

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **CÓDIGO CERTIFICADO:** | | | FC9-09/2020/4730CPP | | | **CODIGO INTERNO CAM:** | | FC/20/6704 | |
| **ACCION:** | 5 | | | **GRUPO** | | 100 | | | |
| **NOMBRE CERTIFICADO:** | | | | IFCT0109- SEGURIDAD INFORMATICA | | | | | |
| **MÓDULO:** | | MF0486\_3 SEGURIDAD EN EQUIPOS INFORMÁTICOS | | | | | | | |
| **CENTRO DE FORMACIÓN/ENTIDAD:** | | | | | Core Networks, SL | | **CENSO:** | | 27.593 |

PRUEBA PRÁCTICA

|  |  |
| --- | --- |
| Nombre y apellidos: Diego Armando Simbaña | |
| NIF: 02562559Z | Fecha: 26/05/2021 |
| Firma: | |

**EXAMEN PRÁCTICO**

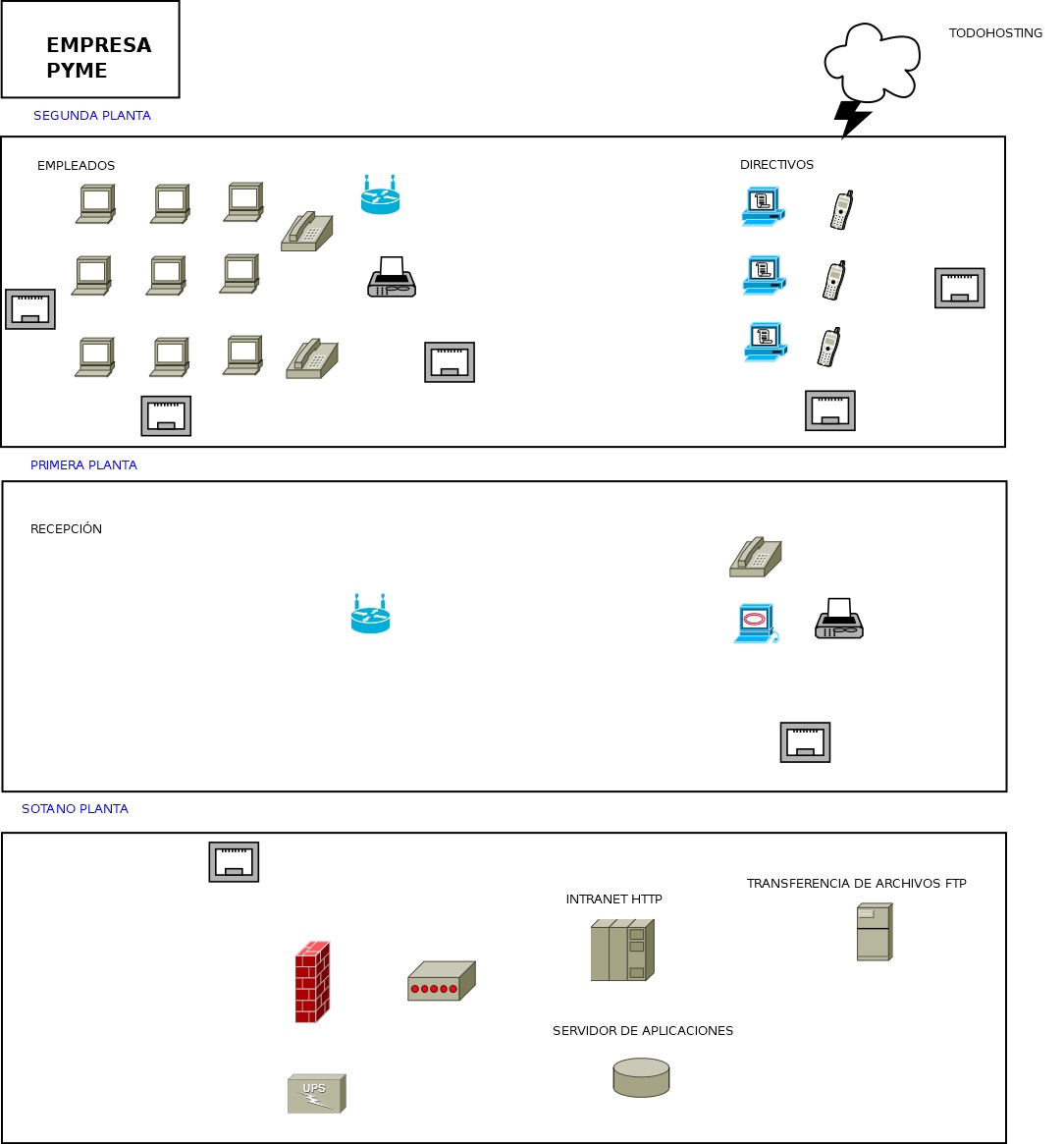
Los directivos de una empresa han aprobado un plan de implantación de “Buenas Prácticas”.

Esta empresa tiene las siguientes características:

* PYME de 13 empleados, cada uno de ellos con su propio ordenador
  + 2 auxiliares administrativos
  + 6 técnicos
  + 2 comerciales
  + 1 director de ventas
  + 1 director operativo
  + 1 director jefe
* Lugar de trabajo
  + Edificio de 3 plantas con la siguiente distribución:
    - Sótano
    - Primera planta recepción
    - Segunda planta zona de trabajo común de los empleados
    - Despachos de los directivos
* Disponen de un servidor que realiza los servicios a la empresa:
  + Intranet (HTTP)
  + Transferencia de archivos (FTP)
  + Aplicación centralizada de ventas (HTTP-Tomcat)
  + Características del servidor
    - Windows server
    - IIS (Internet Information Server)
* Además, tienen acceso a Internet y el correo electrónico se realiza a través del proveedor de servicios de Internet “TODOHOSTING”

**Analizar un plan de implantación**

1. **Determinar los sistemas implicados en la implantación**.
   * Realiza un esquema donde se muestre todos los sistemas que están implicados en la PYME, donde quede detallado: Servicios implicados, puestos informáticos, redes



1. **Analizar los requisitos de seguridad de cada sistema.**
   * Leyendo el plan de implantación que se ha aprobado
     1. ¿Qué sistemas se ven afectados?
        + *Ordenadores personales y servidores*
     2. Realiza un pequeño resumen de los requisitos de seguridad que deben cumplir cada uno de los sistemas que se han analizado en la empresa.
        + *Muchos de nuestros activos, mobiliario, ordenadores, etc., y en particular la información y sus sistemas de almacenamiento y tratamiento, son realmente críticos para nuestra actividad diaria. Estos sistemas, sin los cuales no podríamos desempeñar nuestras funciones, están sujetos a amenazas como virus, login incorrecto, intrusión de externos…*
        + *La divulgación no autorizada de información confidencial, o el no establecimiento de una política correcta en cuanto al control de acceso se refiere, puede acarrear daños importantes para la empresa.*
        + *La empresa debe mantener un ambiente protegido de trabajo que garantice su eficiente funcionamiento; cada uno de nosotros tiene un papel importante para hacer esto posible, por lo que todo el personal debe poner de su parte y mantener una actitud positiva, que encamine a la entidad a lograr sus fines en materia de seguridad de la información.*
        + *Todo esto hace imprescindible marcar una normativa sobre el correcto uso de los equipos y sistemas de información que la empresa pone a disposición de los trabajadores, tanto internos como externos, para que puedan realizar eficazmente su trabajo diario. Esta normativa es de obligado cumplimiento para todo el personal durante la totalidad de su vida laboral en la empresa, desde que se produce su registro inicial como nuevo usuario, hasta su baja como trabajador en caso de que se produzca.*
        + *Para garantizar el cumplimiento de lo establecido en este documento, la empresa realizará auditorias internas periódicas. Estas auditorias, aparte de necesarias, forman parte de las comprobaciones a las que obliga la Ley a las entidades para garantizar la confidencialidad y protección de la información bajo su responsabilidad, reservándose la empresa el derecho de tomar las medidas disciplinarias correspondientes en caso de detectar incumplimiento por parte de los trabajadores.*
2. **Describir las medidas de seguridad a aplicar a cada sistema**
   * Leyendo el plan de implantación que se ha aprobado
     1. ¿Cuáles son las medidas de seguridad que se van a implantar?

*ACCESO AL SISTEMA INFORMÁTICO*

*Identificación y Autenticación*

*Control de Acceso.*

*Servidores Corporativos*

*Puesto de Trabajo*

*Contraseñas*

*Imagen Corporativa*

* + 1. Realiza un pequeño resumen de cada una de ellas.

ACCESO AL SISTEMA INFORMÁTICO

Identificación y Autenticación

*Control de Acceso.*

*Este apartado hace referencia a las medidas y recomendaciones que deben tener en cuenta los usuarios del sistema para intentar garantizar la confidencialidad de la información a la que tienen acceso.*

*Servidores Corporativos*

*A cada usuario autorizado del sistema le son asignados unos permisos de acceso a la información almacenada en los servidores corporativos; estos accesos serán definidos por los Responsables de Proyecto, conjuntamente con el Responsable de Gestión Interna y el Departamento de Sistemas, que es el encargado de aportar la visión técnica de la implementación del esquema de permisos común a todos los Departamentos.*

*Puesto de Trabajo*

*Tan importante o más que el tipo de contraseña seleccionada, es el cuidado que se tenga respecto a la confidencialidad de la misma, y de la información a la que cada usuario tiene acceso.*

*Contraseñas*

*Como vimos en el apartado anterior, cada usuario es responsable de la confidencialidad de su contraseña de acceso, por lo que se prohíbe su comunicación o cesión a cualquier otra persona, incluidos compañeros y superiores.*

*Imagen Corporativa*

*Como todos sabemos, la empresas recibe numerosas visitas, tanto Institucionales como de empresas privadas, por lo que el cuidado de la imagen corporativa supone un objetivo prioritario para la empresa.*

*ACCESO A INTERNET Y CORREO ELECTRÓNICO*

*Es obligado dar ejemplo en el buen uso de los medios tecnológicos, y que tanto los trabajadores de la empresa, como aquellos pertenecientes a empresas externas que realicen algún proyecto o servicio en las instalaciones de la empresa (en adelante usuarios del sistema) promuevan y acaten el código ético que se describe a continuación:*

*• Todos los usuarios del sistema que dispongan de PC con conexión a Internet deben usar solamente el software legal y autorizado por la empresa.*

*• la empresa dispone, para protección de los sistemas informáticos, de un cortafuego (firewall) entre la red interna e Internet. Ningún usuario, puede ‘saltarse’ este elemento de seguridad, usando módems o cualquier otro mecanismo que evite pasar por el cortafuegos.*

*• Algunos sitios de Internet han sido bloqueados por los administradores del sistema. Si realmente se necesita acceder a una página Web determinada por razones de trabajo, el usuario del sistema debe enviar un correo electrónico al Responsable de Gestión Interna, con copia a su responsable de área correspondiente, solicitando dicho acceso y esgrimiendo las razones pertinentes.*

*• Todos los accesos a Internet están monitorizados mediante el software XXXXX . Todos los usuarios del sistema que dispongan de PC con acceso a Internet a través de la red corporativa deben usar únicamente el software legal y autorizado por la empresa, y navegar respetando siempre el firewall instalado.*

*Uso Responsable de Internet*

*Es norma de la empresa confiar en los usuarios de su red corporativa; inherente a esta confianza va ligada la expectativa de que cada usuario actuará de forma responsable, aunque a modo de ayuda, ofrecemos las siguientes directrices para un uso responsable de la conexión a Internet.*

*• Los navegadores están configurados para usar nuestro Proxy, y ningún usuario del sistema está autorizado a modificar los parámetros.*

*• Queda totalmente prohibido navegar o visitar páginas que contengan material ofensivo.*

*• Está prohibido transmitir o recibir material de tipo obsceno, pornográfico, racial o acoso sexual. A todos los usuarios del sistema que utilizan Internet se les hace saber que los navegadores dejan huellas de las visitas a las páginas Web.*

*• Todos los ficheros descargados de Internet deben ser escaneados por el antivirus y en caso de duda se debe informar inmediatamente al Departamento de Sistemas.*

*• Queda prohibido el uso de programas como ‘Messenger’, descargar o escuchar en línea música o emisoras de radio, así como ver vídeos o TV en línea, ya que*

*consumen gran ancho de banda del circuito de datos e interfieren en la operativa de la empresas.*

*• Todo el software de acceso a Internet debe ser aprobado por el RGI y el Departamento de Sistemas, el cual es el único responsable de las actualizaciones del software.*

*• Cuando se tenga que introducir datos en un formulario de una página en Internet, asegúrese que sea una página segura o que tenga algún mecanismo de encriptación antes de enviar los datos a través del navegador. Para ello compruebe que la página dispone de un ‘Certificado de Autenticidad’ emitido por una entidad autorizada.*

*• Todos los accesos a las páginas de Internet deben ser por motivos relacionados con el trabajo.*

*• Todos los datos almacenados en la red de la empresa son propiedad de la empresa, que se reserva el derecho de inspeccionarlos y restringirlos o evitar su transferencia a redes externas.*

*• Los usuarios del sistema no podrán incluir a la empresa en ninguna red externa sin autorización previa.*

*• La utilización del correo electrónico corporativo ‘@laempresa.xx’ deberá ceñirse en exclusividad a fines profesionales, no estando permitido en ningún caso usos distintos de estos.*

*• No se debe enviar ninguna información de tipo confidencial a través de Internet, a menos que el receptor esté expresamente autorizado por la empresa para recibir el material, y dicho material esté protegido de una exposición no autorizada mientras se encuentra en tránsito.*

*• Todas las materias de carácter no confidencial que se envíen por Internet deben ser de naturaleza profesional y cumplir con la normativa de la empresa respecto a publicación de materiales (Departamento de Relaciones Externas).*

*• Todas las materias de carácter no confidencial que se envíen por Internet deben cumplir con las leyes de derechos de autor en el momento de la transferencia (es decir, con la jurisdicción de derechos de autor tanto de la red interna como externa).*

*• Los usuarios del sistema deben intentar cumplir una ética profesional ante un determinado servicio en un foro externo, actuando de forma que no pongan en entredicho la reputación de la empresa.*

*• Los usuarios del sistema que importen información de una fuente externa deben estar autorizados por el propietario de dicha información para recibirla o copiarla.*

*• Los usuarios del sistema que importen información de una fuente externa deben comprobar el material importado (en un contexto aislado), por si tuviera virus ocultos, y deben tener la precaución de no activar los virus importados de forma que los sistemas de las redes internas queden expuestos a ellos.*

*Detección de Actividades Sospechosas*

*Todo el personal, durante de la ejecución de sus funciones en la empresa, debe estar atento a sucesos inesperados, poco comunes, contrarios a las directrices especificadas por la organización en sus procedimientos de trabajo y/o contrarios a la cultura de empresa. A continuación se indican algunos ejemplos de posibles incidencias de seguridad:*

*• Extravío o robo de equipamiento con información corporativa.*

*• Evidencia o sospecha de alteración de permisos de acceso de usuarios.*

*• Comportamientos anómalos en los sistemas de información.*

*• Configuraciones desconocidas en los sistemas de información.*

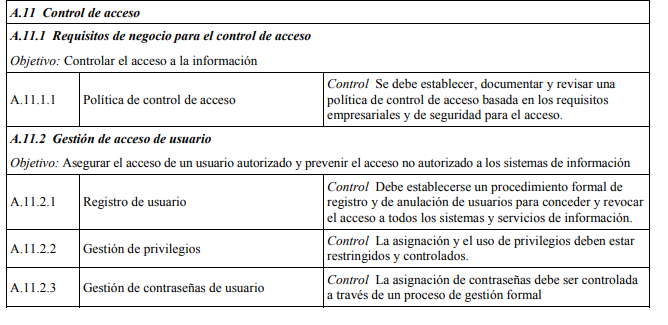
*• Evidencia o sospecha de acceso o modificación no autorizada de información.*

*• Hallazgo de información en ubicaciones no designadas para ello.*

1. **Cumplimentar los formularios para la declaración de ficheros de datos de carácter personal.**
   * Nos han encargado rellenar el formulario NOTA de un **Fichero de Titularidad Privada** con los siguientes datos:
     1. Tipo de solicitud: Alta
     2. Modelo de declaración: Normal
     3. Presentación de la documentación: Internet
     4. Rellena los datos sabiendo:
        + El responsable del fichero es el director de operaciones
        + Solo se va a almacenar información de identificación de clientes
        + Y los datos se van a tratar de forma automatizada
        + No se va a realizar transferencias internacionales

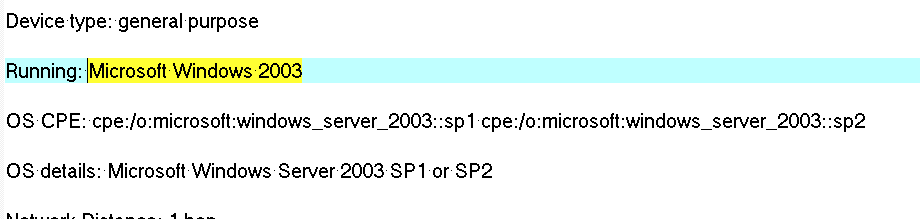
**Implantación de un servidor**

1. **Determinar la ubicación física del servidor para asegurar su funcionalidad**.
   * El servidor ahora se encuentra en la planta de recepción:
     1. ¿Crees que deberíamos trasladar de ubicación el servidor?
        + *Si, se debería mover debido a que se encuentra muy expuesto.*
        + *También por temas de ruido, aire acondicionado, UPS, cableado, rack, acceso restringido.*
     2. Si decides trasladarlo, ¿qué es lo mínimo que necesita para que siga funcionado como servidor?
        + *Conexión a la red, router y un ISP.*
2. **Describir y justificar las medidas de seguridad física a implementar que garanticen la integridad del sistema**
   * Describe una serie de medidas de seguridad física que implantarías en el servidor
     1. *Implantaría, cámaras de seguridad, puertas, barras de seguridad, protección anti incendios acceso con algún sistema autorización y control de acceso (tarjeta, llaves, acceso biométrico, etc ) en la entrada y acceso a servidores y racks, sistema de aire acondicionado, SAI, detectores de intrusos, alarmas, personal de seguridad.*
3. **Identificar los módulos o aplicaciones adicionales para implementar el nivel de seguridad requerido por el servidor**
   * Describe una serie de programas para mejorar la seguridad lógica del servidor
     1. *Firewall, proxy, cifrar comunicaciones, usuarios autenticados, antivirus, política de grupos GPOs, buenas practicas de ciberseguridad e informática, monitoreo, VPN, copias de seguridad.*
     2. *Implantación de políticas, normas de seguridad OSI, UNE, BOE.*
4. **Determinar las amenazas a las que se expone el servidor, evaluando el riesgo que suponen, dado el contexto del servidor**
   * Sino implementamos esas medidas de seguridad física y lógica, describe las amenazas a las que estamos expuesto (diferencia seguridad lógica / física)
     1. *FÍSICA*
        + *Acceso no autorizado a personal externo.*
        + *Perdida de información por falta de acondicionamiento del lugar físico de la empresa.*
        + *Falta de un plan de prevención y contramedidas en caso de emergencia.*
     2. *LÓGICA*
        + *Robo de información por personas no autenticadas.*
        + *Suplantación de información.*
        + *Virus, malware, hackeo, ingeniería social.*
        + *No seguir la normativa y legislación vigente en seguridad de la información, multas, sanciones.*
        + *Fallo en la integridad de los datos.*
5. **Determinar los permisos asignados a los usuarios y grupo de usuarios para la utilización del sistema**
   * Nombra algún control de la ISO27001 relacionado con los permisos/privilegios para mejorar la seguridad los sistemas.

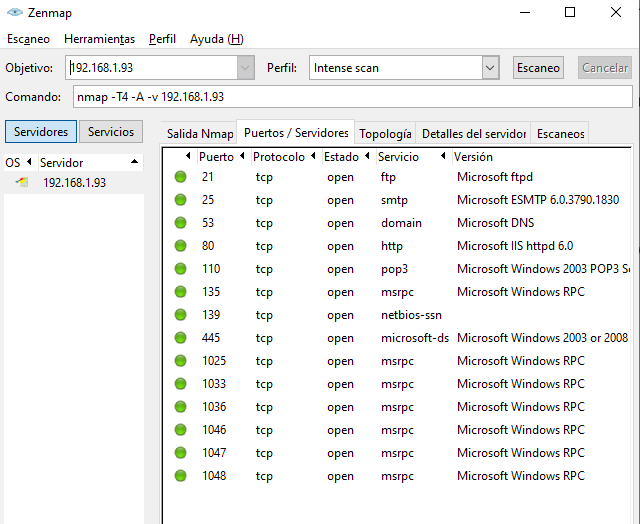


**Servicios del servidor**

1. Indicar las relaciones existentes entre dicho servidor y el resto del sistema informático de la organización.
   * Realiza un esquema de los servicios que se realiza en el servidor con un equipo genérico, detallando:
     1. Tipo de servicio
        + Sevidor web HTTP
        + Transferencia de archivos FTP
        + Servidor de aplicaciones HTTP-Tomcat
     2. Puerto por el que se realiza
        + 80/443
        + 20-21/22
        + 8080
2. Extraer del plan de implantación los requisitos de seguridad aplicables al servidor
   * Enumera los requisitos de seguridad que afectan al servidor del plan de implantación.
     1. A cada usuario autorizado del sistema le son asignados unos permisos de acceso a la información almacenada en los servidores corporativos; estos accesos serán definidos por los Responsables de Proyecto, conjuntamente con el Responsable de Gestión Interna y el Departamento de Sistemas, que es el encargado de aportar la visión técnica de la implementación del esquema de permisos común a todos los Departamentos. Estos permisos le serán comunicados al usuario en el momento de su incorporación, y posteriormente en caso de sufrir alguna modificación. Queda expresamente prohibido trabajar con archivos corporativos altamente confidenciales fuera del servidor de ficheros, así como eliminar o copiar información de dicho servidor, ya sea al disco duro local de los ordenadores corporativos o a un dispositivo de almacenamiento externo, incluyendo USBs, DVDs o cualquier otro soporte, salvo autorización previa del Responsable de Gestión Interna.1 En caso de que por algún motivo se considere necesario realizar alguna de estas acciones se debe informar previamente al Responsable de Departamento / Proyecto correspondiente, que a su vez solicitará la autorización del Responsable de Gestión Interna. Estas solicitudes se realizarán a través del apartado de peticiones de la herramienta de gestión de peticiones. Esta política se establece, entre otras cosas, por el propio beneficio de los trabajadores, ya que el Departamento de Sistemas de la entidad realiza copias de seguridad diarias de la información almacenada en los servidores, susceptible de recuperación en cualquier momento, lo que no sucede en el caso de la información almacenada en el disco duro.
3. Determina los servicios mínimos necesarios para el funcionamiento del sistema
   * La dirección del servidor es: 192.168.1.66
     1. ¿Qué programa utilizas para ello?
        + Nmap o cualquier otro programa de escaneo de puertos.
     2. Realiza un escaneo intensivo de esa dirección IP
        + ¿Qué plataforma es? ¿está actualizada?



* + - * Puertos que tiene abiertos junto con los servicios asociados



* + 1. De todos los servicios que tiene, ¿cuáles son los mínimos necesarios para que funcione el sistema?

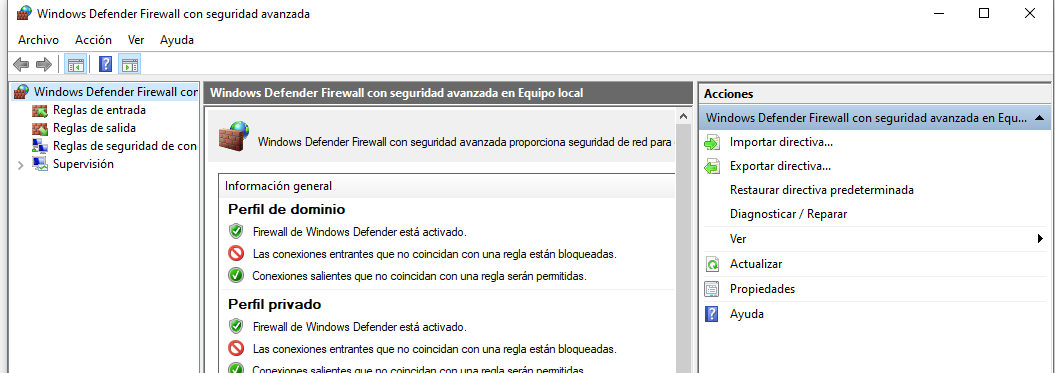
Son esto:

* 1. Intranet (HTTP) 80
  2. Transferencia de archivos (FTP) 21
  3. Correo (POP3) 110
  4. MW2003 (Microsoft ds) 445
  5. Correo (SMTP) 25

**Firewall**

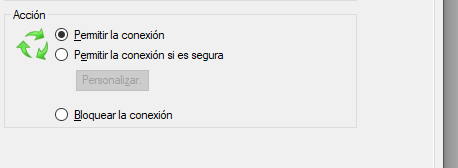
1. Nos llegan los siguientes incidentes debido a la implantación de seguridad en la organización:
   1. “No puedo acceder a internet desde el navegador OPERA (aplicación)”
      1. Realiza un manual de proceso de habilitación de esa aplicación si consideramos que es el Firewall el que está bloqueando la aplicación

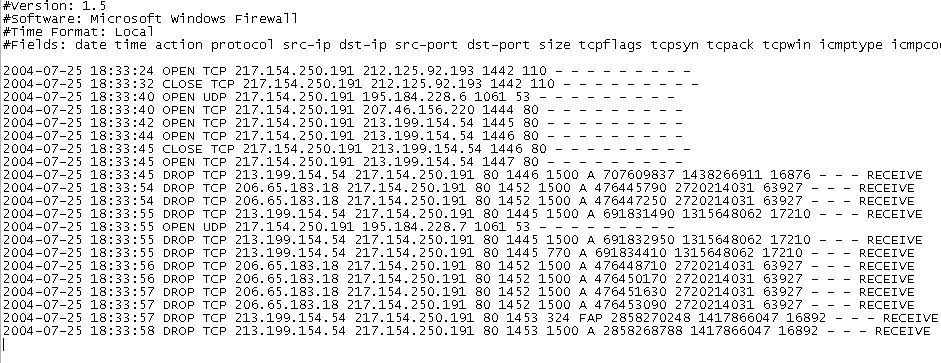
1. Abri firewall

2. Buscar en reglas de entrada y salida la aplicación.

3. Botón derecho habilitar o deshabilitar regla.

4. Si esta habilitado comprobar en propiedades si permite la conexión o no.

1. Comprobamos las pestañas de protocolos y puertos, el ámbito, etc si todo es correcto.
2. Si la regla no existe hay que crearla siguiendo todos los pasos que te muestra el asistente.
3. Cerramos y comprobamos que hay conexión a Internet con nuestra aplicación.
   1. “No puedo acceder al FTP del servidor, uso el Filezilla”
      1. Realiza un manual de proceso de habilitación de esa aplicación si consideramos que es el Firewall el que está bloqueando la aplicación
         * De igual forma si nuestra aplicación no funciona adecuadamente.
         * Abrimos o ejecutamos windows + R escribimos “firewall.cpl”
         * Nos abrirá una ventana del panel de control del firewall
         * Comprobamos tanto en reglas de entrada y salida nuestra aplicación si esta permitida para realizar conexiónes.
         * Si todo es correcto añadimos otra regla permitiendo el puerto 20/21.
         * Comprobamos “preguntamos” que el servidor tiene habilitado tal servicio así como el firewall del propio servidor tiene abierto el puerto 21 de ftp.
         * Volvemos a ejecutar nuestro Filezilla y comprobamos que si hay comunicación con nuestro servidor.
   2. “Quiero acceder por VPN a mi ordenador”
      1. Realiza un manual donde expliques sólo lo que necesita y opciones del firewall que necesitamos configurar
         * Tendremos que habilitar/crear la vpn en nuestro ordenador.
         * Habilitar los puertos en nuestro router.
         * Habilitar una regla de entrada y salida vpn en el firewall de nuestro ordenador.
         * Habilitar las conexión remota en nuestro equipo.
         * Ejecutar Una conexión remota con un cliente para su comprobación.
         * Y ya podrías acceder al equipo por VPN.
   3. Nos llega este fichero de logs del firewall del servidor
      1. Haz una tabla con 4 registros y los campos:
         * Fecha – Puerto – acción – ip origen – ip destino



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Fecha** | **Puerto** | **Acción** | **Ip O** | **Ip D** |
| 25/07/04 | tcp | open | 217.154.250.191 | 212.125.92.193 |
| 25/07/04 | tcp | close | 217.154.250.191 | 212.125.92.193 |
| 25/07/04 | udp | open | 217.154.250.191 | 195.184.228.6 |
| 25/07/04 | tcp | open | 217.154.250.191 | 207.46.156.220 |