MODELO DE CONTROL DE ACCESO PARA SISTEMAS DE INFORMACIÓN BASADOS EN TECNOLOGÍAS WEB

MODEL OF ACCESS CONTROL FOR INFORMATION SYSTEMS BASED ON WEB TECHNOLOGIES

Oiner Gómez Baryolo, PhD.
Doctor en Ciencias Técnicas (Cuba).
Decano de la Facultad de Sistemas Computacionales y Telecomunicaciones de la Universidad Tecnológica ECOTEC, Ecuador.
ogomez@ecotec.edu.es

ARTÍCULO DE INVESTIGACIÓN
Recibido: 11 de septiembre de 2018.
Aceptado: 27 de octubre de 2018.

RESUMEN

La seguridad de los Sistemas de Información se ha convertido en uno de los temas de investigación más activos en los últimos años, debido al entorno hostil donde se desempeñan. Los principales retos están encaminados a lograr la confidencialidad, integridad, disponibilidad y trazabilidad de los recursos patrimoniales de personas u organizaciones, gestionados por Sistemas de Información. Con este objetivo, varios especialistas y organizaciones líderes en el tema han propuesto modelos, estándares, protocolos, entre otras soluciones que permiten desarrollar sistemas de control de acceso con un nivel de seguridad adecuado. La necesidad creciente de utilizar los Sistemas de Información en entornos distribuidos, ha provocado que las soluciones existentes en la bibliografía no cuenten con la robustez y escalabilidad necesaria para guiar el desarrollo de sistemas seguros de control de acceso para este tipo de escenarios. Partiendo de las limitaciones existentes, se desarrolló un modelo de control de acceso que integra de manera armónica los procesos de identificación y autenticación, autorización y auditoría para preservar la seguridad de los recursos gestionados por Sistemas de Información en entornos multidominios.

Palabras clave: seguridad, Sistema de Información, entorno multidominio, control de acceso.

ABSTRACT

The security of Information Systems has become one of the most active research topics in recent years, due to the hostile environment in which they operate. The main challenges are aimed at achieving confidentiality, integrity, availability and traceability of the heritage resources of people or organizations, managed by Information Systems. With this objective, several specialists and leading organizations in the field have proposed models, standards, protocols, among other solutions that allow the development of access control systems with an adequate level of security. The growing need to use Information Systems in distributed environments has meant that existing solutions in the bibliography do not have the robustness and scalability necessary to guide the development of secure access control systems for this type of scenario.

Starting from the existing limitations, an access control model was developed that harmoniously integrates the identification and authentication, authorization and audit processes to preserve the security of the resources managed by Information Systems in multi-domain environments.

Keywords: security, information system, multidomain environment, access control.

INTRODUCCIÓN

Con el paso del tiempo ha cambiado la forma en que las organizaciones gestionan sus procesos, debido a la necesidad de poder contar con información confiable, íntegra y oportuna que facilite la toma de decisiones en función del cumplimiento de sus objetivos estratégicos. Los cambios producidos están relacionados en gran medida con el desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC) y su utilización en las diferentes esferas de la sociedad (Kamal, 2011).

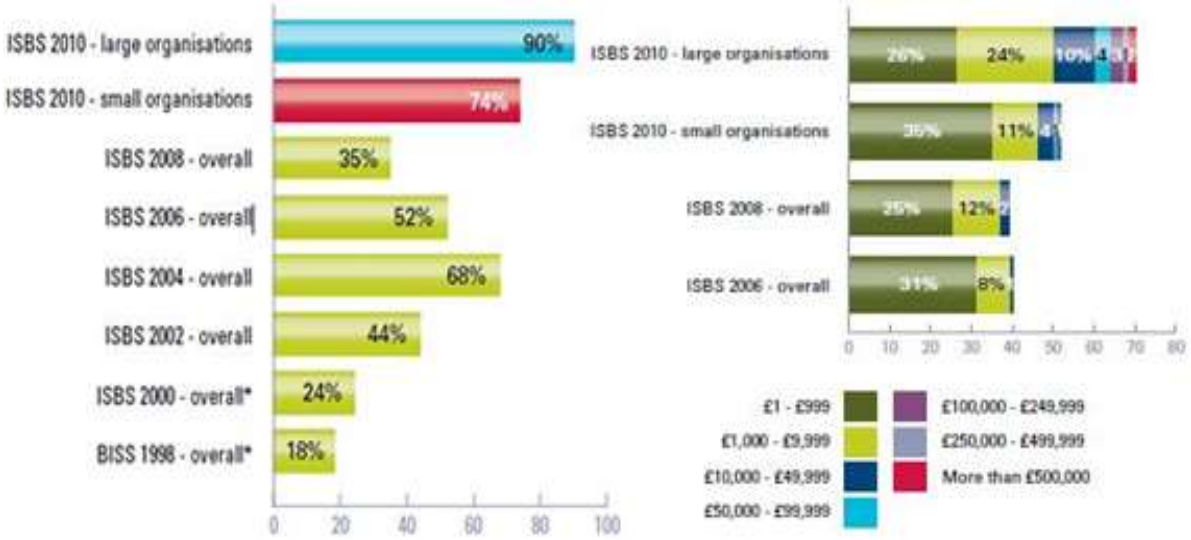
Como parte del desarrollo de las TIC y de la necesidad alcanzar una cultura de gestión de información y conocimiento, que contribuya a lograr mayor eficiencia y efectividad en la gestión de los procesos en las organizaciones, surgen los Sistemas de Información (SI) (Na, C., et al., 2010). Desde el punto de vista práctico un SI está compuesto por un conjunto de procesos, datos, modelos y tecnologías que responden a una estructura coherente en función del propósito de una organización (Davis & Olson, 1985). La utilización de los SI

impacta positivamente en el desempeño, el rendimiento y el cambio organizacional en los diferentes escenarios (Min, & Fei, 2008).

En la actualidad las actividades económicas, sociales, políticas e incluso militares de los países más desarrollados muestran una profunda dependencia hacia este tipo de tecnología, lo que supone una vulnerabilidad que puede ser atacada a través del ciberespacio. La existencia de esta vulnerabilidad ha traído consigo el desarrollo de herramientas y técnicas sofisticadas para ejecutar ataques con diversos objetivos, que han provocado una nueva forma de conflicto denominada ciberguerra (Medero, 2010). Se estima que entre veinte y treinta países han creado dentro de sus Fuerzas Armadas, unidades especializadas para combatir en una nueva dimensión del conflicto bélico, donde el objetivo es penetrar en las computadoras y redes del enemigo para causar daños y alterar sus SI (Santos, 2008).

El aumento en los últimos años de los ataques informáticos y las pérdidas económicas por el uso irracional de las TIC se pueden evidenciar en la **¡Error! No se encuentra el origen de la referencia.** que ilustra el resultado de un estudio realizado por especialistas de Infosecurity Europe, donde el 90% y el 74% de las grandes y pequeñas empresas respectivamente fueron objeto de ataques informáticos en el 2009. Las pérdidas reportadas producto a los mayores incidentes de este tipo oscilan entre £25,000-£40,000 y £3,000-£5,000 para grandes y pequeñas empresas respectivamente (Potter & Bears, 2010).

Figura 1. Reporte de ataques y pérdidas económicas derivadas.



Fuente: (Potter & Beard, 2010)

La constante proliferación de los SI distribuidos y la importancia cada vez mayor de tecnologías de la información, ha provocado que la seguridad se convierta en una preocupación importante en las organizaciones. Este problema puede agravarse en entornos multidominios donde se enmarcan una o varias organizaciones, cada uno empleando su propia política de control de acceso. Los entornos multidominios se están convirtiendo en una realidad que se evidencia en la mayoría de las aplicaciones empresariales basadas en Internet (Zhang & Joshi, 2007).

El control de acceso es un concepto que surge desde la década de 1960 y constituye uno de los dominios críticos que condicionan la seguridad de los SI. En la literatura se pueden encontrar varias definiciones del control de acceso determinadas por el escenario de aplicación (ISO, 2007).

Las propuestas relacionadas con el control de acceso en SI se agrupan fundamentalmente en dos direcciones: orientadas a lograr la seguridad en el uso de las TIC en las organizaciones y enfocadas en el desarrollo de SI seguros. Entre las soluciones más representativas enmarcadas en el primer grupo se encuentran: la familia de estándares ISO 27000, los controles sp800-53, la guía OWASP (siglas de Open Web Application Security Project), la Resolución 127 del 2007 del MIC, los objetivos COBIT (siglas de Control Objectives for Information and related Technology) y la biblioteca de ITIL (siglas de Information Technology Infrastructure Library). Estas soluciones se centran en el qué se debe hacer en términos de seguridad de las TIC y como evaluarlo, sin especificar cómo se debe hacer (ITGI, et al 2008).

El desarrollo y difusión de las primeras directivas que incorporaron elementos de cómo desarrollar soluciones de control de acceso se originaron a inicio de la década de 1970, con la propuesta realizada por el Department of Defense (DOD) de los Estados Unidos. Basado en las directivas descritas por el DOD, en 1983 surgen dos tipos de políticas de control de acceso: Control de acceso Discrecional (en inglés Discretionary Access Control, DAC) y Control de Acceso Obligatorio (en inglés Mandatory Access Control, MAC). En sus inicios ambas soluciones resolvieron las problemáticas existentes, pero el aumento de la complejidad de los SI y los entornos de aplicación demostraron que el carácter discrecional de DAC, la rigidez de MAC, entre otras deficiencias presentes en el diseño de estas soluciones, constituían vulnerabilidades en los nuevos escenarios organizacionales (Li, 2008).

Las insuficiencias mencionadas, unidas a la incapacidad para garantizar robustez, seguridad y escalabilidad en entornos multidominios, constituyen los antecedentes fundamentales que originaron extensiones de este modelo con diferentes enfoques. Los análisis existentes en la bibliografía demuestran que cada una de las extensiones brinda una solución para un escenario específico, por esta razón presentan brechas de seguridad y carecen de robustez y escalabilidad para adaptarse a entornos heterogéneos (O'Connor & Loomis, 2010).

Los referentes teóricos existentes en la literatura demuestran que, a pesar de los esfuerzos realizados por la comunidad científica, en la actualidad constituye un reto preservar la confidencialidad, integridad, disponibilidad y trazabilidad de los recursos gestionados por SI, desplegados en entornos multidominios. La solución se vuelve más compleja con la ausencia de un sistema de control de acceso que integre y logre el funcionamiento de manera armónica de los procesos de identificación, autenticación, autorización y auditoría en los diferentes escenarios donde se aplican los SI.

Para brindarle una solución efectiva la problemática existente, se plantea como objetivo general desarrollar un modelo de control de acceso que integre los procesos de identificación y autenticación, autorización y auditoría para preservar la seguridad de los recursos gestionados por Sistemas de Información en entornos multidominios.

Con el objetivo de analizar el estado de la teoría y de la práctica en la temática objeto de estudio, en el presente capítulo se exponen los conceptos fundamentales asociados al dominio del problema planteado. Se realiza un análisis detallado de los referentes teóricos que preceden la realización de este trabajo y que contribuyen a esclarecer su objeto de estudio. El examen crítico estará dirigido fundamentalmente a los modelos, normas, guías y estándares que propongan soluciones para el desarrollo de sistemas de control de acceso, con el objetivo de identificar debilidades y posibles aspectos a utilizar.

1. REVISIÓN TEÓRICA

1.1 Control de acceso en Sistemas de Información

Las primeras investigaciones sobre el control de acceso tuvieron lugar en la década de 1960. El control de acceso es indispensable en las organizaciones cuyo funcionamiento

requiere el intercambio de recursos digitales con diversos grados de sensibilidad. Las innovaciones en los modelos de negocio actuales, unidos a la constante colaboración entre las organizaciones y sistemas distribuidos requieren de un control de acceso eficiente, para hacer cumplir las políticas de seguridad más allá de los límites de las oficinas convencionales. Los sistemas de control de acceso tienen la responsabilidad de establecer a través de métodos formales las políticas de seguridad que se deben cumplir para preservar la confidencialidad, integridad, disponibilidad y trazabilidad de los recursos gestionados por SI. Según Suhendra, "una infraestructura de control de acceso involucra tres procesos fundamentales, la autenticación, la autorización y la auditoría o contabilidad" (Suhendra, 2011).

1.2 Análisis crítico de las soluciones existentes

Mantener la seguridad de la información ha sido uno de los grandes retos del desarrollo de software a nivel mundial. A menudo se cometen violaciones informáticas aprovechando las vulnerabilidades que incorporan las aplicaciones desde la etapa de desarrollo. La mayoría de estas violaciones están dadas por las limitaciones que presentan las soluciones de control de acceso que implementan los SI. A continuación, se realiza un análisis crítico de los referentes teóricos más destacados por su calidad y aporte al control de acceso. Para facilitar su comprensión se agrupan dentro de los procesos de identificación y autenticación, autorización y auditoría teniendo en cuenta en cuál de estos procesos centran su mayor fortaleza.

1.3 Soluciones para la identificación y autenticación

El proceso de identificación y autenticación es el proceso que inicia el flujo de control de acceso en los SI y que determina en gran medida el nivel de seguridad que se provee en los demás procesos. Para estandarizarlo se han desarrollado varios modelos, estándares y protocolos de gran calidad, que cubren la mayoría de los escenarios existentes. La identificación y autenticación debe proveer la información necesaria para iniciar el proceso de autorización y garantizar el registro de los eventos de este tipo como parte de la auditoría. A continuación, se analizan y describen las principales características de cada una de estas soluciones.

1.3.1 Kerberos

El Instituto Tecnológico de Massachusetts (MIT) desarrolló Kerberos para proteger los servicios de red proporcionados por el proyecto Athena. Steve Miller y Clifford Neuman, los principales diseñadores de la versión cuatro de Kerberos, publicaron esta versión al final de la década de 1980. La versión cinco, diseñada por John Kohl y Clifford Neuman, apareció como la Request for Comments (RFC) 1510 en 1993 (que quedó obsoleta por la RFC 4120 en 2005) (Neuman, 2005), con la intención de eliminar las limitaciones y problemas de seguridad presentes en la versión cuatro. Actualmente, el MIT distribuye una implementación de Kerberos libremente bajo una licencia similar a la Berkeley Software Distribution (BSD).

Es un protocolo de seguridad muy difundido en entornos Unix, aunque adoptado también por otros sistemas operativos como Windows. Kerberos es un sistema de autentificación de usuarios, que establece el intercambio de mensajes entre el cliente y las estaciones que forman parte de su infraestructura, como se refleja en la Figura 2.

Figura 2. Esquema de identificación y autenticación de Kerberos.

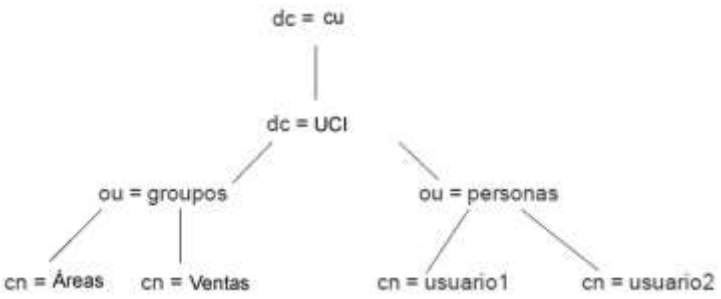
Fuente: (Al-Janabi & Rasheed, 2011)

Kerberos, como protocolo de seguridad, usa una criptografía de claves simétricas, lo que significa que la clave utilizada para cifrar es la misma clave utilizada para descifrar o autenticar usuarios (Echevarría, 2007). Esto permite a dos computadoras en una red insegura, demostrar su identidad mutuamente de manera segura.

1.3.2 Protocolo Ligero de Acceso a Directorios (LDAP)

LDAP está enmarcado en el grupo de protocolos de tipo cliente-servidor para acceder a un servicio de directorio sobre TCP/IP. Generalmente, los datos de un directorio LDAP siguen un modelo de organización de información en árbol. La versión original fue desarrollada por la Universidad de Michigan en el año 1993. El protocolo LDAP especifica formas para que los clientes puedan realizar la autenticación LDAP en la RFC 2251 y la RFC 2829. Algunos de los mecanismos de autenticación que soporta LDAPv3 son: autenticación anónima, autenticación simple (contraseña en texto claro), Kerberos, entre otros. En la **¡Error! No se encuentra el origen de la referencia.**3 se muestra un ejemplo de árbol de directorio de un LDAP.

Figura 3. Estructura de un directorio LDAP.



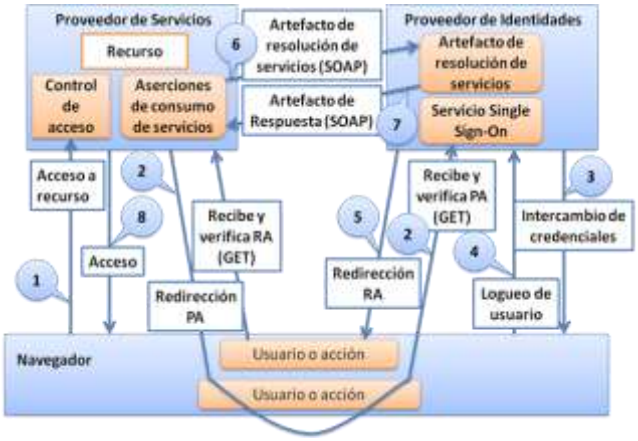
Fuente: (Hodge & Morgan, 2002)

LDAP define operaciones para añadir y borrar entradas del directorio, modificar una entrada existente, cambiar el nombre de una entrada y realizar búsqueda por parámetros. Las implementaciones más significativas del protocolo LDAP son los Active Directory y los OpenLDAP (Canfora, et. al., 2011). Los LDAP no garantizan una arquitectura SSO, por esta razón, cuando se necesita garantizar este tipo de escenario se integra a un componente de identificación y autenticación que implemente soluciones como SAML o Kerberos.

1.3.3 Lenguaje de Enmarcado de Aserciones de Seguridad (SAML)

En marzo del año 2005 OASIS adoptó como estándar SAML en su versión 2.0. En sus especificaciones describe la forma de intercambiar información de autenticación y autorización entre dominios. Está diseñado para ofrecer SSO en interacciones manuales o automáticas entre sistemas en dominios federados. Permite el intercambio de información de autenticación y autorización sobre usuarios, dispositivos o cualquier entidad identificable llamados sujetos. Usando sintaxis de XML, SAML define el protocolo petición-respuesta mediante el cual los sistemas aceptan o rechazan sujetos basados en aserciones. Para su funcionamiento define dos componentes fundamentales que son el PS y el PI que van a ser las partes que intervienen en la comunicación SAML, garantizando así que cualquier aplicación pueda intercambiar información de autenticación abstrayéndose del cómo. En la **¡Error! No se encuentra el origen de la referencia.**4 se muestra el flujo de intercambio de mensajes que se produce entre el PS y el PI en el proceso de autenticación.

Figura 4. Flujo de intercambio de mensajes en la autenticación con SAML.



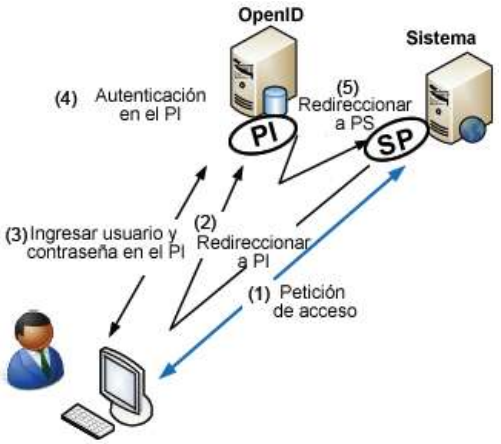
Fuente: Cantor, et al. (2005)

En la gestión del proceso de identificación y autenticación intervienen las aserciones, protocolos, enlaces y perfiles, basándose en el estándar XML. El estudio del estándar SAML permitió concluir que es la solución más robusta para la gestión del proceso de autenticación en entornos multidominios federados (Cantor, et. al., 2011).

1.3.4 OpenID

La primera versión de OpenID fue desarrollada originalmente por Brad Fitzpatrick en el año 2005, se basa en la creación de una única identidad web implementando la arquitectura SSO. Con esta credencial, un usuario puede autenticarse en cualquier sistema que exija identificación previa al acceso. Al ser de código abierto, descentralizado y apoyado ampliamente por la comunidad de internet permite decir que puede llegar a convertirse en un estándar de facto en la web. Para poder acceder a la página personal asociada a esta URL (denominada OpenID URL) es necesario introducir un usuario y una contraseña. En la **¡Error! No se encuentra el origen de la referencia.**5 se ilustran los conceptos que participan en el proceso de autenticación y el flujo de comunicación entre ellos.

Figura 5. Flujo de autenticación de OpenID.



Fuente: McIntyre, Luterroth, & Weber (2011)

El protocolo OpenID se desarrolló con el objetivo de proporcionar seguridad a blog y sitios publicados en internet que no requieren de un mecanismo robusto de autenticación. El carácter descentralizado de esta solución representa una vulnerabilidad crítica ante ataques como la suplantación de usuarios. Para que un usuario pueda acceder a un sistema que implemente OpenID, tiene que memorizar la dirección que lo identifica además de su usuario y contraseña. Otras de las limitantes importantes es que solo implementa los procesos de identificación y autenticación para el entorno web, excluyendo los sistemas de escritorio y dificultando los procesos de autorización y auditoría (McIntyre, Luterroth & Weber, 2011).

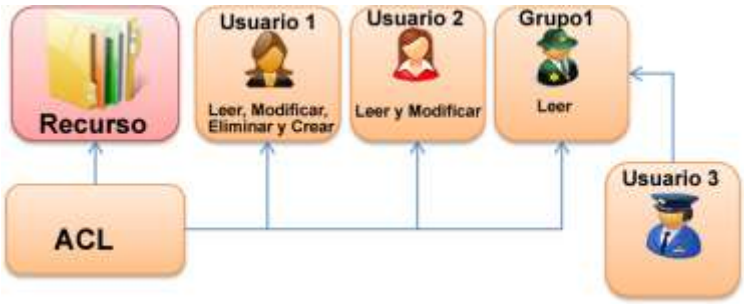
1.4 Soluciones para la autorización

El proceso de autorización se nutre de los datos que arroja como salida el proceso de identificación y autenticación para discernir los privilegios de cada usuario. Este proceso tiene la responsabilidad de establecer las políticas o privilegios de acceso de los usuarios sobre los recursos del dominio. La información asociada a cada uno de los eventos de acceso a los recursos debe almacenarse para facilitar la auditoría. A continuación, se analizan las principales soluciones desarrolladas para fortalecer el proceso de autorización.

1.4.1 Listas de Control de Acceso (ACL)

En el año 1971, Lampson propuso un modelo que permite establecer el control de acceso a través de una matriz que se enmarca dentro de la estrategia de control de acceso discrecional. Su rigidez y falta de escalabilidad constituyen las limitantes fundamentales que propiciaron el surgimiento de las Listas de Control de Acceso (en inglés Access Control List, ACL). Una ACL puede ser considerada como una estructura de datos jerárquica que puede contener múltiples ACL, cada una de ellas define un conjunto de permisos asociados a un determinado recurso. Los *"sujetos, objetos y permisos"* son los conceptos fundamentales que se utilizan para definir las reglas de acceso aplicadas directamente a los usuarios o a los grupos donde pertenecen (Li & Liao, 2009). La Figura 6 se refleja un ejemplo de control de acceso utilizando las ACL.

Figura 6. Listas de Control de Acceso.



Fuente: (Li & Liao, 2009)

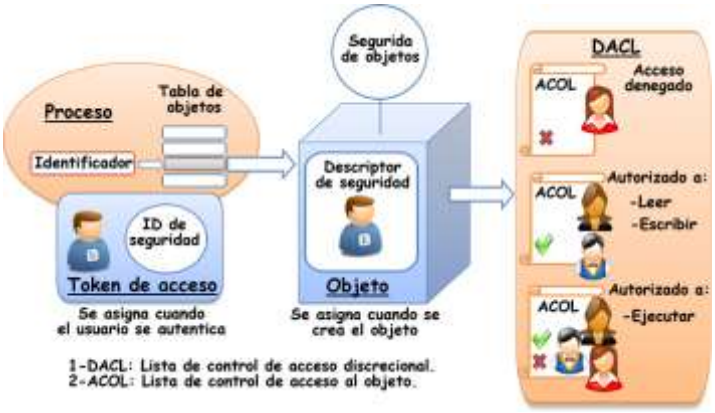
Las ACL solo representan una estructura de almacenamiento de los privilegios autorizados de los usuarios o grupos sobre los recursos. Por esta razón su escalabilidad se ve limitada

en los SI de gran envergadura, integrados por un gran número de recursos y conceptos dinámicos que condicionan las políticas de acceso (Karjoth, Schade & Herreweghen, 2008). A pesar de sus limitaciones, su aplicación se evidencia en varios sistemas operativos y modelos de control de acceso.

1.4.2 Control de acceso Discrecional (DAC)

El modelo DAC, también conocido como modelo de seguridad limitada, fue desarrollado por TCSEC (siglas de Trusted Computer System Evaluation Criteria) a finales del año 1983. En este modelo todos los sujetos y objetos en el sistema son controlados y se especifican reglas de autorización de acceso para cada uno de ellos. DAC es una forma de acceso basada en los sujetos y grupos a los que pertenece un objeto. Se dice que es discrecional en el sentido de que un sujeto puede transmitir sus permisos a otro sujeto sin la aprobación de un administrador general (Downs, et. al. 1985). En la Figura 7 se muestra un ejemplo del modelo DAC para facilitar su comprensión.

Figura 7. Modelo de control de acceso discrecional.



Fuente: (Wei & Jarzabek, 1998)

El carácter discrecional de la gestión de políticas de acceso de DAC puede provocar que un sujeto no autorizado pueda acceder a objetos no autorizados para él. Este riesgo pude ser extendido a todo el sistema violando un conjunto de objetos de seguridad. Es difícil para DAC garantizar las reglas de integridad como "*mínimo privilegio*" o *"separación de tareas"* que son necesarias en los ambientes con procesos colaborativos. DAC es apropiado en ambientes donde el intercambio de información es más importante que su protección. La

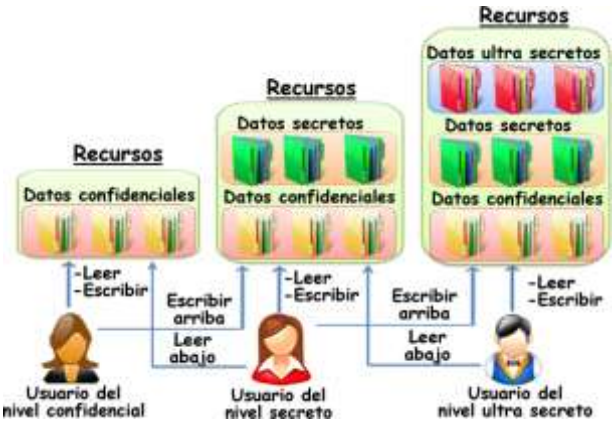
especificación de este modelo no garantiza su implementación en entornos multidominios y no provee soluciones para los procesos de identificación, autenticación y auditoría.

1.4.3 Control de acceso Obligatorio (MAC)

El modelo MAC, al igual que el modelo DAC fue desarrollado por TCSEC a finales del año 1983. En este modelo todos los sujetos y objetos son clasificados basándose en niveles predefinidos de seguridad que son usados en el proceso de obtención de los permisos de acceso. Para describir estos niveles de seguridad todos los sujetos y objetos son marcados con etiquetas de seguridad, que siguen el modelo de clasificación de la información militar (desde *"desclasificado"* hasta *"alto secreto"*), formando lo que se conoce como política de seguridad multinivel. Este modelo puede ser implementado usando mecanismos de seguridad multinivel que usan reglas *"no leer arriba"* y *"no escribir abajo"* también conocidas como restricciones Bell-Lapadula (Wang, Li & Li, 2010).

La Figura 8 muestra los conceptos fundamentales que incluye el modelo MAC y el flujo de acceso entre los diferentes niveles.

Figura 8. Modelo de control de acceso obligatorio.



Fuente: Xu, et al. (2009)

La concepción de MAC estuvo marcada fundamentalmente por la necesidad de un modelo de control de acceso para escenarios militares. Su rigidez impide el establecimiento de políticas, particularmente en SI de gran envergadura que presentan procesos colaborativos en entornos multidominios. Esta situación puede provocar que los usuarios que se

encuentran en un nivel determinado puedan acceder a toda la información del nivel inferior o superior sin restricción. Las especificaciones de MAC solo establecen criterios enfocados a la confidencialidad, dejando al descubierto la integridad y disponibilidad de los recursos.

1.4.4 Control de Acceso Basado en Roles (RBAC)

El principal objetivo del modelo RBAC es prevenir que los usuarios tengan libre acceso a la información de la organización. La definición básica de RBAC establece que los usuarios son asignados a roles, los permisos son asociados a roles y los usuarios adquieren permisos siendo miembros de roles. Las asignaciones usuario-rol y permiso-rol pueden ser muchos-a-muchos, por lo que un usuario puede pertenecer a muchos roles y un rol puede poseer muchos usuarios. De manera similar un permiso puede ser asociado a muchos roles y un rol puede tener asociado muchos permisos. RBAC también incluye el concepto de sesión, que permite la activación y desactivación selectiva de roles, posibilitando que un usuario pueda ejercer los permisos de varios roles simultáneamente (Ferraiolo, et. al., 2001).

Por otro lado, la Separación Dinámica de Deberes (en inglés, Dynamic Separation of Duty, DSD) al igual que la Separación estática de Deberes (en inglés, Static Separation of Duty, SSD), limitan los permisos que son disponibles para un usuario. Sin embargo, DSD difieren de las SSD por el contexto en el cual estas limitaciones son impuestas. Las DSD limitan la disponibilidad de los permisos aplicando las restricciones sobre los roles que pueden ser activados durante una sesión de usuario. La Figura 9 muestra con mayor claridad los conceptos mencionados anteriormente y las relaciones que existen entre ellos.

Figura 9. Modelo de control de acceso basado en roles.

Fuente: Jianxiao, Yimin, & Zongkun (2010)

El control de acceso basado en roles permite expresar de forma sencilla y natural la política de autorización a los recursos de una organización. Según sus propios autores, la utilización de este modelo se ve limitada a la hora de aplicarlo en sistemas colaborativos desplegados en entornos multidominios, donde es necesario integrar los aspectos de seguridad con los funcionales. Entre las debilidades más significativas del modelo RBAC se destacan:

- La naturaleza estática de los roles, al carecer de flexibilidad y sensibilidad para estos escenarios.
- La falta de escalabilidad para garantizar el control de acceso en dominios federados, donde interactúan varias organizaciones con diversos SI y políticas de seguridad.
- La ausencia de un mecanismo para establecer diferencias entre los usuarios que desempeñan un mismo rol.
- Las restricciones solo se establecen a nivel de permisos y roles sin tener en cuenta las que se pueden originar si se definen reglas relacionadas con los atributos de un objeto.

1.4.5 Control de Acceso Basado en Atributos (ABAC)

En el modelo de Control de Acceso Basado en Atributos (en inglés Attribute Based Access Control, ABAC), los privilegios son establecidos en base a la colección de atributos que posee el usuario y una política que los determina. La representación de las políticas en ABAC es semánticamente más expresiva y posee una mayor granularidad ya que puede basarse en cualquier combinación de atributos de sujeto, de recursos y de entorno. En la infraestructura de gestión de políticas se utilizan certificados de atributos para asignar un conjunto privilegios a cada usuario. El verificador comprueba en la política de control de acceso si el usuario tiene los privilegios suficientes para acceder al recurso solicitado. La 10 muestra los conceptos que integran la arquitectura propuesta por ABAC para el control de acceso.

Figura 10. Modelo de control de acceso basado en atributos.

Fuente: (Yuan & Tong, 2005)

Las limitaciones de ABAC radican en la dificultad para definir los atributos de forma consistente en sistemas complejos desplegados en entornos multidominios. La seguridad que proporciona ABAC depende del número de atributos y reglas que se establezcan. Este aspecto influye de forma negativa en el rendimiento del SI a la hora de realizar las búsquedas para conceder o no el acceso. La ausencia del concepto rol en su definición, aumenta la complejidad de mantenimiento de las políticas en entornos heterogéneos y dinámicos (Yuan & Tong, 2005).

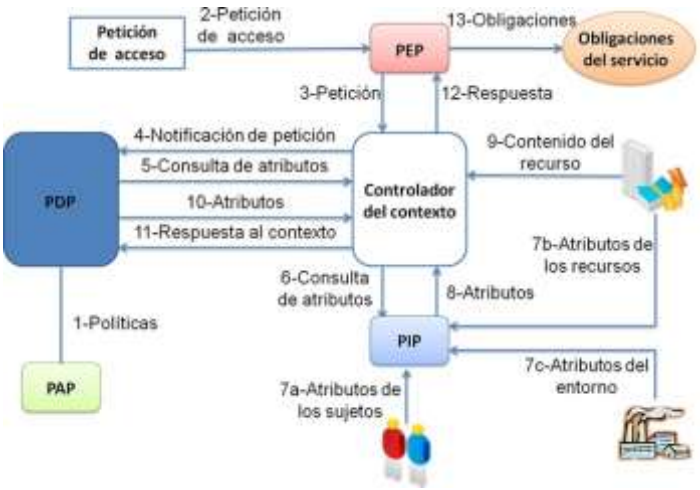
2. Lenguaje de Enmarcado de Control de Acceso Extensible (XACML)

La versión 1.0 de la especificación de XACML fue reconocida como estándar por la OASIS en febrero del año 2003 (Cover, 2009). XACML está basado en XML y tiene como objetivo fundamental promover un mecanismo unificado de control de acceso, definiendo un lenguaje capaz de expresar información de autorización en forma flexible y extensible, de manera que pueda acomodarse a una amplia variedad de sistemas y dispositivos. La especificación define a un sistema de autorización como cinco subsistemas, cada uno con una función bien delimitada descrita a continuación:

- **Punto de Administración de Política (PAP):** es el punto en el cual se crean y administran las políticas de control.
- **Punto de Decisión de Política (PDP):** es el punto responsable de evaluar un pedido de autorización.
- **Punto de Control de Política (PEP):** es el punto que intercepta el pedido de autorización y lo deriva al PDP. Luego de obtener la respuesta del PDP elabora una respuesta para el sistema que hizo el pedido de autorización.
- **Punto de Información de Política (PIP):** en algunos casos la evaluación de un pedido de información puede requerir la búsqueda de información en otras fuentes. En estos casos, el pedido contiene información sobre el recurso que contiene al valor del atributo y el PIP es responsable de interpretar estos datos y obtener el valor.

Para facilitar la comprensión de XACML, la **¡Error! No se encuentra el origen de la referencia.**11 muestra la estructura y el flujo de mensajes de autorización entre cada uno de los conceptos que propone.

Figura 11. Flujo de intercambio de mensajes de autorización de XACML.



Fuente: Yongsheng, et al. (2010)

El área de impacto de la especificación XACML se centra en la estandarización de los mensajes de autorización. A pesar de que no especifica cómo deben establecerse las políticas de asignación de privilegios, es recomendable utilizar las ventajas que provee para el intercambio de mensajes.

2.1 Soluciones para la auditoría

El proceso de auditoría se nutre de la información que le brindan los procesos anteriores para cerrar el flujo del control de acceso. La información contenida en los log de eventos representa una fuente importante para realizar análisis enfocados en el comportamiento de los recursos, usuarios, seguridad y procesos que tienen lugar en el dominio de aplicación. A continuación, se analizan las principales soluciones existentes en la literatura para estandarizar los log de eventos en función de facilitar su análisis para la toma de decisiones.

2.2 Formatos de ficheros de log

El formato de los archivos de log de datos, define los parámetros que deben almacenarse para tener constancia de las acciones ejecutadas sobre los recursos de la red para su

posterior análisis. Actualmente existen tres vertientes fundamentales relacionadas con los log de eventos en SI: el formato NCSA que propone Apache, el formato IIS (siglas de Internet Information Service) que propone Microsoft y el Formato de Log Expandido (en inglés Expanded Log Format, ExLF) que propone W3C (Hernández, Garrigós y Mazón, 2010). Todas están encaminadas al almacenamiento de los log de sistemas web y sus respectivos gestores de base de datos y para ello proponen atributos relacionados con el acceso a los diferentes directorios del servidor de aplicaciones.

Entre los atributos generales se pueden mencionar: la versión, fecha, hora, tiempo de la petición, cantidad de bytes, IP de inicio y de destino, protocolo, URL, método, usuario, tipo de evento, descripción, entre otros parámetros relacionados con el navegador y los recursos que visualiza al usuario. La 12 muestra ejemplos de tipos de eventos contenidos en los log de Apache para facilitar su comprensión.

Figura 12. Formato NCSA de Apache.

```
Log de Erorr
================================================================================
[Tue May 01 18:07:40 2012] [error] [client 127.0.0.1] File does not exist:
D:/Proyecto/DESTEC/web/lib/ExtJS/temas/default/images/images, referer:
================================================================================
Log de Noticia
================================================================================
[Wed May 02 22:52:18 2012] [notice] Apache/2.2.6 (Win32) PHP/5.2.5 configured -- resuming
normal operations
================================================================================
Log de Base de Datos
================================================================================
120401  1:56:30120401  1:56:30 [ERROR] Cannot find table worpress/wp_usermeta from the
internal data dictionary of InnoDB though the .frm file for the table exists.
================================================================================
Log de Acceso
================================================================================
127.0.0.1 - - [02/May/2012:22:52:27 -0300] "POST /seguridad/IdentityProvider/ HTTP/1.1" 200
1783
================================================================================
```

Fuente: Elaboración propia.

La información contenida en los log de eventos de este tipo de soluciones solo permite realizar análisis muy superficiales, en su mayoría engorrosos por el exceso de contaminación en los datos. Los parámetros almacenados no brindan información relacionada con el negocio del sistema, recursos y actores que intervienen en su ejecución. La escalabilidad de estos formatos se ve limitada a la hora de incorporar elementos que caracterizan estos u otros tipos de aplicaciones para realizar análisis más reales del funcionamiento, la seguridad y la ejecución de los procesos de negocios.

2.3 Protocolo Syslog (RFC 5424)

El RFC 5424 o protocolo Syslog, es la versión actualizada del RFC 3164, tiene como objetivo normar el envío de mensajes de notificación de eventos entre dispositivos conectados a la red. Entre los argumentos más importantes se destacan: la prioridad, versión, fecha, hora, nombre de la PC cliente o IP, nombre de la aplicación que envía el mensaje, el identificador del proceso del sistema operativo ejecutado e identificador del tipo de mensaje. Además de estos parámetros, provee un campo de datos que permite enviar pares de campo-valor para especificar otras informaciones (Gerhards, & GmbH, 2009). La Figura 13 muestra el formato de un evento utilizando el protocolo Syslog.

Figura 13. Formato de mensajes del protocolo Syslog.

```
_____________________________________________________________________________
<187> [timestamp in RFC prescribed format] [device dns name | ip address] [Dummy
Value/Counter : ] [ {:|*} yyyy mmm dd hh:mm:ss TimeZone <-|+> hh:mm] %FACILITY-
[SUBFACILITY-]SEVERITY-MNEMONIC: description
=============================================================================
```

Fuente: Elaboración propia.

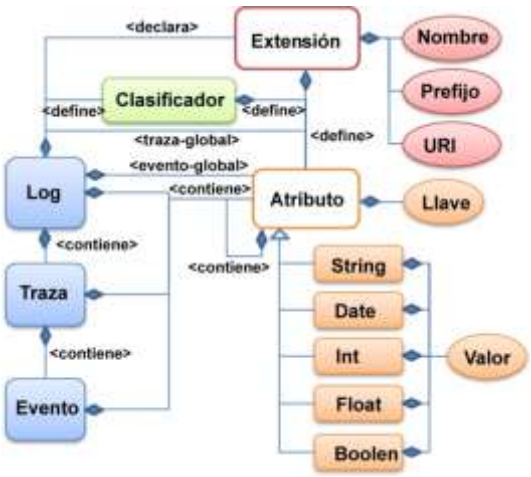
El protocolo Syslog, a pesar de contar con cierto dinamismo para la definición de nuevos parámetros, está diseñado para el envío de mensajes a través de los protocolos UDP y TCP de la capa de transporte (Echavarría, 2007). Esta característica incorpora riesgos de seguridad en las transferencias y almacenamiento de los mensajes y limita su campo de acción a los dispositivos o servicios embebidos en los sistemas operativos. Por esta razón su uso se reduce a este nivel, sin adentrarse en la ejecución interna de los procesos de negocio en un SI. El formato propuesto por esta solución presenta problemas de estandarización con los formatos de algunos campos como el encabezado y el tiempo.

2.4 Flujo de Eventos Extensibles (XES)

XES es un estándar basado en XML para el registro de eventos en un SI, desarrollado en el año 2010. Su propósito es proporcionar un formato genérico para el intercambio de los datos de registro de eventos entre las herramientas y los dominios de aplicación. Su objetivo principal es la minería del proceso, mediante el análisis de procesos operativos basados en sus registros de sucesos. XES ha sido diseñado para soportar la minería de datos, la

minería de textos y el análisis estadístico. Define un modelo para el registro de eventos en función de la mejora de procesos de negocio. Para comprender mejor el funcionamiento de XES es necesario analizar su estructura, ilustrada en la Figura 14.

Figura 14. Esquema del e*stándar XES.*



Fuente: (Günther, 2009)

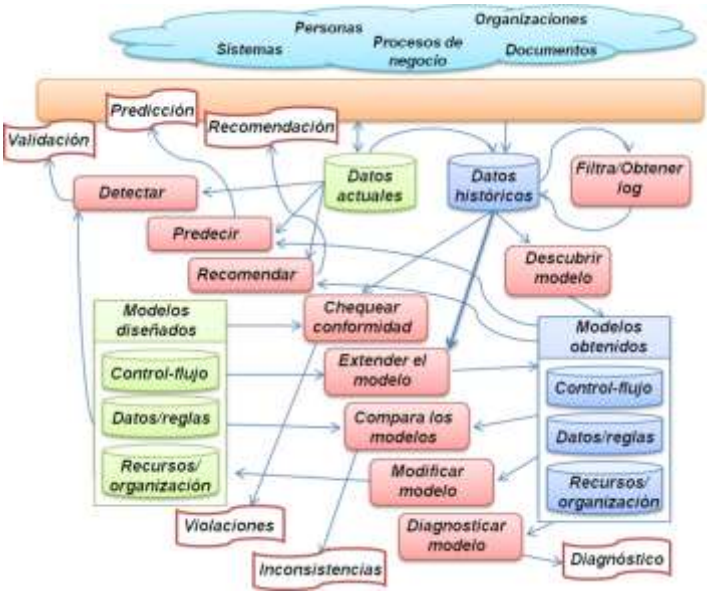
El objetivo principal es proporcionar una estructura genérica para el registro de los datos asociados a los procesos de negocios ejecutados en un SI. No incorpora los elementos necesarios para realizar auditorías en los SI en relación con los procesos de negocio que informatizan. Además, no provee ninguna solución asociada al análisis de los log producidos por los SI para tomar decisiones que impacten positivamente en la seguridad o los procesos de negocio de la organización. XES se limita a proporcionar un formato para estructurar los datos que constituyen la entrada de las herramientas de minería de procesos. No incluye los elementos necesarios para guiar el desarrollo de soluciones de gestión de log de eventos y su aplicación se ve limitada en los SI que no se conciben desde el inicio bajo la filosofía de procesos. Otra de las deficiencias identificadas por los estudiosos del tema, es su incapacidad para garantizar la autenticidad de los log en entornos distribuidos (Buijs, 2010).

2.5 Marco de trabajo Auditing 2.0

El marco de trabajo Auditing 2.0, desarrollado por Van der Aalst en el año 2010, constituye un referente importante para la minería de procesos, con el objetivo de proporcionar información que apoye la toma de decisiones en las organizaciones. Divide los datos producidos por el registro de eventos en "*pre-mortem*" y "*post-mortem*". Los "*post-mortem*" se refieren a la información sobre los casos que han terminado y los "*pre-mortem*" a los casos que aún no han terminado. En su concepción define dos modelos, los modelos prescritos o teóricos (De jure models) y los modelos de facto (De facto models).

Los modelos prescritos describen una manera conveniente o necesaria de realizar el trabajo, mientras que los modelos de facto se basan en la minería de los procesos terminados para descubrir lo que realmente se está ejecutando. La Figura 15 muestra el modelo descrito en Auditing 2.0 para realizar análisis enfocados en mejorar los procesos de negocios de una organización.

Figura 15: Marco de trabajo Auditing 2.0.



Fuente: (Aalst, 2011)

La aplicación de este marco de trabajo permite predecir, detectar y recomendar acciones para mejorar los procesos de negocio en una organización. Recibe como entrada los datos estructurados en el formato que propone el estándar XES, esta característica evidencia que su campo de acción está dirigido a la minería de procesos (Aalst, 2011). A pesar de ser la solución más aceptada por la comunidad científica para desarrollar soluciones que mejoren el análisis del funcionamiento de los procesos, su descripción no incorpora elementos dirigidos al análisis relacionado con el funcionamiento del sistema. La arquitectura que propone Auditing 2.0 para almacenar y analizar los datos pude influir de forma negativa en el rendimiento de los SI, debido a los análisis que se proponen en la base de datos transaccional del sistema. La efectividad de este marco de trabajo en los SI que no estén orientados a procesos, depende de la capacidad de los algoritmos empleados para el descubrimiento de procesos.

3. ANÁLISIS DE RESULTADOS

3.1 Modelo de Control de Acceso

El modelo propuesto está integrado por los tres componentes del control de acceso la identificación y autenticación, la autorización y la auditoría. Una de las deficiencias más significativas identificadas en las soluciones existentes en la literatura, es el hecho de que no conciben de forma integrada los componentes de identificación y autenticación, autorización y auditoría. Esto trae como consecuencia problemas de integración e interoperabilidad que se transforman en vulnerabilidades y pérdida de información valiosa para la gestión de conocimiento con múltiples objetivos. Para suplir estas debilidades se propone un modelo que integra de forma armónica los componentes descritos en los epígrafes anteriores.

3.2 Principios del modelo

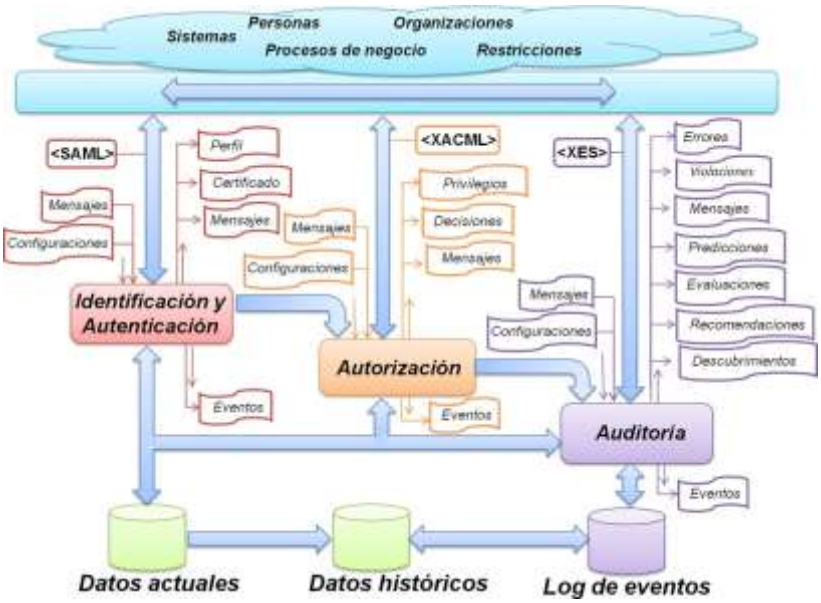
Los principios que sustentan el modelo propuesto para el desarrollo de soluciones de control de acceso que preserven la seguridad de los recursos gestionados por SI en entornos multidominios son los siguientes:

- Un nivel alto de confiabilidad y conocimiento de Seguridad Informática de los desarrolladores y administradores de red.

- Implementación de estándares, protocolos, modelos y métodos criptográficos seguros para la validación y generación de certificados o token de seguridad de los usuarios, el envío, recepción y almacenamiento de información sensible.
- Compartimentar los recursos por dominios organizacionales e implementar reglas que validen las operaciones realizadas sobre ellos.
- Establecer políticas de seguridad a todos los niveles para garantizar un nivel alto de granularidad en el proceso de autorización.
- Garantizar la calidad de los datos contenidos en los log para realizar análisis en función de la seguridad y funcionamiento del sistema y la ejecución de los procesos de negocio.
- Integración entre los componentes que conforman el modelo de control de acceso.

En la Figura16 se muestra un esquema que refleja los componentes que integran el modelo CAEM propuesto por el autor de la presente investigación y sus relaciones.

Figura16. Modelo de control de acceso para SI basado en tecnologías web



Fuente: Elaboración propia.

Las principales entradas del modelo lo constituyen las personas convertidas en usuarios, los procesos informatizados, las restricciones o reglas establecidas en los diferentes niveles, los sistemas a los cuales se necesita proveer seguridad y las organizaciones que forman parte del entorno donde se van a desplegar los sistemas. Las salidas generales se reflejan en las configuraciones, reportes o análisis basados en los log de eventos, identidades de los usuarios y certificados o token de seguridad de los usuarios, políticas establecidas y recursos a los que tiene acceso. Adicionalmente cada componente tiene sus propias entradas y salidas que pueden desencadenar cambios o ejecución de acciones en los demás componentes. El objetivo de este modelo es integrar los componentes de identificación y autenticación, autorización y auditoría de manera armónica y de esta forma proveer una solución al escenario.

El flujo del control de acceso lo inicia el componente de identificación y autenticación con la validación de las credenciales suministradas por el usuario. Esta acción desencadena un conjunto de operaciones relacionadas con la identificación y autenticación del usuario y la ejecución de las reglas establecidas. Las operaciones deben ejecutarse utilizando protocolos o estándares definidos para la comunicación segura entre los diferentes componentes que conforman el modelo. Si en el proceso de identificación y autenticación se detecta que las credenciales no son válidas, se deben tomar acciones para prevenir ataques como la denegación de servicios y activar el mecanismo de mensajería según el nivel de seguridad que se requiera. Si la verificación devuelve un resultado satisfactorio, el componente debe retornar como salida el certificado o token de seguridad del usuario y las identidades que se requieran asociadas a su perfil.

El componente de autorización se activa cuando se solicita el acceso a algún recurso, para ejecutar este proceso es necesario recibir como entrada los parámetros retornados por el componente de identificación y autenticación. Cuando se recibe la petición con los parámetros establecidos, el componente de autorización inicia la verificación de los datos suministrados. En caso de no ser válidos, devuelve un mensaje de error informando las causas y aborta la petición. Si los datos son correctos el componente ejecuta la petición, que debe retornar como salida los privilegios o configuraciones de un usuario para construir un menú de acceso, recursos para mostrarle al usuario o validación de la acción ejecutada en el sistema.

El proceso de auditoría, a pesar de no recibir la atención que amerita, resulta determinante si se quiere hacer un uso eficiente del conocimiento generado producto a la ejecución de los

procesos en una organización. Para lograr este objetivo es necesario registrar los eventos que resulten críticos para la organización, cada uno de ellos con los parámetros establecidos en el componente de auditoría. El componente de auditoría recibe como entrada sus configuraciones y la información asociada a cada uno de los eventos ejecutados en él y en los demás componentes del control de acceso. El análisis de la información contenida en los log puede desencadenar cambio en las configuraciones de los demás componentes o en los procesos ejecutados por el sistema.

La retroalimentación del modelo se refleja en el flujo de mensajes, que pueden estar dirigidos a los usuarios a otros componentes, estos mensajes pueden traer consigo alertas, avisos o cambios en las configuraciones iniciales de las políticas, restricciones, los modelos de procesos, entre otros mecanismos asociados con el control de acceso en los demás componentes. Un ejemplo de ello puede reflejarse en el caso que se detecte alguna violación de seguridad cometida por un usuario, inmediatamente el componente de auditoría puede enviar un mensaje al componente de autorización para que desactive su cuenta. De la misma forma se puede evidenciar en el análisis de los errores, si se detecta que una fuente de identificación y autenticación no está respondiendo, el componente de auditoría puede enviar un mensaje a este componente para que active otra fuente y de esta forma garantizar la disponibilidad de los recursos.

CAEM incorpora los elementos necesarios para contribuir al fortalecimiento del control de acceso y de esta forma preservar la seguridad de los recursos gestionados por SI en entornos multidominios. A continuación, se realiza un análisis de los principales aspectos que sustentan esta afirmación:

- Provee los elementos necesarios para implementar arquitecturas SSO.
- Posibilita la federación de identidades de los usuarios entre sus dominios de confianza.
- Propone la gestión dinámica de las identidades de los usuarios y de las fuentes de identificación y autenticación, así como su integración con los métodos criptográficos a utilizar.
- Incorpora el concepto domino para la gestión y compartimentación de los recursos a través de los mismos.
- Establece relaciones entre los usuarios, dominios, organizaciones y roles para la creación de políticas de control de acceso inter e intra-dominios.

- Permite la compartimentación de los recursos a través de reglas que evalúan los criterios que los identifican.
- Incorpora los conceptos necesarios para gestionar los log de eventos en entornos distribuidos y por dominios organizacionales.
- Integra de manera armónica los procesos de identificación y autenticación, autorización y auditoría.

CONCLUSIONES

Los resultados obtenidos durante el desarrollo de la presente investigación permiten concluir lo siguiente:

- A partir de la sistematización de los principales referentes teóricos que sustentan la presente investigación, donde se identifican las principales limitaciones de los modelos existentes en la bibliografía, se aprecia que estos no brindan soluciones para gestionar la seguridad de los recursos en entornos multidominios garantizando un nivel de granularidad alto en el establecimiento de políticas de autorización.
- El modelo propuesto incluye un componente de autorización que extiende las especificaciones de RBAC para incorporar los elementos presentes en los entornos multidominios y el establecimiento de políticas a través de los criterios que identifican a los recursos.
- Se desarrolla un componente de gestión de log que describe los elementos a tener en cuenta para garantizar la completitud de los datos contenidos en los log para realizar análisis en función de la evaluación del cumplimiento de la seguridad, el funcionamiento del sistema y la ejecución de los procesos de negocio.
- El modelo propuesto integra y describe las relaciones e intercambios de información entre los componentes que conforman el control de acceso. Esto permite la retroalimentación entre ellos y que funcionen como un todo de manera armónica con el objetivo de preservar la seguridad de los recursos gestionados por SI en entornos multidominios.
- El modelo propuesto fue aplicado en el desarrollo de un sistema de control de acceso denominado Acaxia lo que sirvió como base para el diseño y aplicación del pre-experimento utilizado para validar la hipótesis de la investigación. Como parte de la experimentación se pudo observar que Acaxia presenta mayor nivel de seguridad en

los procesos que conforman el control de acceso. A partir de estos resultados se constató que el modelo propuesto permite desarrollar sistemas que proveen mayor seguridad para preservar los recursos gestionados en entornos multidominios.

- La solución fue aplicada en entornos reales demostrando su robustez y escalabilidad para adaptarse a entornos heterogéneos. Los resultados obtenidos en estos escenarios de aplicación fueron satisfactorios, avalados por las cartas de aceptación de los clientes.

El impacto y aporte de Acaxia a la seguridad de los recursos gestionados dentro y fuera del país, al ahorro por concepto de sustitución de importaciones y al tiempo de desarrollo a partir de su reutilización han propiciado que haya sido merecedora de varios premios, certificaciones y reconocimientos en varios escenarios.

REFERENCIAS BIBLIOGRÁFICAS

Aalst, W.V.d. (2011). *Process Mining* in *Discovery Conformance and Enhancement of Business Processes*. Springer-Verlag Berlin Heidelberg: New York, USA. p. 241-244.

Al-Janabi, S.T.F. & M.A.-s. Rasheed. *Public-Key Cryptography Enabled Kerberos Authentication*. *Developments in E-systems Engineering*, *IEEE Computer Society*, Dubai, 2011, p. 209-214.

Buijs, J.C.A.M. (2010). *Mapping Data Sources to XES in a Generic Way*, in *Department of Mathematics and Computer Science*. Technische Universiteit: Eindhoven, Nederland. p. 1-123.

Canfora, G., et al. (2011). *How Long does a Bug Survive? An Empirical Study*. *18th Working Conference on Reverse Engineering*, *IEEE Computer Society*, p. 191-200.

Cantor, S., et al. (2005). *Bindings for the OASIS Security Assertion Markup Language (SAML)*, O. Open, p. 1-46. Disponible en: <http://docs.oasis-open.org/security/saml/v2.0/>.

Cover, R. (2009). *Extensible Access Control Markup Language (XACML)*. OASIS: USA. p. 1-89.

Downs, D.D., et al. (1985). *Issues in Discretionary Access Control*. *Symposium on Security and Privacy*, *IEEE Computer Society*, Oakland, USA, p. 208-218.

Davis, G.B. and M. (1985). Olson, *Management Information Systems. Conceptual Foundations, Methods and Development*, N.Y. McGraw-Hill.

Echavarría, I.C.S. (2007). *Contribución a la Validación de Certificados en Arquitecturas de Autenticación y Autorización*. Universidad Politécnica de Cataluña: España. p. 231.

Ferraiolo, D.F., et al. (2001). *Proposed NIST Standard for Role-Based Access Control*, U. National Institute of Standards and Technology (NIST). ACM Transactions on Information and System Security, p. 224-274.

Gerhards, R. & GmbH, A. (2009). *Request for Comments 5424: The Syslog Protocol*, in *5432*, I.E.T.F. (IETF). Disponible en: <http://tools.ietf.org/html/rfc5424.txt>.

Günther, C.W. (2009). *Extensible Event Stream (XES)*, F.P. Laboratories. 2009: Eindhoven. p. 1-22.

Hernández, P., I. Garrigós, & J.N. Mazón. (2010). *Modeling Web logs to enhance the analysis of Web usage data*. *Workshops on Database and Expert Systems Applications*, *IEEE Computer Society*, Bilbao, España, 2010, p. 297-301.

Hodge, J. and R. Morgan, *Lightweight Directory Access Protocol (v3): Technical Specification*, I.N.W. Group. 2002. p. 1-6.

ISO & IEC. (2007). *International Standard ISO/IEC 27002*, ISO/IEC. Switzerland.

ITGI, et al. (2008). *Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa*, I. ITGI, OGC, TSO, p. 1 - 130. Disponible en: <http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf> .

Jianxiao, C., Yimin, W. & Zongkun, W. (2010). *The applied research of access control model in scientific data sharing platform*. *Second WRI Global Congress on Intelligent Systems*, *IEEE Computer Society*, Wuhan, p. 158-161.

Kamal, M. (2011). *An Approach to Designing IT Interventions in Micro-Enterprises to Facilitate Development*. *44th Hawaii International Conference on System Sciences*, *IEEE Computer Society*, USA, p. 1-10.

Karjoth, G., A. Schade, & Herreweghen, E.V. (2008). *Implementing ACL-based Policies in XACML*. *Annual Computer Security Applications Conference*, *IEEE Computer Society*, Anaheim, CA 2008, p. 183 - 192.

Li, C. & Liao, Z. (2009). *An extended ACL for solving authorization conflicts*. *Second International Symposium on Electronic Commerce and Security*, *IEEE Computer Society*, Nanchang, p. 30 - 34.

Li, N. (2008). *How to make Discretionary Access Control Secure Against Trojan Horses*. *Parallel and Distributed Processing Symposium, International*, *IEEE Computer Society*, Miami, FL, p. 1-3.

McIntyre, J.B., Luterroth, C. & Weber, G. (2011). *OpenID and the Enterprise: A Model-based Analysis of Single Sign-On Authentication*. *15th IEEE International Enterprise Distributed Object Computing Conference*, *IEEE Computer Society*, Helsinki, p. 129 - 138.

Medero, G.S. (2010). *Los Estados y la Ciberguerra.* Dialnet, Vol. 317, p. 63-76.

Min, Q. & Fei, X. (2008). *The Impact of Information System Usage on Performance: Based on the innovation perspective*. *International Conference on Information Management, Innovation Management and Industrial Engineering*, *IEEE Computer Society*, Taipei, p. 137 - 140.

Na, C., et al. (2010). *A value-added service model of mining right information*. *International Conference on E-Business and E-Government*, *IEEE Xplore*, Beijing, China, p. 2292 - 2296.

Neuman, C., et al. (2005). *The Kerberos Network Authentication Service (V5)*, I.E.T.F. (IETF), p. 1-16. Disponible en: <www.ietf.org>.

O'Connor, A.C. & R.J. Loomis, R.J. (2010). *Economic Analysis of Role-Based Access Control Final Report*. 2010, National Institute of Standards and Technology (NIST): Gaithersburg, USA. p. 1-132.

Potter, C. & Beard, A. (2010). *Information Security Breaches Survey 2010: Technical report*. Infosecurity Europe: Earl's Court, London, p. 5.

Santos, H. (2011). *Ciberterrorismo. La guerra del siglo XXI.* Dialnet, Vol. 242, p. 14-23.

Suhendra, V. *A. (*2011). *Survey on Access Control Deployment.* Springer Berlin Heidelberg, Vol. 259, p. 11-20.

Wang, G., W. & Li, W. (2010). *Research On Validity Evaluation Of Mandatory Access Control Policy Under LSM Framework*. *International Conference on Computational Intelligence and Security*, *IEEE Computer Society*, Nanning, China, p. 306 - 309.

Wei, L.K. and S. Jarzabek. *A Generic Discretionary Access Control System for Reuse Frameworks*. *COMPSAC '98*, *IEEE Computer Society*, Vienna, Austria, 1998, p. 356 - 361.

Xu, et al. (2009). *Research on Mandatory Access Control Model for Application System*. *International Conference on Networks Security, Wireless Communications and Trusted Computing*, *IEEE Computer Society*, p. 159-163.

Yongsheng, Z., et al. (2010). *Web Services Security Policy*. *International Conference on Multimedia Information Networking and Security*, *IEEE Computer Society*, Nanjing, Jiangsu, 2010, p. 236 - 239.

Yuan, E. & Tong, J. (2005). *Attributed Based Access Control (ABAC) for Web Services*. *International Conference on Web Services*, *IEEE Computer Society*, USA, p. 1-9.

Zhang, Y. & Joshi, J.B.D. (2007). *A Request-Driven Secure Interoperation Framework in Loosely-Coupled Multi-domainEnvironments Employing RBAC Policies*. *Collaborative Computing: Networking, Applications and Worksharing*, *IEEE Computer Society*, New York, p. 25 - 32.