún concepto el perfil de usuario. Ahora bien, existen tipos de actividad y departamentos o tareas que requieran de ciertas modificaciones las cuales no podemos permitir que el grupo de IT, en caso de que lo haya, esté pendiente de hacerlas cada vez que un usuario lo necesite. Imaginemos que nos dedicamos al desarrollo, como en el módulo que estudiamos. Descargar plugins, IDEs, dependencias y un largo etcétera. Vamos a tener que permitir que los usuarios modifiquen su sesión, sus archivos, que toquen su almacenamiento. No podemos tener perfiles obligatorios para ellos, ya que su actividad puede requerir de muchos cambios que no podemos modificar cada dos por tres. Por otra parte, en casos en el que sean trabajos más repetitivos y estáticos podemos hacer el perfil totalmente inmutable.

Luego siempre hay que tener en cuenta que quizá una empresa pueda contar con trabajadores que se muevan, comerciales, vendedores, servicios técnicos a otras empresas, personas que realizan su trabajo en remoto por el motivo que sea. En esos casos es más que seguro que deberemos tener la posibilidad de habilitar perfiles móviles, que puedan ser ejecutados en diferentes dispositivos y quizá con una libertad de horarios mucho más amplia.

[](https://images.ecestaticos.com/hNzgpu-pQQs-Tm8_Ksu3R3RVDdk=/0x0:1000x750/996x747/filters:fill(white):format(jpg)/f.elconfidencial.com%2Foriginal%2F8d5%2Fa6b%2F4d1%2F8d5a6b4d1ca972753ff6e55729dfe37c.jpg)

HAY ALGUNOS QUE EL TELETRABAJO LO LLEVAN A OTRO NIVEL

<https://images.ecestaticos.com/hNzgpu-pQQs-Tm8_Ksu3R3RVDdk=/0x0:1000x750/996x747/filters:fill(white):format(jpg)/f.elconfidencial.com%2Foriginal%2F8d5%2Fa6b%2F4d1%2F8d5a6b4d1ca972753ff6e55729dfe37c.jpg>

Todo va a depender de los tipos de actividad que llevemos a cabo en nuestra empresa. Luego de seguro tendremos perfiles especiales, ya sean jefes u otro tipo de cargos, con los que habrá que tener más manga ancha.

Pero, en conclusión, yo por mi parte, restrictivo a más no poder, siempre que eso no interfiera con la naturaleza propia de nuestra actividad.

Después de esto, si hablamos de permisos, de nuevo hay que ser restrictivo. Cada perfil de usuario debe de ir asociado a un grupo, dependiendo del departamento y dentro de su actividad en el mismo. Pueden existir trabajadores que, dentro de un departamento en concreto, tengan ciertas atribuciones o responsabilidades que requieran de permisos distintos con respecto a determinados archivos o recursos. Intentaremos siempre que los permisos de ejecución y de escritura estén perfectamente acotados a un directorio, un grupo de ficheros o un recurso en concreto, eliminando estos permisos del resto del sistema, para que no puedan interferir con otros grupos y sus recursos asociados ni con aquellas partes propias del sistema que sólo deberían de ser manipuladas por el departamento de TI.

Por poner algún ejemplo en concreto, aunque va a quedar algo vago, podríamos tener un departamento de desarrollo cuyos permisos van a estar localizados en los archivos compartidos o en la parte de almacenamiento propio de ese departamento. Allí pueden crear sus propios archivos, editarlos y ejecutarlos. Por el contrario, perderán esos permisos en otras zonas del sistema, en aquellas pertenecientes o propias de otros departamentos. No deberán de tener posibilidad de escritura y ejecución en zonas como por ejemplo Marketing, o ventas, ya ni hablar de dirección o recursos humanos. Y sólo deberían de tener permisos de lectura en ciertas zonas o archivos que no supongan un riesgo o cuya lectura no suponga ningún problema.

Evidentemente el único grupo que debe de tener acceso a todos estos permisos son los técnicos, aunque también deben de tener sus limitaciones. A nadie le gustaría que, mientras realizan tareas de mantenimiento, borren archivos propios de otro usuario. Por lo tanto, no deberían de poder modificar esos archivos. Moverlos quizá, leerlos por su puesto, sobre todo por el hecho de que puedan necesitar verificar el contenido de algunos archivos.

En conclusión, mediante el uso correcto de permisos y de almacenaje compartidos, debemos acotar de forma precisa el ámbito de actuación de cada grupo y cada usuario dentro del propio sistema, dándole cierta libertad sólo en ciertas zonas y en lo referente a recursos propios y que son imprescindibles para su trabajo. En el resto de zonas o secciones, las acciones de ese usuario no deberían de tener ningún impacto. Cada grupo o usuario sólo debe de ser consciente de su propia actividad y de aquellas que estén relacionadas con él, del resto, si no es consciente, mucho mejor. Y es con esa mentalidad con la que creo que debemos de preparar los permisos y los perfiles.

# POLÍTICAS DE CONTRASEÑAS Y CONTRASEÑAS

En cuanto a contraseñas tendremos que exigir unos mínimos de longitud y complejidad. Que se deban de cambiar con regularidad, cada dos o tres meses, pero sin ser molesto. Con un máximo de intentos erróneos de conexión, entre tres y cinco me parece un buen número.

Luego ya todo está en manos de los usuarios. Donde apuntan o guardan sus contraseñas, si las comparten o no, si usan las mismas dos o tres contraseñas en bucle cada vez que toca modificarlas. A este tipo de cosas también me refería al hablar del eslabón más débil de la cadena.

Con las contraseñas puede pasar cualquier cosa. Que la tengas en un post-it pegada a la pantalla del ordenador, que uses 1234 y al siguiente cambio sea 4321, que un día, que a todos nos puede pasar, te obceques o te ofusques y rebases el número máximo de intentos permitidos simplemente porque colocaste mal los dedos en el teclado o porque te confundiste con la contraseña que utilizabas el mes pasado.

[](https://www3.gobiernodecanarias.org/educacion/cau_ce/servicios/web/sites/www3.gobiernodecanarias.org.educacion.cau_ce.servicios.web/files/inline-images/img1_conlogo.png)

USANDO CONTRASEÑAS SEGURAS

<https://www3.gobiernodecanarias.org/educacion/cau_ce/servicios/web/sites/www3.gobiernodecanarias.org.educacion.cau_ce.servicios.web/files/inline-images/img1_conlogo.png>

En cuanto al resto de políticas de las cuentas, otra vez lo mismo. Hay que intentar ser restrictivo, en la medida de lo posible. Suena a tirano, pero eso ayuda a prevenir cierto tipo de errores y de situaciones que en un ámbito empresarial y de trabajo pueden ser molestas y su resolución se puede convertir en un dolor de cabeza.

Una vez un trabajador cesa su actividad en la empresa, ya sea de forma permanente o temporal, la medida mínima es deshabilitar su cuenta, luego en determinados casos lo más seguro y lo propio será eliminar de forma permanente esa cuenta y ese perfil de usuario.

En cuanto a las auditorías de seguridad y de sistema, hablando de las experiencias propias en otras empresas, no he visto tantas ni con tanta seguridad. Pero si bien es cierto que deben de ser realizadas, aunque en mi opinión, si tenemos un buen sistema de logs, un buen sistema de seguimiento y la monitorización de eventos podemos espaciar más las auditorias de seguridad, quizá cada año y medio y dos años. Todo ello depende de que bien hayamos preparado todo en un inicio. De todas formas el uso diario de los sistemas hará que vayan apareciendo nuevas situaciones o problemáticas, además de que se tendrán que realizar actualizaciones de software e incluso hardware que puedan cambiar las dinámicas de nuestro trabajo y el funcionamiento de nuestro sistema, por lo que en esos momentos tendremos que realizar nuevas auditorías de seguridad para verificar que los cambios no dan lugar a nuevos problemas o brechas de seguridad que puedan suponer problemas a posteriori o traer de vuelta problemas que considerábamos resueltos.

En este apartado lo que considero más básico es el sentido común para todo y el no querer obviar aspectos que, por obtener una mayor comodidad o flexibilidad, a la larga nos supongan un problema y una carga extra de trabajo que nos podemos ahorrar con unas buenas prácticas básicas. Con esto me refiero a no exigir una determinada complejidad en las contraseñas por hacerlo más fácil a los usuarios, o que sólo se les solicite cambiarlas un mínimo número de veces al año, véase 1 o 2. A veces se nos puede hacer tedioso el tener que llevar a cabo estas tareas que se nos hacen molestas, pero que a la larga pueden hacer nuestro día a día más llevadera y segura en el ámbito del trabajo.

Hay que tener en cuenta en todo esto que somos como somos, por comodidad somos incapaces de pasar un pequeño aprendiendo algo nuevo o realizando una pequeña tarea que no nos supone mucho esfuerzo. Pero en este caso, con estas normas hay que intentar ser lo más estricto posible.

# SERVIDORES

# CONCLUSIÓN Y REFLEXIÓN

En esta pequeña práctica, aunque ficticia, hemos visto, y seguiremos viendo en un futuro si nos encontramos con algo parecido, de lo delicada y minuciosa que puede llegar a ser desarrollar una red. En este caso, dado que nos centrábamos en una red pequeña, nos hemos tenido que plantear gran cantidad de cuestiones, buscar las respuestas y, como ya he mencionado en otros trabajos, navegar por inmensos agujeros negros de información, conocimiento y especificaciones técnicas relativas a todo este ámbito.

Desde elegir una topología de red hasta definir políticas de seguridad, nos damos cuenta de que cada parte de todo el proceso puede ser crítica, puesto que la elección, independientemente de que sea la más o menos optima, de cualquier variable puede afectar a todas las demás.

Podríamos diseñar un complejo sistema que funcione como un reloj, pero en caso de no ser escalable y encontrarnos luego con esa necesidad hace que ya no nos sirva para nuestro propósito. La elección de un sistema operativo o una serie de aplicaciones cuyo soporte no es bueno o no es de una duración larga y que cubra nuestras expectativas puede llevarnos a tener que cambiarlo todo en poco tiempo, lo que de nuevo puede invalidar nuestras elecciones.

Cosas como esta nos dan una idea de lo frágiles que pueden ser estos sistemas ante los cambios y que de forma permanente tendremos que trabajar sobre el mismo, modificando, mejorando y actualizando todo nuestro sistema.

Este pequeño caso, aunque no hayamos entrado en detalles muy concretos y técnicos, nos da una idea de lo titánico y masivo que se puede volver cuando se diseñan redes muy grandes, del tipo MAN o superiores. La cantidad de variables que entran en juego y que hay que tener en cuenta son muchas: segmentar una red, uso de VPNs, tipos de firewalls, como configurarlos, el hardware necesario y un largo etcétera de otras preguntas y variables.

# BIBLIOGRAFIA Y ENLACES

<https://www.genbeta.com/web/son-los-ataques-ddos-efectivos-como-medio-de-protesta>

<https://ultahost.com/blog/es/una-guia-completa-y-comparacion-de-tcp-y-udp/>

<https://es.wikipedia.org/wiki/Anexo:Puertos_de_red#Puertos_bien_conocidos>

<https://www.fortinet.com/lat/resources/cyberglossary/what-is-port-scan>