CONTROL DE ACCESO A LAS APLICACIONES

Requisitos de negocio para el control de acceso

Su objetivo es limitar el acceso a la información y a los recursos de procesamiento de la información.

Política de control de acceso

Se debería establecer, documentar y revisar una política de control de acceso basada en los requisitos del negocio y de la seguridad de la información.

Los propietarios de los activos deberían determinar las reglas de control de acceso apropiadas, los derechos de acceso y las restricciones para las funciones específicas de los usuarios, con respecto a sus activos con el nivel de detalle y el rigor de los controles que reflejan los riesgos asociados de seguridad de la información.

Los controles de acceso son tanto lógicos como físicos y éstos deberían considerarse en forma conjunta. Los usuarios y los proveedores de servicio, deberían proveerse de una declaración clara de los requisitos de negocio que deberían cumplir para los controles de acceso.

La política debería tomar en cuenta lo siguiente:

a) requisitos de seguridad de aplicaciones de negocio;

b) políticas para autorización y distribución de la información, por ejemplo, el principio de la necesidad de saber y los niveles de seguridad de la información y clasificación de la información;

c) coherencia entre los derechos de acceso y las políticas de clasificación de la información de los diferentes sistemas y redes;

d) legislación pertinente y obligaciones contractuales con respecto a la limitación de acceso a los datos o servicios

e) gestión de derechos de acceso en un ambiente distribuido y de redes que reconozca todos los tipos de conexión disponibles;

f) segregación de roles de control de acceso, por ejemplo, solicitud de acceso, autorización de acceso, administración de acceso;

g) requisitos para autorizaciones formales de solicitudes de acceso;

h) requisitos para revisión periódica de derechos de acceso;

i) eliminación de derechos de acceso;

j) archivo de los registros de todos los eventos importantes relativos al uso y a la gestión de las identidades del usuario y la información de autenticación secreta;

k) roles con acceso privilegiado.

Debería tenerse cuidado cuando se están especificando las reglas de control de acceso considerando:

a) estableciendo reglas basadas sobre la premisa “Todo está generalmente prohibido salvo que expresamente sea permitido” más que sobre la regla más débil “Todo está generalmente permitido salvo que sea expresamente prohibido”;

b) cambios en las etiquetas de la información que son propiciados automáticamente por los recursos de procesamiento de información y aquellos que son propiciados a discreción de un usuario;

c) cambios en los permisos de usuario que son propiciados automáticamente por el sistema de información y aquellos que son propiciados por un administrador;

d) reglas que requieren una aprobación específica antes de habilitarse y aquellas que no lo requieren.

Las reglas de control de acceso deberían ser soportadas por procedimientos formales y responsabilidades definidas.

El control de acceso basado en roles es un enfoque utilizado exitosamente por muchas organizaciones para vincular los derechos de acceso con los roles de negocios.

Dos de los principios frecuentes que dirigen la política del control de acceso son:

a) necesidad de saber: solo se le concede el acceso a la información que necesita para realizar sus tareas (diferentes tareas/roles significan necesidades de saber diferentes y, por lo tanto, perfil de acceso diferente);

b) necesidad de utilizar: solo se les concede el acceso a los recursos de procesamiento de información (equipos de TI, aplicaciones, procedimientos, recintos) que necesita para llevar a cabo su tarea/trabajo/rol.

Acceso a las redes y a los servicios de red
Los usuarios solamente deberían contar con acceso a las redes y servicios de red para los que han sido específicamente autorizados a usar.

Debería formularse una política relativa al uso de redes y servicios de red. Esta política debería cubrir:

a) las redes y servicios de red a los cuales es permitido acceder;

b) los procedimientos de autorización para determinar a quién se le permite el acceso a qué redes y a qué servicios en red;

c) los controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red;

d) los medios utilizados para acceder a las redes y servicios de red (por ejemplo, el uso de VPN o redes inalámbricas).

e) los requisitos de autenticación del usuario para acceder a varios servicios de red;

f) seguimiento del uso de los servicios de red.

La política sobre el uso de servicios de red debería ser coherente con la política de control de acceso de la organización.

Conexiones no autorizadas o inseguras a servicios de red pueden afectar a toda la organización. Este control es particularmente importante para conexiones de red a aplicaciones sensibles o críticas del negocio o de usuarios en ubicaciones de alto riesgo, por ejemplo, áreas públicas o externas que están fuera de la gestión y control de seguridad de la información de la organización.

Gestión del acceso de usuarios

Su objetivo es asegurar el acceso autorizado de los usuarios y evitar el acceso no autorizado a los sistemas y servicios.

Registro y cancelación de usuarios

Se debería implementar un proceso formal de registro y de cancelación de usuarios para habilitar la asignación de derechos de acceso.

El proceso de gestión de identificación (ID) de usuarios debería incluir:

a) la utilización de una ID única de usuario para hacer que los usuarios queden vinculados y sean responsables de sus acciones; el uso de IDs compartidas debería permitirse solamente cuando sea necesario por razones de negocio u operativas, y debería ser aprobado y documentado;

b) la desactivación o eliminación inmediata de los IDs de los usuarios que han dejado la organización;

c) la identificación y eliminación o desactivación periódica de IDs de usuarios redundantes;

d) asegurarse de que las IDs de usuarios redundantes no se otorguen a otros usuarios.

Proporcionar o revocar el acceso a la información o a los recursos de procesamiento de información es, por lo general, un procedimiento de dos pasos:

a) asignar y habilitar, o revocar el ID de usuario;

b) proporcionar o revocar los derechos de acceso a dicho ID de usuario.

Aprovisionamiento de acceso a usuarios

Debería implementarse un proceso formal para aprovisionar de acceso a los usuarios con el fin de asignar o revocar derechos de acceso para todos los tipos de usuario a todos los sistemas y servicios.

El proceso de aprovisionamiento para asignar o revocar los derechos de acceso concedidos al ID de usuario debería incluir:

a) la obtención de la autorización del propietario del sistema o servicio de información para el uso del sistema o servicio de información; la aprobación por separado de los derechos de acceso por la administración también puede ser apropiada;

b) la verificación de que el nivel de acceso concedido sea adecuado a las políticas de acceso y sea coherente con otros requisitos, tales como la segregación de funciones;

c) el aseguramiento de que los derechos de acceso no sean activados (por ejemplo, por los proveedores del servicio) antes de que se completen los procedimientos de autorización;

d) el mantenimiento de un registro central de los derechos de acceso concedidos a un ID de usuario para acceder a los sistemas y servicios de información;

e) la adaptación de los derechos de acceso de los usuarios que han cambiado los roles o puestos de trabajo y eliminar o bloquear inmediatamente los derechos de acceso de los usuarios que han abandonado la organización;

f) la revisión periódica de los derechos de acceso con los propietarios de los sistemas o servicios de información.

Debería considerarse la posibilidad de establecer los roles de acceso del usuario basados en los requisitos del negocio, que resuman una serie de derechos de acceso en perfiles típicos de acceso del usuario. Las solicitudes y las revisiones de acceso son más fáciles de gestionar a nivel de tales roles que a nivel de los derechos particulares.

Debería considerarse la posibilidad de incluir cláusulas en los contratos de personal y en los contratos de servicio que especifiquen sanciones si se intenta el acceso no autorizado por parte del personal o de los contratistas.

Gestión de derechos de acceso privilegiados
Se debería restringir y controlar la asignación y el uso de derechos de acceso privilegiados.

Debería controlarse la asignación de derechos de acceso privilegiados a través de un proceso formal de autorización, de acuerdo con la política de control de acceso pertinente. Deberían considerarse los siguientes pasos:

a) deberían identificarse los derechos de acceso privilegiado asociados a cada sistema o proceso; por ejemplo, sistema operativo, sistema de gestión de base de datos y cada aplicación y a los usuarios a los que es necesario asignar tales privilegios;

b) los privilegios de los derechos de acceso deberían asignarse a usuarios sobre una base de necesidad de uso y sobre una base de evento por evento, alineados con la política de control de acceso, es decir, basados en el requisito mínimo para sus roles funcionales;

c) debería mantenerse un proceso de autorización y un registro de todos los privilegios asignados. Los derechos de acceso privilegiados no deberían otorgarse sino hasta que el proceso de autorización sea completado;

d) deberían definirse requisitos para la expiración de los derechos de acceso privilegiados;

e) deberían asignarse los derechos de acceso privilegiados a una ID de usuario diferente del utilizado para las actividades regulares del negocio. Las actividades regulares del negocio no deberían ser desempeñadas desde las IDs de usuarios privilegiadas;

f) deberían revisarse regularmente las competencias de los usuarios con derechos de acceso privilegiados, a fin de verificar si se encuentran alineadas con sus funciones;

g) deberían establecerse y mantenerse procedimientos específicos para evitar el uso no autorizado de IDs de usuarios de administración genéricos, de acuerdo con las capacidades de configuración de los sistemas;

h) para los IDs de usuarios de administración genéricos, la confidencialidad de la información secreta de autenticación debería mantenerse cuando se comparte (por ejemplo, cambio de contraseñas frecuentemente y lo antes posible cuando un usuario privilegiado deja o cambia de trabajo, comunicando entre los usuarios privilegiados con los mecanismos adecuados).

El uso inapropiado de los privilegios de administración del sistema (cualquier característica o recurso de un sistema de información que habilite al usuario a hacer caso omiso de los controles del sistema o de la aplicación) puede ser un factor importante de contribución a las fallas o violaciones de los sistemas.

Gestión de la información secreta de autenticación de los usuarios
La asignación de información secreta de autenticación debería ser controlada a través de un proceso formal de gestión.

El proceso debería incluir los siguientes requisitos:

a) los usuarios deberían ser obligados a firmar una declaración para mantener la información de autenticación personal secreta y para mantener la información secreta de autenticación del grupo (es decir, compartida) únicamente con los miembros del grupo; esta declaración firmada puede ser incluida en los términos y condiciones del empleo;

b) cuando los usuarios son obligados a mantener su propia información de autenticación secreta, se les proporciona inicialmente información secreta de autenticación temporal y segura; a la que se ven obligados a cambiar a partir del primer uso;

c) deberían establecerse procedimientos para verificar la identidad de un usuario antes de proporcionar información secreta de autenticación nueva, sustitutiva o temporal;

d) la información secreta de autenticación temporal debería proporcionarse a los usuarios de forma segura; debería evitarse el uso de partes externas o mensajes de correo electrónico sin proteger (texto sin cifrar);

e) la información secreta de autenticación temporal debería ser única para cada individuo y no debería ser fácil de adivinar;

f) los usuarios deberían acusar recibo de la información de autenticación secreta;

g) la información secreta de autenticación del proveedor debería ser cambiada después de la instalación de los sistemas o del software.

Las contraseñas son un tipo de información secreta de autenticación comúnmente utilizadas y son un medio común para verificar la identidad del usuario. Otros tipos de información secreta de autenticación son llaves criptográficas y otros datos almacenados en hardware de autenticación (por ejemplo, “tokens”, tarjetas inteligentes) que producen códigos de autenticación.

Revisión de los derechos de acceso de los usuarios
Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios en intervalos regulares.

La revisión de los derechos de acceso debería considerar lo siguiente:

a) los derechos de acceso de usuarios deberían revisarse a intervalos regulares, y luego de cualquier cambio, tal como una promoción, una degradación, o una terminación del empleo;

b) los derechos de acceso de usuario deberían ser revisados y reasignados cuando se mueve de un rol a otro dentro de la misma organización;

c) las autorizaciones para derechos de acceso privilegiados deberían revisarse a intervalos más frecuentes;

d) debería verificarse la asignación de privilegios a intervalos regulares para garantizar que no se obtengan privilegios no autorizados;

e) los cambios en las cuentas privilegiadas deberían registrarse para su revisión periódica.

Eliminación o ajuste de los derechos de acceso
Los derechos de acceso de todos los empleados y de los usuarios de partes externas a la información y a los recursos de procesamiento de la información deberían ser eliminados al finalizar el empleo, contrato o acuerdo, o ajustados en caso de cambios.

Cuando ocurre la desvinculación, los derechos de acceso de un individuo a la información y los activos asociados con recursos de procesamiento y servicios de información, deberían eliminarse o suspenderse. Esto determinará si es necesario eliminar los derechos de acceso. Los cambios en la relación laboral deberían estar reflejados en la eliminación de todos los derechos de acceso que no fueron aprobados para el nuevo puesto. Los derechos de acceso que deberían eliminarse o ajustarse incluyen aquellos para acceso físico y lógico. La eliminación o el ajuste se pueden hacer mediante eliminación, revocación o reemplazo de las claves, tarjetas de identificación, recursos de procesamiento de información o suscripciones. Cualquier documentación que identifique los derechos de acceso de los empleados y contratistas debería reflejar la eliminación o el ajuste de los derechos de

acceso. Si un empleado o usuario de tercera parte que se marcha ha conocido las contraseñas para IDs de usuarios que permanecen activos, éstas deberían cambiarse al momento de la desvinculación o cambio de cargo, contrato o acuerdo.

Los derechos de acceso a la información y a los activos asociados con los recursos de procesamiento de información, deberían reducirse o eliminarse antes de que el empleo termine o cambie, dependiendo de la evaluación de los factores de riesgo tales como:

a) si la desvinculación o cambio es iniciado por el empleado, usuario de tercera parte, o por la dirección y la razón de la desvinculación;

b) las responsabilidades actuales del empleado, usuario de tercera parte o cualquier otro usuario;

c) el valor de los activos accesibles actualmente.

En ciertas circunstancias los derechos de acceso podrían estar asignados sobre la base de estar disponibles a más personas además del empleado o usuario de terceras partes que egresa, por ejemplo, IDs de grupo. En tal circunstancia, los individuos que egresan deberían eliminarse de toda lista de acceso de grupo y deberían realizarse acuerdos para recomendar a todos los otros empleados y usuarios de terceras partes involucrados, que no compartan más la información con la persona que egresa.

En caso de que la desvinculación sea iniciada por la administración, los empleados o usuarios de terceras partes descontentos pueden deliberadamente dañar información o sabotear los recursos de procesamiento de información. En casos de personas que están renunciando o siendo despedidas, podrían estar tentados a recolectar información para uso futuro.

Responsabilidades del usuario

Su objetivo es hacer responsables a los usuarios de salvaguardar su información de autenticación.

Uso de la información secreta de autenticación

Los usuarios deberían estar obligados a seguir las prácticas de la organización en el uso de la información secreta de autenticación.

Todos los usuarios deberían ser advertidos sobre:

a) mantener en secreto la información de su autenticación confidencial, asegurando que no se divulgue a otras partes, incluidas las personas de autoridad;

b) evitar mantener un registro (por ejemplo, en papel, archivo de software o dispositivo de mano) de la información de autenticación secreta, salvo que pueda almacenarse de forma segura y el método de almacenamiento haya sido aprobado (por ejemplo, repositorio de contraseñas);

c) cambiar la información de autenticación secreta siempre que existan indicios de su posible compromiso;

d) cuando las contraseñas son utilizadas como información de autenticación secreta, seleccione contraseñas de calidad con suficiente largo mínimo, que sean:

   1) fáciles de recordar;

   2) no se basen en algo que alguien pueda adivinar fácilmente o usando información relacionada con la persona, por ejemplo, nombres, números telefónicos, fechas de nacimiento, entre otros;

   3) no vulnerables a ataques tipo diccionario (es decir, que no consistan en palabras incluidas en diccionarios);

   4) libres de caracteres idénticos sucesivos ya sean todos numéricos o alfabéticos;

   5) si es temporal, cambiadas en el primer inicio de sesión.

e) no compartir la información secreta de autenticación del usuario individual;

f) asegurar una adecuada protección de las contraseñas cuando éstas sean utilizadas como información secreta de autenticación en procedimientos de inicio de sesión automático y luego almacenadas;

g) no utilicen la misma información secreta de autenticación para las propuestas comerciales y no comerciales.

La prestación de un Punto Único de Acceso (Single Sign On, SSO) o de otras herramientas de gestión de la información de autenticación secreta, reduce la cantidad de información secreta de autenticación que los usuarios están obligados a proteger y por lo tanto puede aumentar la eficacia de este control. Sin embargo, estas herramientas también pueden aumentar el impacto de la divulgación de la información secreta de autenticación.

Control de acceso a sistemas y aplicaciones

Su objetivo es prevenir el acceso no autorizado a los sistemas y aplicaciones.

Restricción de acceso a la información

El acceso a la información y a las funciones del sistema de aplicación debería ser restringido de acuerdo con la política de control de acceso.

Las restricciones al acceso deberían basarse en los requisitos de aplicación de negocios individuales y estar de acuerdo con la política de control de acceso definida.

Debería considerarse lo siguiente para dar soporte a los requisitos de restricción de acceso:

a) proveer menús para controlar el acceso a las funciones del sistema de aplicación;

b) controlar cuáles pueden ser accedidos por un usuario particular;

c) controlar los derechos de acceso de usuarios, por ejemplo, leer, escribir, borrar y ejecutar;

d) controlar los derechos de acceso de otras aplicaciones;

e) limitar la información contenida en las salidas;

f) proporcionar controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicación o sistemas sensibles.

Procedimientos de accesos (log-on) seguros
Donde sea requerido por la política de control de acceso, se debería controlar el acceso a los sistemas y a las aplicaciones por medio de un procedimiento de acceso (log-on) seguro.

Debería elegirse una técnica de autenticación adecuada para confirmar la identidad de un usuario.

Cuando se requiere una autenticación fuerte y la verificación de la identidad, deberían utilizarse métodos de autenticación alternativos a las contraseñas, tales como medios criptográficos, tarjetas inteligentes, hardware de autenticación o medios biométricos.

El procedimiento para iniciar sesión en un sistema o aplicación, debería ser diseñado para minimizar la oportunidad de acceso no autorizado. Por lo tanto, el proceso de conexión (log-on) debería divulgar el mínimo de información sobre el sistema o aplicación, de manera que evite proveer a un usuario no autorizado con asistencia innecesaria. Un buen procedimiento de acceso (log-on) debería:

a) no mostrar identificadores de sistema o aplicación hasta que el proceso de acceso se haya completado exitosamente;

b) desplegar un mensaje general advirtiendo que el sistema debería accederse solamente por usuarios autorizados;

c) no ofrecer mensajes de ayuda durante el proceso de acceso (log-on) que pudieran ayudar a un usuario no autorizado;

d) validar la información de acceso (log-on) solamente al completar todos sus datos de entrada. Si se produce una condición de error, el sistema no debería indicar qué parte de esos datos es correcta o incorrecta;

e) proteger contra intentos de acceso (log-on) por fuerza bruta;

f) registrar los intentos fallidos y exitosos;

g) emitir un evento de seguridad si se detecta una posible violación fallida o exitosa de los controles de inicio de sesión;

h) mostrar la siguiente información tras completar un acceso con éxito:

   1) fecha y hora del acceso (log-on) anterior realizada con éxito;

   2) detalles de cualquier intento de acceso fallido desde el momento del último acceso exitoso.

i) no mostrar la contraseña que está siendo ingresada;

j) no transmitir contraseñas en texto limpio por una red;

k) terminar sesiones inactivas después de un período de inactividad definido, especialmente en las ubicaciones de alto riesgo, tales como áreas públicas o externas fuera de la gestión de seguridad de la organización o en dispositivos móviles;

l) restringir los tiempos de conexión para proporcionar seguridad adicional para aplicaciones de alto riesgo y reducir la ventana de oportunidades para el acceso no autorizado.

Las contraseñas son una forma común de proporcionar identificación y autenticación basada en un secreto que solo el usuario conoce. Lo mismo se puede lograr también con medios criptográficos y protocolos de autenticación. La fortaleza de la autenticación del usuario debería ser acorde con la clasificación de la información a ser accedida.

Si las contraseñas son transmitidas en texto limpio a través de una red durante la sesión de acceso (log-on), pueden ser capturadas por un programa rastreador (“sniffer”) de red.

Sistema de gestión de contraseñas
Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurarse de la calidad de las contraseñas.

Un sistema de gestión de contraseñas debería:

a) imponer el uso de contraseñas e ID de usuario individuales con el fin de mantener la rendición de cuentas;

b) permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para tener en cuenta los errores de entrada;

c) forzar la selección de contraseñas de calidad;

d) forzar a los usuarios a cambiar sus contraseñas en su primer acceso(log-on);

e) forzar los cambios regulares de contraseña y cuando sea necesario;

f) mantener un registro de las contraseñas anteriores utilizadas e impedir su reutilización;

g) no mostrar las contraseñas en la pantalla cuando se están introduciendo;

h) guardar archivos de contraseñas separados de los datos del sistema de aplicaciones;

i) guardar y transmitir las contraseñas en formas protegidas.

Algunas aplicaciones requieren que una autoridad independiente asigne contraseñas de usuario; en tales casos, los puntos b), d) y e) de la guía anterior no se aplican. En la mayoría de los casos las contraseñas son seleccionadas y mantenidas por usuarios.

CONTROL DE ACCESO A LAS APLICACIONES

Uso de programas utilitarios privilegiados
El uso de programas utilitarios que puedan ser capaces de sobrepasar controles de sistemas y aplicaciones deberían ser restringido y estrictamente controlado.

Deberían considerarse las siguientes directrices para el uso de programas utilitarios que podrían ser capaces de anular los controles del sistema y de la aplicación:

a) el uso de procedimientos de identificación, autenticación y autorización para los programas utilitarios;

b) la segregación de los programas utilitarios de las aplicaciones de software;

c) la limitación del uso de programas utilitarios a un número mínimo práctico de usuarios autorizados y de confianza;

d) la autorización para el uso ad hoc de programas utilitarios;

e) la limitación de la disponibilidad de los programas utilitarios, por ejemplo, por la duración de un cambio autorizado;

f) el registro de todo uso de los programas utilitarios;

g) la definición y documentación de los niveles de autorización para los programas utilitarios;

h) la eliminación o desactivación de todos los programas utilitarios innecesarios;

i) no poner a disposición de los usuarios los programas utilitarios que tienen acceso a las aplicaciones en sistemas donde se requiere la segregación de funciones.

La mayoría de las instalaciones de las computadoras tienen uno o más programas utilitarios que podrían ser capaces de anular los controles del sistema y de aplicación.

Control de acceso al código fuente de programas
El acceso al código fuente de los programas debería ser restringido.

El acceso al código fuente de programas e ítems asociados (como diseños, especificaciones, planes de verificación y validación) debería estar estrictamente controlado, para prevenir la introducción de una funcionalidad no autorizada y evitar cambios involuntarios, así como mantener la confidencialidad de la propiedad intelectual valiosa. Para el código fuente de programas, esto puede alcanzarse por medio del almacenamiento central controlado de dicho código, preferiblemente en las bibliotecas de programas fuentes. Las siguientes directrices deberían ser consideradas para controlar el acceso a tales bibliotecas de programas fuente para reducir el potencial de corrupción de programas de la computadora:

a) de ser posible, las bibliotecas de programas fuente no deberían ser colocadas en sistemas de producción;

b) el código fuente de programas y las bibliotecas de programas fuente deberían gestionarse según procedimientos establecidos;

c) el personal de apoyo no debería tener acceso irrestricto a bibliotecas de programas fuente;

d) la actualización de bibliotecas de programas fuente e ítems asociados y la entrega de programas fuente a programadores sólo debería realizarse después de que la autorización apropiada haya sido recibida;

e) los listados de programas deberían mantenerse en un ambiente seguro;

f) debería mantenerse un registro de auditoría de todos los accesos a bibliotecas de programas fuente;

g) el mantenimiento y la copia de bibliotecas de programas fuente deberían estar sujetos a procedimientos estrictos de control de cambios.

Si el código fuente del programa va a ser publicado, deberían considerarse controles adicionales para ayudar a conseguir garantías sobre su integridad (por ejemplo, la firma digital).