

Gestión Avanzada de Identidades

IRENE - Enterprise Identity Management

Dada la creciente relevancia de la IT, la Gestión de Identidades es el catalizador clave necesario que más claramente cumple con los objetivos de contención de costes, control de riesgos, cumplimiento legal, eficiencia operacional y calidad de servicio para los usuarios.

El Grupo SIA cuenta, desde el año 2000, con más de 40 proyectos de éxito, en materia de Gestión de Identidades, implantados en las organizaciones más representativas de nuestro país. En cada uno de ellos, se ha aportado el conocimiento que otorga esta única experiencia, relevando así algunas de las conclusiones y mejores prácticas para optimizar su desarrollo evitando la repetición de errores.

Gestión de Identidades

Los servicios de GID incluyen la automatización de los procesos de aprovisionamiento de cuentas, control de accesos y Single Sign On para usuarios. Pero, además, deben de incluir, entre otros, componentes diferenciadores como la trazabilidad y herramientas de auditoría para verificar el cumplimiento de políticas y normativas, la gestión de usuarios especiales (root, DBAdmin, Administrador), las páginas blancas de empresa y las tarjetas inteligentes.

Los síntomas de una deficiente Gestión de Identidades son claros: tiempo perdido y burocracia hasta que se da acceso a los usuarios, gran cantidad de contraseñas sin modificar, privilegios excesivos que se acumulan y no caducan, accesos que no se autorizan por la persona adecuada, cuentas fantasma de las que se desconoce el propietario y no se atreven a borrar, enormes dificultades para auditar los accesos de un usuario y determinar quién lo autorizó, etc.

En paralelo, es importante dar a conocer y trasladar el valor que aporta la Gestión de Identidades a toda la organización, tanto para arrancar la iniciativa como para llevarla a buen puerto, justificando así la inversión y el cambio.

Aprovisionamiento de Cuentas y Recursos

Uno de los aspectos más importantes en la Gestión de Identidades es la necesidad de gestionar usuarios, cuentas y políticas de acceso a un parque heterogéneo de aplicaciones y servicios.

Igualmente, hay que facilitar un eficiente sistema de altas de nuevos empleados, clientes o partners. Es importante la rápida suspensión en el acceso a los sistemas de aquellos usuarios que han finalizado su relación profesional con la compañía.

Gestión de Contraseñas

La sincronización de contraseñas evita los inconvenientes que sufren los usuarios que deben acceder a diferentes sistemas con múltiples cuentas y contraseñas. De esta manera, los usuarios únicamente deben de cambiar su contraseña en uno de los sistemas.

Un sistema de auto-reseteo de la contraseña evita, además, la gran cantidad de llamadas que se reciben al help-desk de forma habitual, así como los tiempos de espera del usuario afectado.

Gestión de Roles

Un buen sistema de gestión de roles está considerado actualmente como un componente clave en los sistemas de Gestión de Identidades. Permite, de una forma muy efectiva, la creación y asignación de grupos de privilegios que deben corresponder con la estructura organizativa, puesto de trabajo, proceso de negocio, etc.

Ya existen de forma implícita roles o grupos en nuestros Sistemas de Información que resultan alterados cada vez que se solicitan nuevos accesos, o la modificación de los existentes.

El conocimiento, identificación y correlación de estos roles (implícitos o explícitos) aporta una valiosísima información para una correcta Gestión de Identidades, Análisis de Riesgos y Cumplimiento de Normativas y Auditorías.

Gestión de Peticiones, Administración Delegada y Autoservicio (Workflow)

Con una administración delegada, las compañías pueden repartir la carga de trabajo en la gestión del usuario a los correspondientes responsables (por departamento, aplicación, administración delegada, localización geográfica, o cualquier otro criterio). En todos los casos se debe garantizar el control de los derechos sobre los administradores delegados para visualizar, actualizar o borrar únicamente los datos sobre los que es responsable. La implementación de un proceso de Workflow, permite establecer y automatizar un flujo de aprobaciones y acciones encadenadas acorde a la política y método de trabajo de la compañía.

Autenticación y PKI

El uso de Usuario/Contraseña es lo más común y extendido, pero existen otras opciones que fortalecen los mecanismos de autenticación, proporcionando un mayor grado de seguridad (PINs, tokens, etc.). El uso de otro mecanismo, como el certificado digital, facilita y habilita la prestación de otros servicios de seguridad como la firma digital, no repudio, cifrado, etc.

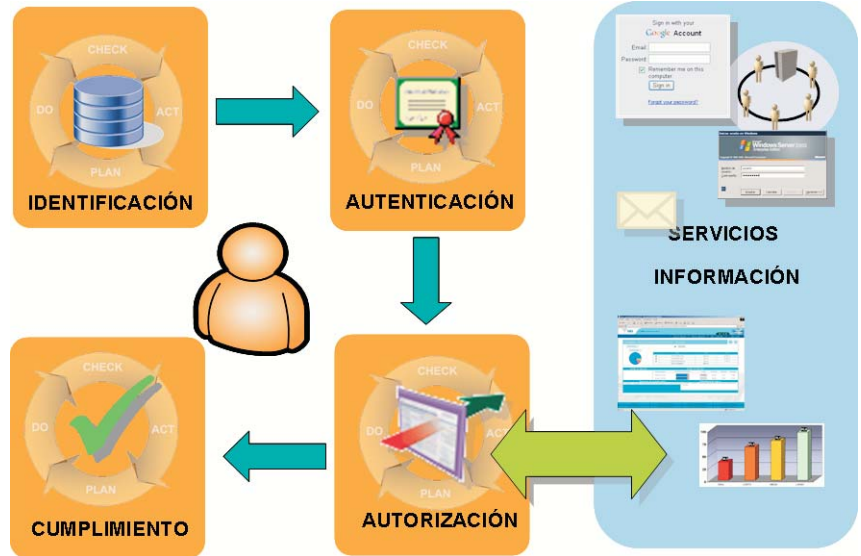


El departamento de Seguridad Informática se convierte en el garante de que la información es accedida por la persona que la necesita con los mínimos privilegios requeridos para realizar su trabajo, siendo percibido por la organización como habilitador de los procesos de negocio en lugar de como un freno

Logon reducido y Single Sign On Corporativo

La necesidad de acceder a diferentes aplicaciones y servicios, normalmente con distintas credenciales y contraseñas, conlleva grandes inconvenientes a los usuarios que se ven forzados a introducir sus distintas credenciales en cada uno de los sistemas/aplicación a los que desean acceder, así como a mantener una lista de las mismas.

Los mecanismos de SSO, ya sea para entornos WEB o de escritorio, mejoran la confortabilidad de los usuarios en el acceso a los diferentes sistemas y aplicaciones, debiendo recordar y usar una sola vez una única credencial.



Control de acceso

Los sistemas de Gestión de Accesos, aplicaciones WEB, legacy o cualquier otro recurso, deben soportar y forzar el cumplimiento de las políticas y reglas que gobiernan el acceso a los recursos, tanto para los usuarios internos como para los externos. El sistema debe mantener, de forma consistente, la política de accesos de forma centralizada, evitando así la dispersión y la falta de control sobre las configuraciones.

La política de accesos debe manetener un conjunto de reglas sobre quién tiene accesos a qué en base a su rol. Las consideraciones sobre la privacidad han de estar presentes.

Auditoría y Cumplimiento de Políticas

El cumplimiento de las políticas de seguridad y regulaciones son siempre de obligado cumplimiento. La centralización sobre la gestión de los usuarios permite establecer los puntos de control más adecuados para su seguimiento y auditabilidad. Se facilita el conocimiento sobre cambios de privilegios no autorizados, cuentas fantasma, contraseñas débiles, etc.

La auditabilidad del sistema proporcionaría toda la información necesaria para verificar el grado de cumplimiento y no conformidad sobre las normas, políticas o regulaciones precedentes, como ISO17799, Basilea II, PCI, Sabarnes Oxley y HIPAA.

Usuarios privilegiados

En todo el sistema GID, son de especial atención los usuarios con privilegios especiales o Administradores de Sistemas que, en muchas ocasiones, son personal externo. Se hace necesario proteger y vigilar este tipo de accesos, al mismo tiempo que garantizar la identidad real de la persona que lo usa y su trazabilidad.

Igual de importante es liberar a los Administradores de los sistemas de la tediosa gestión de las cuentas y contraseñas que deben ofrecer a este tipo de usuarios (generación de contraseña, custodia de la misma), proporcionando mecanismos de autoprovisión completamente auditados.

Federación

La Federación extiende las capacidades de la Gestión de Identidades a diferentes dominios de seguridad, como podrían ser los entornos B2B donde se podrían aportar mecanismos de seguridad basados en la identidad. Los estándares de Servicios WEB de Seguridad, Liberty Alliance y otros, definen las especificaciones técnicas y de negocio necesarios para habilitar la federación.

Adicionalmente, la federación puede ser usada internamente para conseguir altos grados de interoperabilidad entre unidades de negocio descentralizadas y autónomas.

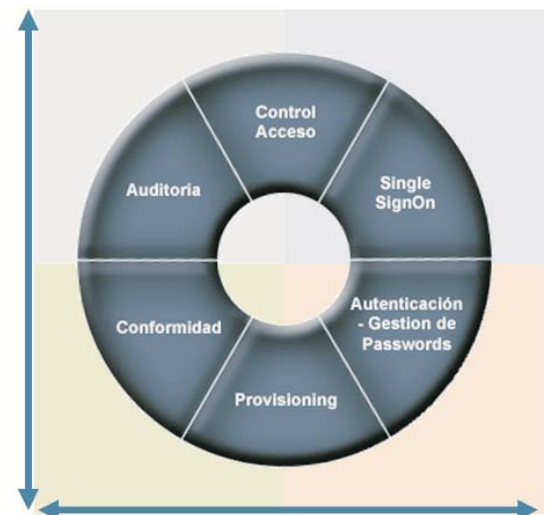
Otra funcionalidad que aporta un sistema de Federación es la obtención de un SSO entre dominios de seguridad independientes a los que un mismo usuario debe tener acceso.

Valores y beneficios

- Reducción de costes operacionales
 - Reducción de esfuerzo y tiempos de provisión y resolución de incidencias
 - Reducción de errores e incremento de la productividad
- Control de Riesgos
 - Implantación de políticas de seguridad
 - Reducción de impacto y probabilidad de incidentes motivados por suplantación o abuso
 - Cumplimiento legal
 - Visibilidad centralizada de las autorizaciones e información de identidad y acceso
- Mejora de la experiencia del usuario
 - Una contraseña
 - Autoservicio: Cambio de contraseña, peticiones de acceso
 - Único punto de acceso
- Ventaja competitiva
 - Habilitador de relaciones de negocio

Control de Acceso

Gestión Identidad

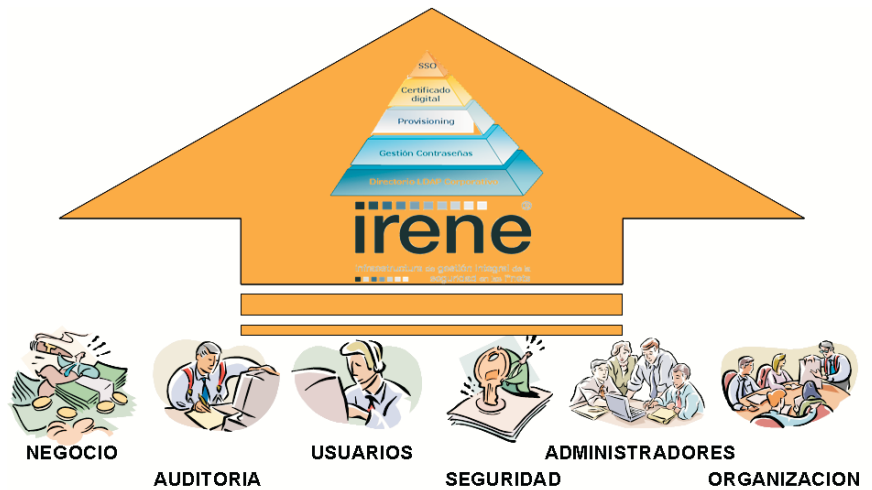


Control de Riesgos

Usabilidad

Consultoría, Integración, Servicio

Es de gran importancia contar con el apoyo de un proveedor experimentado y comprometido, que permita abordar este tipo de proyectos por módulos (consolidación, single sign on, aprovisionamiento, autenticación fuerte, ...) y que además ofrezca a la organización beneficios a corto y medio plazo sin perder la visión y estrategia dirigida al logro de objetivos a largo plazo.



Funcionalidad	Características	Beneficios
<ul style="list-style-type: none"> ■ Aprovisionamiento en sistemas y aplicaciones 	<ul style="list-style-type: none"> • Componente fundamental para dar de alta, baja y modificaciones a usuarios • Integración con los sistemas nativos de seguridad • Despliegue con o sin agentes en los sistemas 	<ul style="list-style-type: none"> • Automatización del trabajo de Administradores de Sistemas. Reducción de los tiempos de aprovisionamiento de recursos a empleados, socios y clientes • Homologación de políticas de acceso a recursos • Unificación de repositorios de usuarios
<ul style="list-style-type: none"> ■ Logon reducido 	<ul style="list-style-type: none"> • Utilización del mismo identificador de usuario y contraseña en los distintos entornos 	<ul style="list-style-type: none"> • Facilidad para el usuario, reduciendo el número de identificadores y claves de acceso que necesita para trabajar • Mejora la seguridad evitando que se compartan usuarios o se apunten las claves • Reducción de incidencias con el CAU relacionadas con olvidos de contraseñas o reseteo de usuarios
<ul style="list-style-type: none"> ■ Single Sign On 	<ul style="list-style-type: none"> • Sólo se suministra una vez la identificación de usuario y contraseña, y se conecta de forma transparente a las aplicaciones 	<ul style="list-style-type: none"> • Facilidad para el usuario, porque sólo se autentica una vez y obtiene acceso transparente a las aplicaciones y sistemas en que trabaja • Mejora de la seguridad evitando que se compartan usuarios o se apunten las claves • Reducción de incidencias con el CAU relacionadas con olvidos de contraseñas o reseteo de usuarios
<ul style="list-style-type: none"> ■ Sincronización de contraseñas 	<ul style="list-style-type: none"> • Cambio automático de las contraseñas en las plataformas sincronizadas 	<ul style="list-style-type: none"> • Reducción del número de contraseñas requeridas • Menor coste por incidencias con el CAU en relación con olvidos de contraseñas o reseteo de usuarios
<ul style="list-style-type: none"> ■ Autenticación fuerte 	<ul style="list-style-type: none"> • Combinación de métodos de autenticación • Id usuario/contraseña • Certificados digitales • Tarjetas inteligentes • Biométricos 	<ul style="list-style-type: none"> • Flexibilidad para combinar distintos mecanismos de autenticación permitiendo adaptar el nivel de seguridad en función del tipo de acceso o activo • Permite integrar en el sistema el DNIe (u otros certificados o tarjetas inteligentes) y la Incorporación de Firma Digital
<ul style="list-style-type: none"> ■ Federación 	<ul style="list-style-type: none"> • Integración de dominios distintos de gestión de identidades • Integración en entornos SOA - Web Services • Soporte SAML, Liberty 	<ul style="list-style-type: none"> • Muy importante en los nuevos entornos SOA-Web Services • Permite la combinación de dominios distintos de gestión de identidades en caso de fusión de organizaciones • Implementa los nodos de IdP (Identity Provider) y SP (Service Provider). Permite la generación de los token SAML para autenticación en otros entornos (Web Services Single Sing On)

Funcionalidad	Características	Beneficios
<ul style="list-style-type: none"> ■ Gestión de Peticiones - Autoservicio 	<ul style="list-style-type: none"> • Workflow de Peticiones y Autorizaciones • Delegación de Autorizaciones • Autoservicio de recursos autorizados • Recuperación automática de contraseñas 	<ul style="list-style-type: none"> • Permite implantar procesos de administración distribuida, donde los que necesitan los recursos pueden solicitarlos y la autorización depende de los responsables de los activos. Permite flexibilizar la administración mediante la delegación de las autorizaciones y habilita el autoservicio de peticiones simples o repetitivas (como el reseteo de la cuenta para recuperar la contraseña)
<ul style="list-style-type: none"> ■ Perfilado de usuarios 	<ul style="list-style-type: none"> • Descubrimiento e identificación de roles técnicos • Ingeniería y gestión de roles • Identificación de colectores de recursos y separación de responsabilidades 	<ul style="list-style-type: none"> • Simplifica la administración y la operación del día a día • Permite mantener el nivel adecuado de seguridad • Permite identificar las agrupaciones más comunes de derechos, o asignar recursos por analogía con otros usuarios • La ingeniería de roles es un proceso dinámico que permite la identificación de usuarios colectores de derechos, usuarios que infringen la separación de responsabilidades y también la identificación de recursos utilizados (o no utilizados)
<ul style="list-style-type: none"> ■ Gestión de la organización 	<ul style="list-style-type: none"> • Uso social de usuarios, recursos y organización • Geolocalización • Páginas Blancas 	<ul style="list-style-type: none"> • La información del sistema de Gestión de Identidades dispone de gran cantidad de información sobre usuarios, recursos, departamentos, roles, etc., de utilidad para compartir con el fin de mantener organigramas actualizados, directorios de recursos (páginas blancas), geolocalización
<ul style="list-style-type: none"> ■ Auditoría y cumplimiento 	<ul style="list-style-type: none"> • Registro de autorizaciones, quién, qué, cuándo • Auditoría de acceso a recursos • Contraste de cumplimiento de normativas y políticas • Alertas sobre incumplimientos 	<ul style="list-style-type: none"> • Permite la generación automática de informes de auditoría sobre asignación de recursos • Permite la elaboración de contrastes de cumplimiento con distintas normativas y políticas internas • Permite la generación de alertas en caso de incumplimientos, como la separación de responsabilidades
<ul style="list-style-type: none"> ■ Usuarios privilegiados 	<ul style="list-style-type: none"> • Control de usuarios privilegiados (root, admin., super-usuarios, DBA) • Identificación obligatoria de usuarios privilegiados • Auditoría de asignación de privilegios 	<ul style="list-style-type: none"> • El Portal de Administrador permite la identificación y autenticación de cada administrador o usuario privilegiado, para evitar que actúen como super-usuarios (root, Administrador, ...) anónimos • Permite la asignación temporal de estos privilegios, lo que es esencial en los casos de subcontratación de la administración de sistemas • Guarda registro de todas las asignaciones para análisis forenses en situaciones de problemas o fraudes

Otras soluciones de seguridad

SIA, como proveedor global de Seguridad, consciente de la importancia y trascendencia que una adecuada Gestión de Identidades tiene para sus clientes, dispone de una serie de soluciones relacionadas que la complementan y facilitan:

- Consultoría de perfilado de usuarios
- Elaboración de Políticas
- Servicios Gestionados de Administración de Usuarios
- Accesos Remotos



www.sia.es

Avda. de Europa, 2 · Alcor Plaza · Edificio B
Parque Oeste Alcorcón · 28922 Alcorcón
Tel: +34 902 480 580 Fax: +34 913 077 980

Roger de Llúria, nº 50
08009 Barcelona
Tel: +34 902 480 580 Fax: +34 93 467 58 30

delivering value