Imagen que contiene nombre de la empresa

Descripción generada automáticamente

**Asignatura: Desarrollo de Sistemas  
  
Trabajo Práctico:” Pregunta 22 –** **Política de red.”  
  
Profesor: Osvaldo Pérez  
  
Alumna:** **María Candelaria Slobodiamsky Clariá  
  
Fecha de entrega: 10/6/2022  
  
Curso: 6to 3ra  
  
Turno: Mañana  
  
Año: 2022**

**Pregunta:**

¿Como se debe diseñar una Política de Red?

**Respuesta:**

Para diseñar una política de red, hay que seleccionar un procedimiento de creación de cuentas de usuario que sea él más sencillo y fácil de entender, asegurando menos errores y que sea más probable que lo sigan los administradores del sistema; debe tener una política para seleccionar la contraseña inicial siendo está muy débil, y evite establecer la contraseña inicial como una función del nombre de usuario, o parte de este, o alguna contraseña generada por un algoritmo que pueda adivinarse con facilidad. La selección de la contraseña inicial no debe ser tan obvia.  
Tambien error muy común es permitir que los usuarios sigan usando su contraseña inicial en forma indefinida por lo que muchos sistemas cuentan con una política de caducidad de contraseñas, lo cual termina siendo útil para protegerlas de posibles vulneraciones que pudiesen llegar a ocurrir en algún momento.

La política de seguridad de la red debe definir los derechos y las responsabilidades de los usuarios que utilizan los recursos y servicios de la red siendo los siguientes posibles de modificar al gusto que usted (programador) desee poseer:

* Lineamientos acerca del uso de los recursos de red, tales como que los usuarios estén restringidos.
* Que constituye un abuso en términos de usar recursos de red y afectar el desempeño del sistema y de la red.
* Está o no permitido que los usuarios compartan cuentas o permitan a otros usar la suya.
* Pueden o no los usuarios revelar su contraseña en forma temporal, para permitir que otros que trabajen en un proyecto tengan acceso a sus cuentas.
* Política de contraseña de usuario: con qué frecuencia deben cambiar de contraseña los usuarios y que otras restricciones o requerimientos hay al respecto.
* Los usuarios son responsables de hacer respaldos de sus datos o es esto responsabilidad del administrador del sistema.
* Consecuencias para los usuarios que divulguen información que pueda estar patentada. Que acciones legales u otros castigos pueden implantarse.
* Una declaración sobre la privacidad del correo electrónico.
* Una política respecto a correo o publicaciones controversiales en las listas de correo o grupos de discusión.
* Una política sobre comunicaciones electrónicas, tales como falsificación de correo.

Las organizaciones deben establecer políticas que no se limiten a correo electrónico, sino que también abarque otros medios, como discos, cintas y documentos impresos, habiendo 5 criterios para evaluarlos:

* ¿La política cumple con la ley y con las obligaciones hacia otras empresas?
* La política compromete innecesariamente los intereses del empleado, del patrón o de otras empresas.
* ¿La política es funcional, práctica y de posible cumplimiento?
* La política aborda apropiadamente todas las formas de comunicación y mantenimiento de archivo en la oficina.
* ¿La política fue anunciada por anticipado y aceptada por todos los interesados?

El administrador del sistema necesita recabar información del directorio privado de un usuario para diagnosticar problemas del sistema mientras que los usuarios, por otra parte, tienen el derecho de conservar su privacidad, habiendo aquí una contradicción entre ambas, cuando se presente algún tipo de amenaza de seguridad de red, el administrador del sistema tendrá mayor necesidad de recabar información de los archivos, incluidos los del directorio base de los usuarios. La política de seguridad de la red debe especificar el grado al que el administrador del sistema pueda examinar los directorios y archivos privados de los usuarios para diagnosticar problemas del sistema e investigar violaciones de la seguridad. Si la seguridad de la red está en riesgo, la política debe permitir mayor flexibilidad para que el administrador corrija los problemas de seguridad, teniendo ciertas opciones para lo nombrado:

* Puede el administrador revisar o leer los archivos de un usuario por alguna razón.
* Los administradores de la red tienen el derecho de examinar el tráfico de la red o del host.
* Cuáles son las responsabilidades legales de los usuarios, los administradores del sistema y de la organización por tener acceso no autorizado a los datos privados de otras personas.

Tambien se debe determinar qué tipo de datos delicados pueden almacenarse en un sistema específico.  
Para darle a un usuario acceso a un servicio de un host, se debe considerar que otros servicios e información se proporcionan y a los cuales el usuario podrá tener acceso, también pensar si existe una seguridad adecuada en el sistema para proteger la información delicada. Para evitar esto, la política debe de tener en cuenta el hecho de que se le necesita decir/comentar a los usuarios que podrán guardar información delicada que servicios son apropiados para el almacenamiento de dichos datos y no en otros.