

# Modelo de seguridad empleado en sintetice



**Sintetice**  
Cms&Framework



# Sintetice

Cms&Framework

## Tabla de contenido

1. [Presentación](#)
2. [Estructura de seguridad básica](#)
- 3.



## Presentación

*Sintetice* aplica naturalmente "juegos" de restricciones de seguridad a los documentos que aloja, de modo que los usuarios que no cuentan con una autorización, adecuada, no puedan tener acceso a los mismos. Para ello se definen *grupos de usuarios* y se establecen *privilegios de acceso* por tipo de documento, de modo que cada grupo puede acceder y/o modificar únicamente aquellos tipos para los que le han sido otorgados los privilegios necesarios para ejecutar cada acción (creación, lectura, modificación, revisión, etc). Y, en caso de no contar con privilegio de lectura, ni siquiera le aparecen en los listados de documentación existente.

Más aún, **cuando existen necesidades de confidencialidad absoluta**, integra restricciones mediante utilidades criptográficas de modo que el acceso a los mismos esté condicionado al uso de claves especiales para poder decodificarlos, luego de transferidos, y leerlos después, fuera de línea (en entornos privados).

Estos hechos dan lugar a dos estructuras de seguridad complementarias:

1. Una estructura de seguridad básica de uso general para todos los usuarios en circunstancias de operación normal. y
2. Una estructura formada por un conjunto de utilidades criptográficas orientado a garantizar la confidencialidad de los documentos que la requieran en los procesos de circulación y acceso a los mismos, de modo que bajo ninguna circunstancia circulen decodificados (como textos planos).

Obviamente, *Sintetice* no puede garantizar lo que pase con dichos documentos una vez se encuentren en manos de quienes tienen derechos de acceso a ellos. Sólo puede garantizar que circulan sujetos a las restricciones de seguridad ofrecidas.

Adicionalmente, la velocidad de operación, en la preparación y transferencia de claves y documentos encriptados, está condicionada a la eficiencia de los algoritmos criptográficos y, puede evidenciar pequeños retrasos en los tiempos de operación haciéndose molesto para algunos usuarios.

## Estructura de seguridad básica

Dado que *Sintetice* está orientado al manejo de sitios web orientados a la gestión documental, es natural pensar que los sitios que soporta muestran páginas públicas que pueden ser visitadas por cualquiera; en particular su página principal. En consecuencia, su administrador(es) debe decidir qué parte de la información es pública, cual es privada y cuales son los mecanismos de acceso disponibles para sus visitantes. Así, establece mecanismos de control de usuarios, y de control de acceso a contenidos.

## Control de usuarios

Luego de instalar un sitio que emplea *Sintetice* se debe decidir las condiciones en que sus eventuales visitantes pueden crear cuentas. Es la primera tarea a realizar, incluso antes de decidir cómo será su portada, pues de ella depende su funcionamiento (a no ser que no se piense tener usuarios registrados y sólo se vaya a distribuir algún tipo de información pública).

Debe entrar a la opción de menú Administración y en el bloque Usuarios y usar el enlace Preferencias administrativas para gestión de usuarios (imagen abajo).

Siteticce local Inicio Contenido **Administración** Ayuda Luis Guillermo

Administrar contenido Construcción del sitio Configuración del sitio Administrar usuarios Reportes

## Construcción del sitio

Controla la apariencia y el funcionamiento básico del sitio.

**Bloques**  
Establecer los bloques de contenido y cómo deben ser ubicados en las diferentes regiones de las páginas del sitio.

**Menús**  
Controla el menú de navegación del sitio, define los enlaces primarios y secundarios y permite renombrar, reorganizar y agregar ítems y menús personalizados.

**Modulos**  
Habilita/deshabilita los módulos instalados en el sitio. Permite extender en tiempo de producción las funcionalidades instaladas.

**Temas**  
Establece qué temas son usados en el sitio y si los usuarios pueden personalizar el que se usa en sus páginas.

## Configuración del sitio

Ajusta las preferencias básicas del sitio.

**Acciones**  
Administra las acciones definidas para el sitio.

**Comportamiento del sitio**  
Establece la página de inicio, alterna los modos de depuración y producción y el estatus del sitio On/Off de modo que se muestre un mensaje de alerta a los visitantes, mientras se ejecutan tareas de mantenimiento del mismo.

**Fecha y hora**  
Configurar cómo se muestran los datos de fecha y hora a los usuarios y cual es la zona horaria usada para registrar la información del sistema.

**Información del sitio**  
Establece la información básica del sitio, tal como nombre del sitio, lema, dirección de contacto (e-mail), misión, página de inicio, etc.

**Reporte de errores**  
Establece las características generales de las páginas de notificación de errores como 403/404 entre otros.

**Sistema de Archivo**  
Establece preferencias de archivo (ubicación, tipos admitidos, tamaño, etc.)

## Reportes

Ver reportes del registro de eventos del sistema e información de estatus.

**Reporte de estatus**  
Obtiene un reporte actualizado del estatus del sitio e informa de los problemas de estatus detectados.

## Administración de contenidos

Página de administración de contenidos.

**Contenidos**  
Ver, editar, administrar y borrar contenidos.

**Estructura categorial**  
Administra la estructura de categorías del sistema de etiquetado y clasificación multidimensional empleado para organizar los contenidos.

**Palabras claves**  
Administra el subsistema de etiquetado libre de los contenidos.

**Preferencias de publicación**  
Controla opciones generales de publicación tales como longitud de resúmenes (para casos no establecidos), exigencia de vista previa antes de publicar, número de publicaciones en la página principal, etc.

**Preferencias del sistema de ayudas**  
Establece preferencias para el sistema de ayudas: longitud de listados, estilo de presentación, etc.

**Taxonomía**  
Administra el subsistema de etiquetado, categorización y clasificación de contenidos mediante una taxonomía.

**Tipos de contenido**  
Administra el modelo de datos del sitio. Permite establecer qué información se recoge, cómo está organizada y cómo debe ser mostrada.

## Administración de usuarios

Ofrece las funciones básicas para administrar usuarios, roles, permisos, reglas de acceso etc.

**Evaluación de usuarios**  
Ofrece una página para gestionar condiciones que afectan la reputación de los usuarios y establecer nexos entre está y los roles de modo que al ganar reputación se pueda acceder a algunos privilegios.

**Preferencias administrativas para gestión de usuarios**  
Establecer las preferencias generales para control de usuarios, acceso, registro etc.

**Reglas de acceso**  
Listar las reglas de acceso definidas y crear o gestionar filtros especiales para control de acceso.

**Roles - Grupos de usuarios**  
Ofrece el listado de grupos de usuarios y permite editarlos, administrar sus configuraciones y gestionar privilegios de acceso por rol.


**Usuarios**  
Ofrece la lista de usuarios registrados y permite gestionar su relación con el sitio.

© 2017 - 2022 by Sinteticce - soluciones informáticas. All rights reserved.

Una vez allí. Se establece el mecanismo de creación de usuarios (y si se desea se pueden configurar los mensajes por defecto para las acciones vinculadas con los procesos administrativos de su vínculo con el sitio web):

#### ► Mecanismo de registro

- Sólo los administradores pueden crear cuentas
- Los visitantes que cuenten con invitación pueden registrarse automáticamente
- Los visitantes pueden registrarse y crear su cuenta libremente
- Los visitantes pueden registrarse pero la cuenta debe ser autorizada por un administrador

 : Los administradores crean las cuentas de usuario y se comunican con los usuarios para entregarles sus credenciales. Es ideal para intranets y redes empresariales en las que sólo personas conocidas van a actuar como usuarios registrados.

Como se ilustra en la imagen hay 4 opciones para registro de nuevos usuarios:

1. Sólo los administradores pueden crear cuentas (ideal para intranets y redes empresariales). Un administrador crea las cuentas y notifica a los futuros usuarios entregándoles credenciales de acceso. Mientras el sitio no sea puesto en producción se sugiere mantener la creación de cuentas sujeta a esta opción.
2. Los visitantes que cuenten con invitación pueden registrarse (ideal para redes educativas y similares en las que un comprobante de matrícula o un documento similar, con número de serie, e identificación, permite al sistema validar la autorización del registro).
3. Los visitantes pueden registrarse libremente. En redes públicas (foros, etc) dónde un modelo de participación hace posible controlar privilegios, puede ofrecerse.
4. Los visitantes pueden registrarse libremente, pero se requiere una acción de validación realizada por un funcionario a cargo. Es muy similar al tercer caso, pero permite aplicar filtros iniciales.

Para los casos en que se necesita, limitar el acceso, a personal vinculado estrechamente con la institución que impulsa el sitio se sugiere establecer uno de los dos primeros modelos y agregar un mecanismo de contacto en las páginas públicas.

Si el sitio debe publicitar opciones comerciales y eventualmente promover el acercamiento de personal indeterminado se sugiere emplear el tercer mecanismo, integrando un protocolo de calificación de la actividad adelantada por los visitantes registrados, de modo que se les pueda elevar progresivamente sus privilegios.

## Grupos de usuarios - Roles

Una vez definido el mecanismo a emplear para creación de cuentas se debe proceder a crear algunos grupos de usuarios (En *Sintetice* se los llama **Roles** - imagen).



Un grupo de usuarios se define mediante la **asignación de un nombre y eventualmente una pequeña descripción** (con funciones nemotécnicas para los administradores). En principio todos los grupos son indistinguibles, ninguno tiene algo que lo haga especial. **Sólo cuando les son asignados privilegios** adquieren funcionalidad y cobran sentido. No hay límite para la creación de grupos.

*Sintetice* ofrece tres grupos por defecto (aunque como se dijo arriba en un primer momento no se distinguen en un sentido funcional):

1. **Usuario anónimo:** Es asignado automáticamente a todos los visitantes que no se hayan registrado, o que habiéndolo hecho no han realizado proceso de acceso.
2. **Usuario registrado:** Es asignado a todos los usuarios que han creado una cuenta y la están usando para acceder alguna página publicada en el sitio web.
3. **Usuario administrador:** Es asignado (en principio por el superadministrador) a usuarios que van a realizar tareas delicadas en la administración del sitio.

Es **tarea importante** del superadministrador (creador del sitio) **asignar privilegios iniciales** a estos tres grupos de usuarios, para que se diferencien y adquieran sentido.

Cuando sea necesario crear un Grupo de usuarios basta con usar el enlace situado bajo la lista de roles, en la página de administración de los mismos (imagen abajo). Y, una vez creado establecer sus privilegios.

Nombre del rol	Descripción	acciones
Usuario anónimo	se asigna por defecto a los visitantes que no realizan proceso de validación de credenciales de acceso.	no editable <a href="#">privilegios</a>
Usuario registrado	Se asigna a todos los usuarios que poseen una cuenta y validan sus credenciales de acceso	no editable <a href="#">privilegios</a>
Usuario administrador	Usuarios que cuentan con permisos especiales para administrar funciones <i>sensibles</i> del sitio web. <b>Este rol de acceso a funciones especiales asignarlo sólo a usuarios confiables</b>	no editable <a href="#">privilegios</a>
Evaluador	Usuario a cargo de un proceso de evaluación del funcionamiento del sitio	<a href="#">editar</a> <a href="#">privilegios</a>

▼ [Agregar rol](#)

Para establecer los privilegios generales de un grupo basta con usar el enlace situado a su derecha (en la lista) aunque, no se define allí algunos privilegios específicos, que determinan la posibilidad de ver o no algunos objetos usados para presentar partes y/o funciones de manejo de contenidos.

## Asignación de privilegios a los Grupos de usuarios

En *Sintetice* han sido establecidos tres mecanismos para hacer asignación de privilegios; dos de ellos situados en el conjunto de páginas de administración de usuarios y el otro situado en las páginas de configuración de los objetos (bloques, tipos de contenido, menús, etc) a los que estos van a ser asignados.

1. Al hacer click en el enlace de la derecha de un rol, en la lista de roles, se abre una página en la que se puede elegir los que serán asignados al mismo (imagen)

Administración de usuarios: Usuarios Roles Evaluación Privilegios Preferencias Reglas de acceso

Privilegios del rol "Usuario administrador"

Marque las casillas de verificación para los privilegios (permisos) que desea asignar a los miembros del grupo **Usuario administrador**. Algunos privilegios, como "administrar ..." suponen la asignación automática de otros del mismo grupo como "accesar, ver, editar o crear". Se recomienda tenerlo presente para asegurar que la validación de acceso sea más rápida. Salvo casos especiales como páginas de usuario o tipos de contenido en los que el modelo de definición lo restringe, los permisos fuertes asignan automáticamente los más débiles del juego correspondiente (ej: crear y modificar, asignan, acceder). Algunos módulos, establecen reglas de acceso especiales para usuarios individuales; debe tener presente este hecho, porque aquí se establecen para grupos, y aquellos pueden negar el acceso a los miembros de un grupo autorizado que no hayan recibido autorización explícita.

▶ Módulo: Administrador de bloques

Administrar bloques

Establecer visibilidad de bloques

Usar PHP para controlar visibilidad

▶ Módulo: Administrador de usuarios

Administrar privilegios

Administrar usuarios

Accesar perfiles de usuario

Cambiar su propio nombre de usuario

▶ Módulo: Administrador del menú

Administrar el menú

**Siguen los privilegios de otros módulos**

basta marcar los que serán asignados y dejar sin marca los que deben ser negados. Los nombres de los privilegios son suficientemente descriptivos (autoexplicativos) y cabe esperar que no necesiten comentarios adicionales para ser entendidos.

2. En el menú interior de las páginas de administración de usuarios aparece la opción **Privilegios** (se resalta con gris cuando se desliza el mouse sobre ella) y da acceso a una página en la que se listan los módulos que ofrecen funciones de configuración de los mismos:

Sitetice local Inicio Contenido Administración Ayuda Luis Guillermo

Administrar contenido Construcción del sitio Configuración del sitio Administrar usuarios Reportes

Administración de usuarios: Usuarios Roles Evaluación Privilegios Preferencias Reglas de acceso

Esta página le da acceso a los formularios para administrar privilegios de acceso implementados por los diferentes módulos. No se reúnen en una sola lista pues podría llegar a ser inmanejable y convertirse en invitación al error.

Úsela para elegir el módulo para el que desea establecerlos; en cada caso se ofrecen enlaces para entrar a formularios de asignación específica. En la lista de asignación encontrará un resumen del estado de asignación de los mismos.

**Administrador de bloques**  
Ofrece las utilidades necesarias para definir, implementar y mostrar bloques en las páginas.

**Administrador de usuarios**  
Ofrece las utilidades necesarias para definir, implementar y controlar contenidos por usuario.

**Administrador del menú**  
Ofrece las utilidades necesarias para definir, implementar y mostrar menús en las páginas.

**Clasificación multidimensional**  
Módulo controlador del sistema de clasificación multidimensional Dewey ampliado a base 36<sup>2</sup>.

**Editor de ayudas**  
Asistente para editar y navegar ayudas, al vuelo, en tiempos de desarrollo y producción.

**Gestor de registros de documentos**  
Ofrece un tipo de contenido base para administrar el registro de documentos.

**Gestor de taxonomías**  
Habilita la categorización de contenidos. Creación y mantenimiento de etiquetas y de asociaciones dinámicas de contenidos con las mismas.

**Mentefactos**  
Soporte para crear redes conceptuales y categoriales con el fin de enlazar y clasificar la información en estructuras significantes.

**ZfExtensor**  
Gestiona extensiones al vuelo. Permite extender Zend en tiempo de producción a la manera de Drupal6x.

© 2017 - 2022 by Sintetice - soluciones informáticas. All rights reserved.

Al hacer click sobre uno cualquiera de ellos se accesa la página de configuración de los mismos. ej:

Sitetice local Inicio Contenido Administración Ayuda Luis Guillermo

Administrar contenido Construcción del sitio Configuración del sitio Administrar usuarios Reportes

Administración de usuarios: Usuarios Roles Evaluación Privilegios Preferencias Reglas de acceso

Elija el rol a autorizar : Usuario anónimo Elegir rol anular elección

Privilegios del rol Usuario anónimo en módulo: Clasificación multidimensional

- Administrar clasificaciones jerárquicas
- Crear clasificaciones jerárquicas
- Editar clasificaciones jerárquicas
- Editar clasificaciones jerárquicas propias
- Eliminar clasificaciones jerárquicas
- Eliminar clasificaciones jerárquicas propias
- Accesar clasificaciones jerárquicas
- configurar la clasificación jerárquica

Establecer privilegios Cancelar

© 2017 - 2022 by Sintetice - soluciones informáticas. All rights reserved.



En ella se encuentra un control de lista para elegir uno a uno el rol a configurar, se marcan las opciones a otorgar y acto seguido se activa el control establecer privilegios.

- Finalmente, algunos elementos como los bloques (ver modelo gráfico de *Sintetice*) permiten establecer en sus páginas de configuración a quienes van a ser mostrados.

Los tipos de contenido, al ser configurados, ofrecen la posibilidad de configurar todos sus privilegios sin necesidad de regresar a las opciones que ya fueron presentadas. Esto es muy importante en el caso de contenidos confidenciales o que requieran restricciones significativas pues pueden ser establecidos, uno a uno en función de la necesidad.

## Inclusión de usuarios en los Grupos (asignación de roles)

Para otorgar privilegios a un usuario se lo debe incluir en al menos un grupo de modo que la suma de grupos en los que sea incluido posea los privilegios que se desea otorgarle. De esta manera, un usuario puede tener privilegios derivados de pertenecer a varios grupos. Un usuario puede ser incluido en tantos grupos como sea necesario y excluido de los que posean derechos que no le deban ser concedidos. Para hacerlo, en la página de usuarios, aparece una lista con controles de comando:

Elija un filtro adecuado para trabajar con un número limitado de usuarios. Hará la lista más amigable. Use el az y el paginador para recorrerla y buscar los que deba procesar. (El paginador se muestra cuando la lista contiene más de 15 items)

Las acciones ofrecidas en el control de menú emergente, situado bajo la lista, aplican a todos los items marcados.

(*)	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
S	T	U	V	W	X	Y	Z												
Id	Nombre de usuario	Roles	Estado	Registrado	Acceso	acción													
<input type="checkbox"/>	1	Luis Guillermo	<input checked="" type="checkbox"/>	2020/09/15	2022/11/09														
<input type="checkbox"/>	2	Santiago	<input checked="" type="checkbox"/>	2020/11/15	2022/03/28														
		Usuario administrador																	

Filtro ? : [ninguno] v

acción ? : [ninguno] v

basta con marcar los cuadros a izquierda de sus nombres y elegir la acción a ejecutar sobre el conjunto electo en la lista titulada **acción** a la derecha. O, en caso de querer afectar a un sólo usuario hacer click en el lápiz situado en la columna acción a la derecha del nombre.

En tal caso se ingresa a la página de edición de la información administrativa del usuario, donde es posible establecer a qué grupos pertenece usando el control de comando [ elegir roles ] imagen abajo:

### Administración de usuarios:

#### Modificación de cuenta del usuario "Santiago"

Esta página está dispuesta para hacer cambios administrativos a las cuentas de usuario. No da acceso a la información de perfil - que es personal y privada. Úsela para asignar/quitar privilegios, modificar el estatus y recuperar las claves de acceso manualmente, si algún usuario lo solicita.

Nombre de usuario\*: Santiago

Escriba el nombre de usuario sin caracteres especiales u ortográficos. Puede contener números dígitos, letras del alfabeto latino, espacios y guiones. No se admiten barras, inclinadas o no, ni guiones bajos.

Correo (e-mail)\*: santiagoquevedo @ sintetice.com

#### Cambio de password

Generar y asignar clave aleatoria

Clave de acceso:

Confirmar clave:

Roles: Elegir roles desvincular todo Romper nexos

Usuario administrador

Estado: inactivo activo bloqueado en observación

Enviar correo de notificación al usuario

Guardar cambios Cancelar

## El mecanismo básico de control de acceso

Como síntesis de las características descritas tenemos un modelo de seguridad básico general: Se definen las circunstancias en que los usuarios / visitantes a un sitio web creado con sintetice pueden obtener una cuenta, acto seguido se crean tantos grupos como sea necesario y se establece, en función de las necesidades que privilegios de acceso se otorga a los mismos. Cuando se necesita, que un usuario posea unos privilegios se incluye dentro de uno de dichos grupos. Cada usuario puede pertenecer simultáneamente a varios grupos cuando se desea ofrecerle combinaciones de privilegios que en general deban permacer separados para la mayoría. Si conviene que un conjunto significativo de usuarios posea un determinado privilegio, basta con crear un grupo, asignarle el privilegio e incluir dichos usuarios en el mismo; de esta manera, no hace falta modificar los grupos creados con anterioridad y se evitan posibles conflictos de asignación inconveniente de permisos.

# Confidencialidad

Existen casos en los que las medidas de seguridad básica pueden parecer insuficientes y requieren del uso de utilidades criptográficas complementarias para proteger información sensible, que no debe ser vista accidentalmente o por acciones de espionaje.

Para ellos *Sintetice* ofrece un módulo utilitario "**confidencialidad**" que administra el alojamiento e intercambio de información que debe ser guardada y circular bajo medidas extremas de protección. Este módulo ofrece los siguientes servicios:

1. Creación de roles seguros en los que cada usuario registra una clave pública<sup>1</sup> que va a ser usada para entregarle encriptada la información alojada de modo seguro en el servidor.
2. Alojamiento de información segura: Los usuarios proveedores de la información que deba alojarse de modo seguro, reciben o consultan la clave pública del sitio, encriptan la clave simétrica usada para cifrar la documentación y suben al servidor el par de elementos información cifrada y clave simétrica de acceso al material debidamente encriptada. Esta documentación nunca es desencriptada en el servidor.
3. Transferencia segura de la información: Cuando un usuario con autorización para acceder un material "seguro" quiere descargarlo, se identifica, *sintetice* valida su acceso y en caso correcto le entrega la información requerida encriptada con su clave pública (de modo que si es impostor no le sirve) y el documento encriptado.
4. Los documentos seguros nunca son abiertos o decodificados en el entorno web, ni en el servidor. Y, es responsabilidad de sus usuarios finales, decifrarlos y manejarlos en un entorno seguro.

---

1 Ver [Criptografía asimétrica](#) en wikipedia