tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

198

HACIA LA IDENTIFICACIÓN ELECTRÓNICA ÚNICA EN LA SEGURIDAD SOCIAL

Santiago Rodríguez Yunta
Jefe de Servicio de Seguridad Internet / Intranet
Gerencia de Informática de la Seguridad Social

Pedro Valcárcel Lucas
Jefe de Servicio de Políticas de Seguridad y Análisis de Riesgos
Gerencia de Informática de la Seguridad Social

Santiago Rodríguez Yunta
Pedro Valcárcel Lucas

Palabras clave

Seguridad, Gestión de identidades, Control de accesos, Provisión de usuarios, Identificación, Autenticación, Autorización.

Resumen de su Comunicación

La Gerencia de Informática de la Seguridad Social está afrontando un proyecto de Gestión de Identidades, para la unificación de la identidad de un usuario sus sistemas de información.

La idea subyacente en este proyecto se basa en los principios de sincronización de identidades, políticas y reglas de negocio, repositorio de autenticación estándar, administración global y delegada, junto con una autenticación única y fuerte.

Con ello se pretende preparar el sistema de información para la apertura a nuevos servicios, no sólo para trabajadores y empresas, sino para otras administraciones públicas.

Santiago Rodríguez Yunta
Pedro Valcárcel Lucas

HACIA LA IDENTIFICACIÓN ELECTRÓNICA ÚNICA EN LA SEGURIDAD SOCIAL

1. Antecedentes

Esta presentación se enmarca dentro de las comunicaciones para el Tecnimap dentro del punto 1 del Temario de las Comunicaciones:

"Estrategias y Planes de desarrollo de la Administración Electrónica".

2. Motivación del proyecto

Una de las funciones de la Gerencia de Informática de la Seguridad Social (en adelante GISS), como órgano común que realiza el soporte informático a las Entidades Gestoras y Servicios Comunes de la Secretaría de Estado de la Seguridad Social, es coordinar las medidas técnicas de los sistemas de información en su ámbito.

Entre otras, debe proporcionar un sistema de seguridad que garantice que se cumplan las medidas en cuanto a autenticación, confidencialidad, integridad, disponibilidad y trazabilidad de la información.

Dentro del apartado de autenticación, que la definiremos en el contexto de este informe como la capacidad de los sistemas de comprobar la identidad de la persona que accede al sistema de información, la GISS ha comenzado un ambicioso proyecto, cuyo objetivo es la unificación de la identidad de un usuario en cualquiera de los entornos informáticos donde esté definido.

Por otra parte, el número de personas involucradas en la gestión de la Seguridad Social ha ido ampliándose paulatinamente a lo largo de los años y actualmente los tipos de usuarios que pueden acceder al mismo se han ampliado. Esto hace que existan varios mecanismos de identificación en los sistemas de información, de los cuales el más importante es SILCON, pero ninguno de ellos almacena el perfil conjunto de todas las autorizaciones en todos los ámbitos.

La administración de usuarios en los sistemas de información actuales

Cuando una persona se incorpora a la organización, debe darse de alta en varios sistemas, como la intranet, el correo electrónico o la red de área local, pero no existe una herramienta que integre y trate esta configuración de forma centralizada, con el consiguiente problema de gestión y de retrasos en la asignación de recursos.

Si se trata de un cambio de una persona de un departamento a otro dentro de la organización, tampoco es visible un perfil que integre el conjunto de autorizaciones que es necesario modificar. Por ello, los cambios en las autorizaciones de esa persona se deben hacer de forma parcial y aislada y accediendo a otros sistemas.

El alta, baja y actualización de las propiedades de los usuarios en los sistemas actuales de la GISS se realiza mediante la aplicación SILCON, que tradicionalmente ha sido el soporte en los entornos de los grandes sistemas, pero en la actualidad existen una serie de problemas cuya solución no es sencilla, como:

- La administración de usuarios no está integrada en todos los sistemas (Unix, Bases de Datos,...).

- Los procedimientos de provisión de usuarios son semimanuales en ciertos sistemas (Notes, red Novell,..).

• Es complejo determinar el conjunto de autorizaciones y permisos de acceso que tiene un usuario.

3. La solución: gestión de identidades

La identidad se entiende como la representación de un individuo (o entidad) dentro de un sistema IT heterogéneo.

Por ello, la Gestión de identidades simplifica el proceso de administrar usuarios: gestión de los accesos / cuentas, las palabras de paso, información asociada. Las funciones típicas de estos sistemas son: directorio, sincronización de identidades (metadirectorio), administración basada en roles, auditoría, informes y registro de eventos.

Esto se realiza mediante una serie de elementos:

• **Sincronización de identidades.** De forma que todas las cuentas o identidades de una persona que accede al sistema informático se puedan administrar desde un sistema común.

• **Perfiles organizativos.** Su objetivo es seguir la estructura de la organización de manera que para cada posición o función dentro de la organización, esté definido un rol que otorgue los privilegios necesarios a los miembros para desempeñar su función

- Identidad es más que Personas: Usuarios, Dispositivos, Aplicaciones / Servicios, y cualquier otro recurso de la organización -

Un perfil de identidad incluye:

Identificación única

Información personal

Credenciales de Autenticación

Permisos de Acceso / Funciones

Información de activos

Preferencias

• **Políticas y reglas de negocio.** Se pueden establecer políticas y normas que regulen los roles de negocio.

Metadirectorio

Nombre: Juan Peña
FNac: 26-Jul-1969
Emp #: 447995
Tlfno: 913901234
Email: jpeña@seg-social.es
Prefs:

Políticas y reglas de negocio

Nombre: Juan A. Peña
Nac: 26/7/69
Emp #: 447995
Salario: 65.000€
Email: jpeña@seg-social.es
Ext: 1234

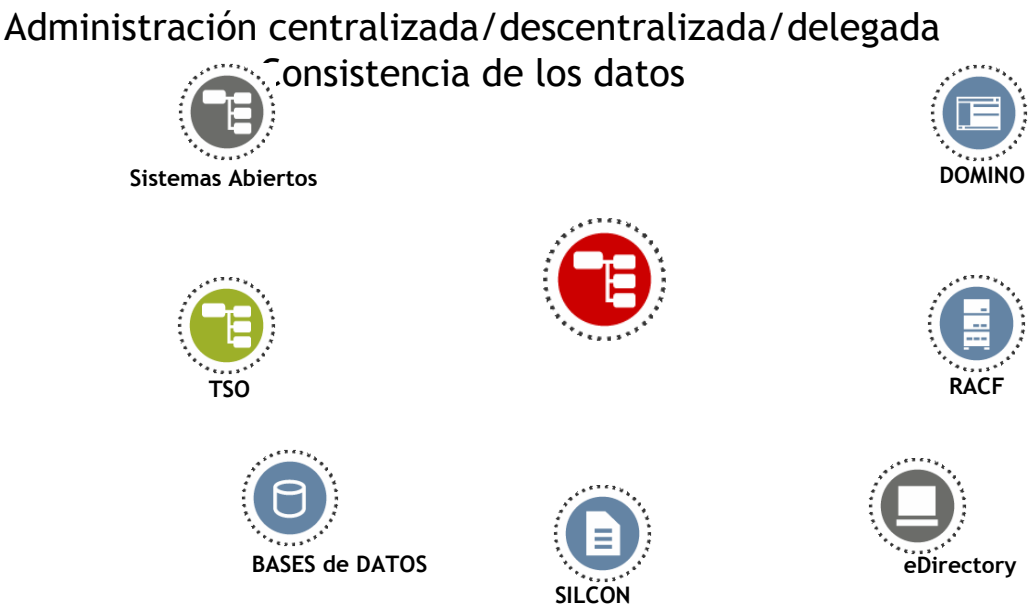
Nombre: J Peña
Tlfno: 3901234

Nombre: Juan Peña
Email: jpeña@seg-social.es
Telefono: 913901234

• **Repositorio de autenticación estándar.** En un único repositorio se almacena la información de la identificación del usuario.

• **Administración global y delegada.** La administración de las cuentas de usuario es conjunta o global, y por ello, es susceptible de poder delegarse en otros organismos o personas.

La administración delegada proporciona la posibilidad de asignar tareas administrativas específicas a usuarios autorizados. Para ello presenta al usuario autorizado solamente las herramientas necesarias para realizar ese conjunto de tareas.



• **Integración con procesos de auditoría.** El proyecto tiene también integración con los procesos de auditoría implantados en la GISS, en los siguientes aspectos:

• Monitorización: Existe la capacidad de muestra gráfica del estado del motor del metadirectorio y de cada uno de los conectores.
• Informes. Con la posibilidad de informes por tipo de evento, sistema sincronizado, objeto sincronizado y la exportación de la información en múltiples formatos.
• Trazas. Consiste en el seguimiento detallado de los eventos de motor, de estado, de operación y de transformación. También permite el almacenamiento para análisis y las auditorías forenses.

4. Beneficios para la organización

Lo que proporciona el sistema a los usuarios de los servicios de la Seguridad Social:

• Consolidación de la información de usuarios en un único punto (repositorio único de usuarios).

• Sincronización de la información de usuarios entre todos los sistemas, aplicaciones y bases de datos en tiempo real. Identidad única.

• Implantación de Procedimientos Efectivos, Rápidos y Seguros para el alta, baja y modificación de usuarios.

• Automatización de los procesos de gestión de usuarios y flujos de trabajo.

• Punto único de gestión de la información de usuario y sus perfiles. Administración global y delegada.

• Login / contraseña unificados y administración única para los usuarios de los diferentes sistemas.

• Gestión de la seguridad de los diferentes sistemas de una manera centralizada.

• Gestión de Usuarios de los sistemas centralizados y descentralizados.

- Mainframe.
- Correo electrónico.
- Red de area local.
- Sistemas abiertos.
- etc ...

5. Conclusiones

Con la administración única de la identidad del usuario, se hace más sencilla la adopción de medidas de seguridad integradas en los sistemas de información, que hará más manejable en el futuro esta labor de seguridad.