DESCRIPCIÓN DE MEDIDAS DE SEGURIDAD PARA SERVIDORES UBICACIÓN

- Los servidores implicados deben estar identificados en su alojamiento físico, CPD

- Todos los sistemas de información deben encontrarse en una sala cerrada denominada CPD.

- El CPD debe cumplir con una serie de normas de seguridad como son:

    Acceso al Edificio controlado por sistema de videovigilancia

    Acceso al CPD controlado mediante claves personales

    Sistema de detección de incendios

    Sistemas y equipos de comunicaciones conectados a SAI y a Grupo Electrógeno

    Sala refrigerada todo el año.

- Todos los empleados que deban acceder a la ubicación de los sistemas, poseen un código numérico/tarjeta de acceso personal que deben introducir en los sistemas de apertura de puertas del CPD.

- Los soportes con las copias de seguridad de los sistemas de información se encuentran bien en el CPD (para las copias del día en cuestión) o guardados, por los Técnicos autorizados, en un "armario ignífugo" bajo llave fuera del CPD.

- No se permite la utilización de soportes del tipo CD, DVD, llaves USB, etc. en los servidores ubicados en el CPD. Solo cierto personal técnico autorizado puede tener acceso a los sistemas de información y a los ficheros y todos los empleados deberán firmar una Acuerdo de Confidencialidad, secreto y responsabilidad para el tratamiento de ficheros de datos personales.

COMUNICACIONES

- La conexión con el CPD se realizará de forma segura utilizando la siguiente infraestructura:

    Línea ADSL con Internet conectada a servidor de túneles y Firewall o

    Línea ATM simétrica con Internet conectada a servidor de túneles y Firewall.

IDENTIFICACIÓN Y AUTENTIFICACIÓN EN LOS SERVIDORES:

- Se establece que todos los usuarios que tengan acceso a los sistemas lo deben realizar mediante un "Login" y un "Password" personal e intransferible. El primero sirve para identificar al usuario cuando acceda al sistema de información y el segundo permite la autenticación del mismo ante el sistema.

- El "Login" es único y es asignado por los Administradores de los sistemas está formado por una cadena de caracteres.

- El "password", que se almacena de forma cifrada (de modo que son ininteligibles) en los sistemas, es elegido por cada usuario y puede estar formado por una combinación de letras y/o números con una longitud mínima de 8 caracteres.

- Es obligatorio el cambio de la contraseña con una periodicidad de 180 días.

- La contraseña varía con cada renovación, no permitiéndose la práctica de mantener un juego de contraseñas utilizándolas de forma cíclica.

- El sistema de seguridad sólo permite la recuperación de las contraseñas al RESPONSABLE DE SEGURIDAD o a la persona designada por el, siendo el usuario el único responsable de su memorización. En el caso de olvido es necesario solicitar al Responsable de seguridad o a la persona designada por el, una contraseña nueva inmediatamente que sustituirá a la anterior.

- Las contraseñas se almacenan de forma encriptada en el sistema, de modo que ni siquiera los Administradores pueden saberlas.

- El sistema bloquea el acceso de un usuario cuando se introduce la contraseña erróneamente durante 3 ó 5 intentos. El bloqueo consistirá, en bloquear la estación de trabajo, pudiendo ser desbloqueada la máquina exclusivamente por el responsable de seguridad.

En todo caso, se registrará el intento de acceso no autorizado por el sistema de seguridad.

- Cada vez que se crea un nuevo perfil de usuario o cada vez que un usuario ha olvidado su contraseña, los Administradores de los sistemas establecen una clave idéntica al nombre de usuario y obligan al usuario a cambiarla, siguiendo todos los patrones mencionados anteriormente, en el primer inicio de sesión. En caso de que no la cambien en ese momento, no se les permite el acceso.

CONTROL ACCESO LÓGICO

- Existirá una Política de control de los accesos a los sistemas de información que cubre todos los puntos de acceso de la red de modo que cada acceso es personalizado e inequívoco y cada perfil de acceso es definido y atribuido con respecto a la actividad de cada usuario.

- Cada perfil de usuario tendrá asignado un tipo de usuario en función de sus responsabilidades, una serie de autorizaciones que serán estándares para cada perfil y una serie de autorizaciones especiales que puedan ser necesarias. Todas las características que debe tener un perfil de usuario son asignadas por los Administradores del Sistema.

GESTIÓN DE SOPORTES

- Respecto a los datos, habrá implementada una política de copias de seguridad a cintas / pen / Hdd externos con un ciclado semanal, de modo que diariamente se realizarán copias en distintos soportes magnéticos, los cuales son guardados en “armarios ignífugos” y tal que siempre hay una copia de la semana en otro edificio distinto al del CPD.