# Identificación y análisis del control de acceso para la seguridad de TIC

Prof. Dr. Javier Areitio Bertolín[1] – e mail: *jareitio@eside.deusto.es*

Prof. Dra. Gloria Areitio Bertolín[2] – e mail: *ebparbeg@bs.ehu.es*

(1) Director del Grupo de Investigación Redes y Sistemas. Catedrático de la Facultad de Ingeniería. ESIDE. Universidad de Deusto (UD).
(2) Laboratorio de Informática Aplicada. Universidad del País Vasco (UPV /EHU)

*En el presente artículo se analiza el control de acceso desde sus elementos y componentes funcionales a los mecanismos mas relevantes para su implantación en sistemas de computación aplicados en TIC (Tecnologías de Información y Comunicaciones).*

## Monitores de Referencia y elementos del Control de Acceso

El control de acceso es un término genérico que se utiliza para designar el proceso por el cual un sistema de computación controla la interacción entre usuarios y recursos del sistema. Así mismo, el control de acceso permite implementar una política de seguridad que puede ser determinada por:
(a) Los requisitos de la organización.
(b) Los requisitos estatutarios, por ejemplo registros médicos.

Los requisitos de política pueden incluir:
(a) Confidencialidad, por ejemplo restricciones en el acceso de lectura.
(b) Integridad, por ejemplo restricciones en el acceso de escritura.
(c) Disponibilidad. Desde una visión esquemática un usuario pide acceso (leer, escribir, imprimir, etc.) a un recurso de un sistema de computación.

Un monitor de referencia establece la validez de una petición y devuelve una decisión de si concede o deniega el acceso al usuario

Veamos algunas analogías sencillas. Consideremos una oficina (tradicional que utiliza papeleo) en la que ciertos documentos sólo deberían ser leídos por determinados individuos. Se puede implementar seguridad almacenando los documentos en cajones bajo llave y entregar las llaves a los individuos relevantes autorizados para que puedan abrir los cajones apropiados. El monitor de referencia es el conjunto de cajones bajo llave. Una petición de acceso es un intento de abrir un cajón, se concede si la llave que se dispone permite abrirlo y se deniega en caso contrario. Otro caso sería un club donde sólo ciertos individuos se les permite la entrada. Se puede implantar seguridad utilizando un portero con una lista de invitados que se les permite la entrada. El monitor de referencia es el portero-guarda de seguridad con la lista de invitados.

Una petición de acceso se concede si una persona puede probar su identidad (autenticación) y esta en la lista de invitados. Los elementos del control de acceso son pues:
(a) Sujetos. Son entidades activas de un sistema de computación (usuarios, procesos, "threads" (ó "hilos"), demonios, etc.). Se suele suponer que un Sujeto es sinónimo de usuario.
(b) Objetos. Son entidades pasivas o recursos de un sistema de computación (ficheros, directorios, carpetas, impresoras, etc.).

Los Principales y Sujetos se utilizan para referirse a una entidad activa de una operación de acceso. Un Principal generalmente se asume que es un atributo o propiedad asociada con un Sujeto (por ejemplo: identificador de usuario, clave pública, proceso, "thread" / "hilo"). Un Sujeto puede representarse por uno o varios Principales.

## Operaciones de Acceso

Las operaciones de acceso son interacciones entre un objeto y un sujeto. Un sujeto puede observar (leer) un objeto (la información fluye del objeto al sujeto). Un sujeto puede alterar (escribir) un objeto (la información fluye del sujeto al objeto).

En un sistema operativo multiusuario, los usuarios abren ficheros para obtener acceso. Los ficheros se abren para leer o escribir de modo que el sistema operativo puede evitar conflictos cuando dos usuarios tratan de escribir simultáneamente al mismo fichero. En el modo de acceso de escritura, normalmente implementado como modo lectura / escritura, a un usuario que edita un fichero no se le debería preguntar para abrirlo dos veces. El modo de acceso "append" (ó sólo escritura ó "blind write") permite a los usuarios alterar un objeto sin observar su contenido (se utiliza por ejemplo para ficheros de "log" (registro) de auditoria y en Multics). A veces un objeto puede utilizarse sin abrirlo en modo lectura o escritura (directorios, ficheros ejecutables binarios, claves criptográficas). La operación de acceso "ejecución" significa diferentes cosas en diferentes contextos y sistemas.

Una matriz de control de acceso, base de muchos modelos de seguridad teóricos e introducida por Lampson (1972) (y extendida por Harrison, Ruzzo y Ullman 1976-78), es una estructura 2D en donde, en vertical se sitúan los sujetos y en horizontal los objetos. Los elementos de la matriz son los conjuntos de operaciones de acceso entre el sujeto y el"objeto correspondiente.

En una matriz de control de acceso, una política se representa por una terna de valores (s, o, a) donde "s" es un sujeto, "o" es un objeto y "a" es una operación de acceso. Una petición la concede el monitor de referencia si "a" pertenece a la matriz de acceso correspondiente al sujeto "s" y al objeto "o".

Los inconvenientes que se pueden identificar en torno a la matriz de control de acceso son:
(i) Formulación abstracta del control de acceso.
(ii) No adecuada para implementación directa:
  a) La matriz es probable que sea demasiado escasa de elementos y por tanto la implementación sea ineficiente.
  b) La gestión de la matriz es probable que sea muy difícil si existen 0000s de ficheros y 00s de usuarios, dando lugar a 000000s de entradas en la matriz.

Una lista de control de acceso (ó ACL) definida por objeto, es una columna de la matriz de control de acceso. Las ACLs se enfocan en los objetos y normalmente se implementan a nivel de sistema operativo (Windows NT utiliza ACL).

Una lista de capacidad definida por sujeto, corresponde a una fila de la matriz de control de acceso. Las listas de capacidad se enfocan en los sujetos, normalmente se implementan en software de servicios y aplicaciones. Las aplicaciones de bases de datos normalmente utilizan listas de capacidad para implementar acceso de fina granularidad a tablas y "queries".

Existe un interés renovado en el control de acceso basado en capacidad para sistemas distribuidos. Se puede identificar como inconveniente: ¿cómo podemos comprobar que sujetos pueden acceder a un objeto dado?. Volviendo a las analogías una ACL es similar a una lista de invitados (el club es el objeto, las personas que pueden entrar aparecen en la lista). Una lista de capacidad es análoga al conjunto de llaves que se proporciona a un usuario (el sujeto) para abrir los cajones bajo llave (los objetos) de una oficina.

Las tareas administrativas del control de acceso son: crear nuevos objetos y sujetos, borrar objetos y sujetos, cambiar los elementos de la matriz de control de acceso. La administración de estructuras de control de acceso consume mucho tiempo, es complicado y es proclive a errores.

## Técnicas de agregacion

Existen varios resultados teóricos importantes (Harrison – Ruzzo - Ullman; Lipton – Zinder) que demuestran que es muy difícil anticiparse a las consecuencias de acciones administrativas.

Las estructuras de control de acceso que "agregan" sujetos y objetos se utilizan para simplificar la carga administrativa.

Las principales técnicas de agregación son: grupos de usuarios, roles, procedimientos y tipos de datos. Los derechos de acceso a menudo se definen utilizando grupos de usuarios:

(a) En Unix, existen tres grupos asociados con cada objeto: "owner", "group" (owner) y "others".

(b) En VMS (sistema operativo Digital de VAX) existen cuatro grupos: "owner", "group", "world" y "system".

(c) En VST se construye un grupo jerárquico complicado de estructuras basados en el modelo Unix.

Un tipo datos es un conjunto de objetos con la misma estructura (por ejemplo, cuentas de banco). Se definen operaciones de acceso (procedimientos o permisos) sobre un tipo de datos. Los permisos se asignan a "roles". Los usuarios se asignan a "roles". Los "roles" normalmente se ordenan de forma jerárquica.

Consideremos un ejemplo: Los objetos son cuentas de banco, los sujetos son empleados de banco, el conjunto de cuentas de banco forma un tipo de datos. Se definen tres roles: cajero, empleado y administrador. Se definen procedimientos para: crear una cuenta (CA), cobrar cuentas (DA), transferir fondos entre cuentas (TF), crear nuevas cuentas (NA) y autorizar descubiertos de cuentas bancarias (AO). Se asigna un procedimiento: CA y DA al rol de cajero; TF al rol de empleado; NA y AO al rol de administrador. Se asigna a todos los usuarios que son cajeros el "rol de cajero". El rol de administrador puede ejecutar todos los procedimientos.

Los principales beneficios del control de acceso basado en roles (ó RBAC) son:

1) Sólo se necesita asignar usuarios y permisos a roles.

2) Se puede utilizar herencia en la jerarquía de roles para reducir el número de asignaciones necesarias.


Figura 1. Visión esquemática del Control de Acceso de Seguridad.

3) Simplifica la administración.

Algunos modelos de RBAC son: NIST (Ferraiolo 1992-2000), RBAC96 (Sandhu 1996), ARBAC97 (Sandhu 1997-99), OASIS (Hayton 1996-2001), Modelo gráfico de roles (Nyanchama – Osborn 1995-2001), Modelo NIST RBAC96 unificado (Ferraiolo, Sandhu 2001), etc.

Algunas implementaciones RBAC son: Windows NT (como groups local y global), OS/400 de IBM, Oracle 8, Framework .NET, etc. No existe un estándar aceptado por todos para el RBAC, habiendo jerarquías de roles y semánticas de jerarquías de roles.

## Operaciones de acceso Unix

El acceso a ficheros se realiza utilizando: read (r), write (w), execute (x). El acceso a directorios se efectúa utilizando: read (lista de contenidos del directorio), write (crear o renombrar ficheros del directorio), execute (buscar en directorio).

Los usuarios tienen un identificador y un identificador de grupo. 10.7 representa un usuario con identificador de grupo 10 e identificador de usuario 7 dentro de ese grupo. Los objetos tienen un identificador (determinado por el creador) y un identificador de grupo determinado por el identificador de grupo del creador. 10.7 es el identificador de objeto de un objeto creado por el usuario 10.7.


Figura 2. Representación de una Tabla de Control de Acceso y sus subconjuntos: ACLs y Listas de Capacidad.

Los objetos también tienen una máscara de acceso. Un patrón de 9 bits en tres grupos de tres. La máscara de acceso del directorio TRITON es 101 101 111 que representa x-r x-r xwr. La salida del comando Unix ls es inversa del orden de los bits.

Supongamos que el identificador del directorio TRITON es 12.6. Cualquier usuario tiene el acceso por defecto dado por los tres primeros bits (read y execute en este caso).

Cualquier usuario con identificador 12.x tiene el acceso "group" debido a que el identificador de usuario y el de objeto coinciden en la primera parte. El usuario con identificador 12.6 tiene acceso "owner" debido a que el identificador de usuario y el de objeto coinciden en ambas partes.

## Consideraciones sobre registros en la recuperación de desastres de seguridad informatica

Los registros de cara a un desastre de seguridad se pueden clasificar en una de las tres siguientes categorías:

1) Registros vitales. Son irremplazables.
2)Registros importantes pueden obtenerse o reproducirse a un costo considerable y sólo después de un retardo considerable.
3) Registros útiles deberían causar inconvenientes si se pierden, pero pueden reemplazarse sin costo considerable.

Los registros importantes y vitales deberían duplicarse y almacenarse en un área protegida del fuego, inundaciones, explosiones, etc. o sus efectos.

Los registros que se guardan en la sala de computadoras deberían ser los mínimos y deberían almacenarse en armarios o archivadores metálicos cerrados. Los registros almacenados fuera de la sala de computadoras deberían estar en armarios resistentes al fuego con resistencia de al menos dos horas.

La protección de registros también depende de la amenaza concreta que este presente. Una consideración importante es la velocidad de respuesta y la cantidad de tiempo disponible para actuar. Esto puede suponer desde recoger papeles precipitadamente y salir rápidamente hasta poder colocar metódicamente los documentos en una zona acorazada.

El identificar los registros e información es más crítico para asegurar la continuidad de las operaciones. Un enfoque sistemático para la gestión de los registros es también una parte importante del proceso de análisis de riesgos de seguridad y la planificación de recuperación de negocios.

Entre los beneficios adicionales obtenidos podemos identificar: costos de almacenamiento reducidos, servicio rápido, cumplimiento con la normativa del país. Los registros no se deberían conservar sólo como prueba de transacciones financieras sino también para verificar el cumplimiento con los requisitos de estatutos y legales.

Además, los negocios deben satisfacer los requisitos de conservación a nivel de organización y de empleado.

Estos registros se utilizan para examen y verificación independiente de prácticas de negocios. Se deben analizar los requisitos del país para la conservación de registros. Cada organización debería tener sus aboga-

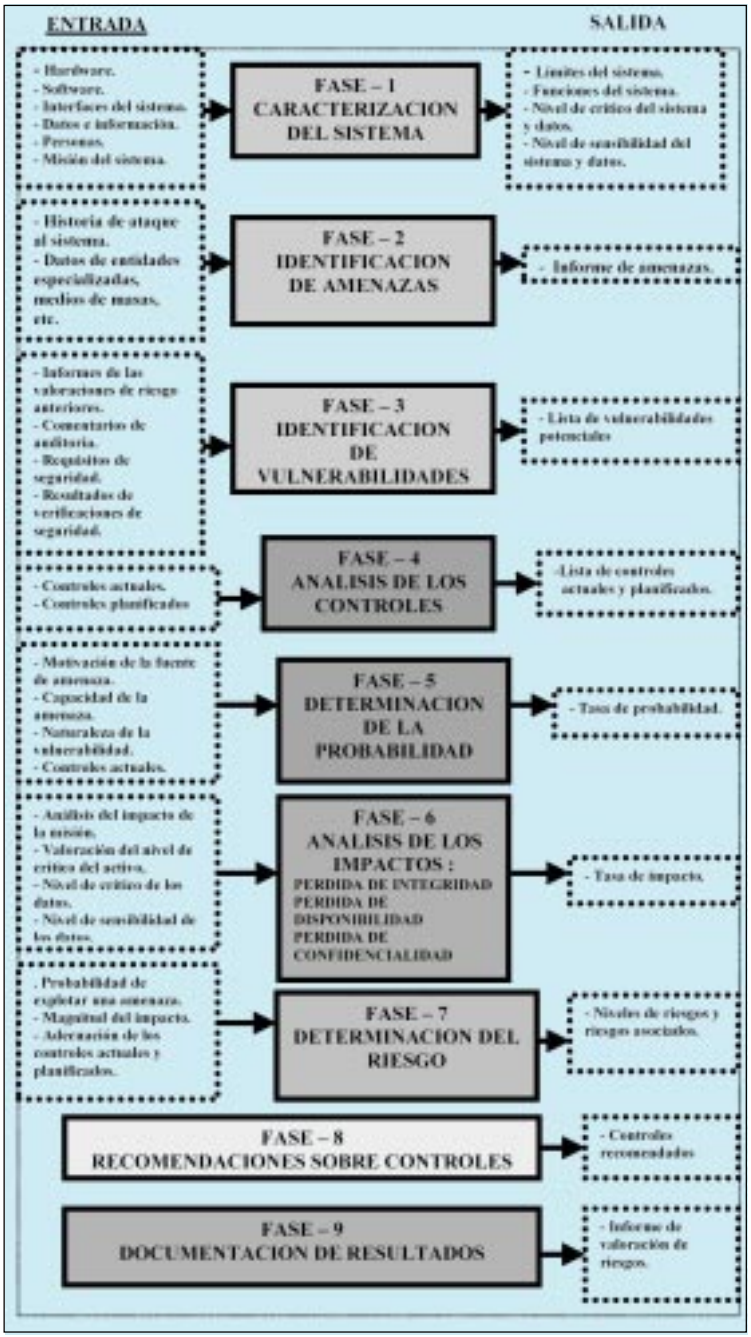


Figura 3. Metodología de Actividades de la Valoración de Riesgos de Seguridad

dos que aprueben su planificación de conservación. Del mismo modo que existen procedimientos de conservación de los registros, la organización debería prever los procedimientos de recuperación a seguir, según los diferentes tipos de medios exixstentes después de un desastre.

## Aspectos para la mejora de la seguridad

Pueden identificarse cuatro aspectos o fases fundamentales a la hora de conseguir una mejora significativa de la seguridad global de cualquier tipo de organización:

*Prevención*.- Para evitar un problema de seguridad en primer lugar se eliminan las posibles vulnerabilidades y se reduce la visibilidad del recurso. Se pueden utilizar medidas disuasorias.
*Detección*.- Se compara lo que se ha considerado aceptable por las directrices de política de seguridad de la organización con lo que se observa de hecho y se notifica al personal de seguridad de las inconsistencias existentes.
*Forense*.- Recoge información al detectar una violación de seguridad para crear la base de una respuesta. La ciencia forense digital es "el uso de métodos científicos, para la preservación, recogida, validación, identificación, análisis, interpretación, documentación y presentación de evidencias digitales a partir de fuentes digitales para reconstruir los eventos encontrados como delito o ayudar a anticipar acciones no autorizadas que demuestren ser un trastorno para la operativa planeada".
*Respuesta-Actuación*.- Responder a una brecha detectada de una manera que sea consistente con las directrices de la organización. La respuesta puede ser reactiva, ante algo evidente o proactiva, anticipándose al devenir con la sola utilización de ligeros indicios.

## Bibliografía

- Areitio, J. "Identificación, Clasificación de Objetivos de Seguridad y Creación de un Modelo de ST para las TIC". REE No. 588. Nov. 2003.
- Areitio, J. et al. "Mecanismo de Administración y Control Remoto Transparente y de Bajo Costo para Seguridad-Auditoria Telemática". Simposio Negocio Electrónico. Malaga. 2001.
- Moeller, R.R. "Computer Audit., Control and Security". John Wiley & Sons. Inc. 2004.
- Bishop, M. "Computer Security: Art and Science". Addison-Wesley Pub. Co. 2002.
- Harrington,"An Introduction to Network Security". Kaufmann. 2004. ❑