SEGURIDAD LOGICA

La seguridad lógica se refiere a la seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información. La “seguridad lógica” involucra todas aquellas medidas establecidas para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información. Los principales objetivos que persigue la seguridad lógica son:

* Restringir el acceso a los programas y archivos
* Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.

Las amenazas lógicas.

Las amenazas de un sistema informático pueden provenir desde un hacker remoto que entra en nuestro sistema desde un troyano, pasando por un programa descargando de forma gratuita que nos ayuda a gestionar nuestras fotos pero que supone una puerta trasera a nuestro sistema permitiendo la entrada a espías hasta la entrada no deseada al sistema mediante una contraseña de bajo nivel de seguridad.

Amenazas lógicas pueden ser:

Personal: la persona de la organización incluso a la persona ajena a la estructura informática, puede comprometer la seguridad de los equipos, es el que provoca más destrozos y el más peligroso de todos.

Ex-empleados: generalmente se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema del que conocen perfectamente, pueden insertar troyanos, bombas lógicas, virus o simplemente conectarse al sistema como si aún trabajaran en la organización o conocen sus accesos, son muy peligrosos.

Hackers, Crackers o similar: una persona ajena que intenta tener acceso no autorizado a los recursos de la red con intención maliciosa aunque no siempre tiende a ser esa su finalidad.

Puertas traseras: durante el desarrollo de aplicaciones grandes o sistemas operativos es habitual que entre los programadores insertar atajos en los sistemas habituales de autenticación del programa o núcleo de sistema que se está diseñando.

Malware: como virus, gusanos o Caballos de troya.

Software incorrecto, sin ser malware hay errores en la ejecución del software que pueden comprometer nuestra seguridad.

Controles de Acceso

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Cada usuario debe tener un identificador único e inequívoco. Debemos reconocer cada usuario por su código. El sistema de identificación debe ser único, exclusivo y confidencial.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina "single login" o sincronización de passwords. La identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.

Identificación hace referencia al uso de un código y contraseña o biometría para identificar al usuario en el sistema, autenticación es el proceso de validación de esa cuenta. Todo lo visto en seguridad física relativo a la biometría también es aplicable a la seguridad lógica. Es recomendable reforzar la seguridad de la contraseña haciéndola compleja y con caducidad.

Una de las técnicas más habituales para implementar esta única autenticación de usuarios sería la utilización de un servidor de autenticaciones sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder. Este servidor de autenticaciones puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas.

El control de acceso puede ser interno o externo. Interno es cuando se identifica dentro de la propia organización a través de la red local. El acceso interno está reforzado por control de acceso físico. Externo es cuando la identificación se realiza a través de una red pública (internet). El acceso externo debe ser restringido mientras sea posible y usar herramientas que refuercen la seguridad: acceso con VPN, uso de firewalls, DMZs o servidores en la nube.

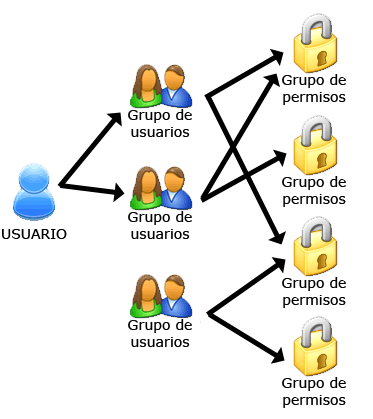
Gestión de usuarios

Cada usuario debe tener un código único y claramente identificativo. La clave de acceso de cada usuario debe ser privada, reforzada por documento de confidencialidad y de una mínima complejidad para evitar el ataque fuerza bruta. Administración del proceso de gestión de usuarios:

* Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios.
* Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos.
* Detección de actividades no autorizadas. Además de realizar auditorías o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas.
* Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado.
* Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando "bombas lógicas" o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente. Para evitar estas situaciones, es recomendable anular los permisos de acceso a las personas que se desvincularán de la organización, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación.

Grupos o roles

Se deben tantos o roles como haya en la organización y asignar permisos a los roles, nunca a los usuarios. Los permisos siempre son en positivo, concediendo el permiso correspondiente al rol (o grupo) que lo necesite. El permiso de no-acceso solo debe usarse para penalizar un usuario en concreto.



Ubicación y Horario

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana. De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

Encriptación

La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso.