CONTROL DE ACCESOS

INTRODUCCIÓN Y ANTECEDENTES

Las empresas día con día se enfrentan a la necesidad de saber quién entra y sale de sus instalaciones, por lo que un Sistema de Control de Accesos es la herramienta ideal para la administracion integral de sus accesos y el incremento de la seguridad de sus instalaciones, activos y personal.

Los equipos suelen formar parte de una red de equipos. Una red permite que los equipos conectados intercambien información. Los equipos conectados a la red pueden acceder a datos y demás recursos de otros equipos de la red. Las redes de equipos crean un entorno informático potente y sofisticado. Sin embargo, las redes complican la seguridad de los equipos.

Por ejemplo, dentro de una red de equipos, los sistemas individuales permiten el uso compartido de información. El acceso no autorizado es un riesgo de seguridad. Debido a que muchas personas tienen acceso a una red, el acceso no autorizado es más probable, especialmente como consecuencia de errores del usuario. Un mal uso de contraseñas también puede originar el acceso no autorizado lo que puede implicar perdida de información o falsificación de identidad.

La seguridad de red, generalmente, se basa en la limitación o el bloqueo de operaciones de sistemas remotos.

OBJETIVOS

Impedir el acceso no autorizado a los servicios en red dentro de nuestra empresa y tener un mejor control de que usuarios están en nuestra red y que es la información que genera cada uno de ellos, así como también saber qué tipo de información revisan, a que páginas web entran y lo más importante saber que documentos entran y salen de dicha red.

Se deberían controlar los accesos a servicios internos y externos conectados en red.

El acceso de los usuarios a redes y servicios en red no debería comprometer la seguridad de los servicios en red si se garantizan:

a) que existen interfaces adecuadas entre la red de la Organización y las redes públicas o privadas de otras organizaciones;

b) que los mecanismos de autenticación adecuados se aplican a los usuarios y equipos;

c) el cumplimiento del control de los accesos de los usuarios a los servicios de información.

Algunos consejos que puede seguir para mejorar el control de acceso, puede llevar estadísticas de cortafuegos, tales como porcentaje de paquetes o sesiones salientes que han sido bloqueadas (p. ej., intentos de acceso a páginas web prohibidas; número de ataques potenciales de hacking repelidos, clasificados en insignificantes/preocupantes/críticos).

Requisitos de negocio para el control de accesos.

*Controlar los accesos a la información.

Se deberían controlar los accesos a la información, los recursos de tratamiento de la información y los procesos de negocio en base a las necesidades de seguridad y de negocio de la Organización.

Las regulaciones para el control de los accesos deberían considerar las políticas de distribución de la información y de autorizaciones.

*Política de control de accesos

Las políticas son las que otorgan a los usuarios acceso al sitio. A menos que estén autorizados a ejercer sus responsabilidades mediante una o varias políticas de control de acceso, los usuarios no tienen acceso a funciones del sitio.

Elementos de una política de control de acceso
Una política de control de acceso se compone de cuatro elementos:

Las cuatro partes de una política de control de acceso

Grupo de acceso
El grupo de usuarios al que se aplica la política.

Grupo de acciones
Un grupo de acciones que el usuario realiza en los recursos.

Grupo de recursos
Los recursos controlados por la política. Un grupo de recursos puede incluir objetos de negocio como, por ejemplo, contrato o pedido, o bien un conjunto de mandatos relacionados. Por ejemplo, todos los mandatos que los usuarios de un determinado rol pueden realizar.

Relación
Opcional: cada clase de recurso puede tener asociado un conjunto de relaciones. Cada recurso puede tener un conjunto de usuarios que satisfacen cada relación. Por ejemplo, una política puede especificar que sólo el creador de un pedido pueda modificarlo. En este caso, la relación sería la de creador y es entre el usuario y el recurso de pedido.

Estas cuatro partes juntas definen una política especificando los usuarios, las acciones que éstos pueden realizar, el objeto de negocio o el conjunto de mandatos en los que se efectúan las acciones y, opcionalmente, la relación que los usuarios tienen con el grupo de recursos.

Las políticas de control de acceso otorgan a los usuarios acceso al sitio. A menos que estén autorizados a ejercer sus responsabilidades mediante una o varias políticas de control de acceso, los usuarios no tienen acceso a funciones del sitio.

*Control de acceso a las redes y servicios asociados.

El objetivo es impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.

Los medios deberían ser controlados y físicamente protegidos.

Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas.

Asegure los soportes y la información en tránsito no solo físico sino electrónico (a través de las redes). Cifre todos los datos sensibles o valiosos antes de ser transportados.

Gestión de acceso de usuario

Objetivo

El objetivo es el de garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.

Se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información.

Los procedimientos deberían cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información.

Se debería prestar especial atención, si fuera oportuno, a la necesidad de controlar la asignación de permisos de acceso con privilegios que se salten y anulen la eficacia de los controles del sistema.

Actividades de control del riesgo

- Gestión de altas/bajas en el registro de usuarios: Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.

- Gestión de los derechos de acceso asignados a usuarios: Se debería de implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.

- Gestión de los derechos de acceso con privilegios especiales: La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.

- Gestión de información confidencial de autenticación de usuarios: La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.

- Revisión de los derechos de acceso de los usuarios: Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.

- Retirada o adaptación de los derechos de acceso: Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.

Control de acceso a sistemas y aplicaciones

Los medios deberían ser controlados y físicamente protegidos.

Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas.

Asegure los soportes y la información en tránsito no solo físico sino electrónico (a través de las redes). Cifre todos los datos sensibles o valiosos antes de ser transportados.

Actividades de control del riesgo

- Restricción del acceso a la información: Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.

- Procedimientos seguros de inicio de sesión: Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de inicio de sesión.

- Gestión de contraseñas de usuario: Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad.

- Uso de herramientas de administración de sistemas: El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas deberían estar restringidos y estrechamente controlados.

- Control de acceso al código fuente de los programas: Se debería restringir el acceso al código fuente de las aplicaciones software.