MNEMO

Anexo 9

CONTROL DE ACCESOS

Dentro de esta área se localizan los siguientes objetivos y principios, controles y posibles mediciones asociadas:

A5.15	Control de acceso
Objetivo	Reglas para controlar el acceso físico y lógico a la información y a otros activos relacionados, deberían ser establecidas e implementadas, basadas en los requerimientos del negocio y de la seguridad de la información.
Principios	Garantizar el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados. Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información. Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados. Se establecerá una política de control de acceso, sobre la base de los requisitos de seguridad de negocios y la información. Los usuarios sólo dispondrán de acceso a la red y de la red servicios que han sido específicamente autorizados para su uso.
Información	Los propietarios de activos de información que son responsables ante la dirección de la protección "sus" activos deberían tener la capacidad de definir y/o aprobar las reglas de control de acceso y otros controles de seguridad. Asegúrese de que se les responsabiliza de incumplimientos, no conformidades y otros incidentes. Las normas de control de acceso deben estar respaldadas por procedimientos documentados (véase 5.16, 5.17, 5.18, 8.2, 8.3, 8.4 8.5, 8.18) y responsabilidades definidas (véase 5.2, 5.17).

A5.15	Control de acceso
	Hay varias formas de implementar el control de acceso, como MAC (control de acceso obligatorio), DAC (control de acceso discrecional), RBAC (control de acceso basado en roles) y ABAC (control de acceso basado en atributos). Las reglas de control de acceso también pueden contener elementos dinámicos (por ejemplo, una función que evalúa los accesos anteriores o valores específicos del entorno). Las reglas de control de acceso pueden implementarse con diferente granularidad, desde cubrir redes o sistemas completos hasta campos de datos específicos, y también pueden considerar propiedades como la ubicación del usuario o el tipo de conexión de red que se utiliza para el acceso. Estos principios y la forma en que se define el control de acceso granular pueden tener un impacto significativo en los costes. Unas reglas más estrictas y una mayor granularidad suelen suponer un mayor coste. Los requisitos de negocio y las consideraciones de riesgo deben utilizarse para definir qué reglas de control de acceso se aplican y qué granularidad se requiere.
Medición	Porcentaje de sistemas y aplicaciones corporativas para los que los "propietarios" adecuados han: (a) sido identificados, (b) aceptado formalmente sus responsabilidades, (c) llevado a cabo -o encargado- revisiones de accesos y seguridad de aplicaciones, basadas en riesgo y (d) definido las reglas de control de acceso basadas en roles.

A5.15	Requerimientos de negocio frente al control de acceso
Objetivo	Limitar el acceso a las instalaciones de procesamiento de información y a la información.
Principios	Se establecerá una política de control de acceso, sobre la base de los requisitos de seguridad de negocios y la información. Los usuarios sólo dispondrán de acceso a la red y de la red a servicios que han sido específicamente autorizados para su uso.
Información	Los propietarios de activos de información que son responsables ante la dirección de la protección de "sus" activos deberían tener la capacidad de definir y/o aprobar las reglas de control de acceso y otros controles de seguridad. Asegúrese de que se les responsabiliza de incumplimientos, no conformidades y otros incidentes.
Medición	Porcentaje de sistemas y aplicaciones corporativas para los que los "propietarios" adecuados han: (a) sido identificados, (b) aceptado formalmente sus responsabilidades, (c) llevado a cabo -o encargado- revisiones de accesos y seguridad de aplicaciones, basadas en riesgo y (d) definido las reglas de control de acceso basadas en roles.

A9.2	Gestión de accesos de usuario
Objetivo	Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información.
Principios	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.
Información	Cree la función diferenciada de "administrador de seguridad", con responsabilidades operativas para aplicar las reglas de control de acceso definidas por los propietarios de las aplicaciones y la dirección de seguridad de la información. Invierta en proporcionar al administrador de seguridad herramientas para realizar sus tareas lo más eficientemente posible.
Medición	Tiempo medio transcurrido entre la solicitud y la realización de peticiones de cambio de accesos y número de solicitudes de cambio de acceso cursadas en el mes anterior (con análisis de tendencias y comentarios acerca de cualquier pico / valle (p. Ej., "implantada nueva aplicación financiera este mes").

A9.3	Responsabilidades de los usuarios
Objetivo	Impedir el acceso de usuarios no autorizados y el compromiso o robo de información y recursos para el tratamiento de la información.
Principios	La cooperación de los usuarios autorizados es esencial para una seguridad efectiva. Los usuarios deberían ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición. Se debería implantar una política para mantener mesas de escritorio y monitores libres de cualquier información con objeto de reducir el riesgo de accesos no autorizados o el deterioro de documentos, medios y recursos para el tratamiento de la información.
Información	Asegúrese de que se establecen las responsabilidades de seguridad y que son entendidas por el personal afectado. Una buena estrategia es definir y documentar claramente las responsabilidades relativas a seguridad de la información en las descripciones o perfiles de los puestos de trabajo. Son imprescindibles las revisiones periódicas para incluir cualquier cambio. Comunique regularmente a los empleados los perfiles de sus puestos (p. Ej., en la revisión anual de objetivos), para recordarles sus responsabilidades y recoger cualquier cambio.
Medición	Porcentaje de descripciones de puesto de trabajo que incluyen responsabilidades en seguridad de la información: (a) totalmente documentadas y (b) formalmente aceptadas.

A9.4	Control de acceso al sistemas y las aplicaciones
Objetivo	Prevenir el acceso no autorizado a los sistemas y aplicaciones.
Principios	El acceso a la información y a las funciones del sistema y/o las aplicaciones debe limitarse de acuerdo con la política de control de acceso. Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones deben ser controladas por un procedimiento seguro LOG-ON. El sistema de gestión de contraseñas deberá garantizar la calidad de las mismas. El acceso al código fuente del programa se restringirá.
Información	Mantenga el equilibrio entre controles de seguridad perimetrales (LAN/WAN) e internos (LAN/LAN), frente a controles de seguridad en aplicaciones (defensa en profundidad). Aplique controles que no permitan el uso de contraseñas débiles y sobre todo intente siempre que pueda el uso de cuentas nominativas.
Medición	Estadísticas de cortafuegos, (p. Ej., intentos de acceso a páginas web prohibidas; número de ataques potenciales de hacking repelidos, clasificados en insignificantes/preocupantes/críticos).