



**SEGURINFO  
2009**

**Quinto Congreso Argentino de Seguridad de la Información  
19 de marzo de 2009 - Hotel Sheraton Buenos Aires**

# **Usuarios sensitivos Problemática y gestión**

**Penta Security Solutions SRL**

**Ing. Silvana Colasurdo ([scolasurdo@pentass.com](mailto:scolasurdo@pentass.com))**

**Ing. Agustín Zorgno ([azorgno@pentass.com](mailto:azorgno@pentass.com))**



# Usuarios sensitivos

## Definición

---

### ¿Qué es un usuario sensitivo?

Es una cuenta de acceso a un sistema que tiene características especiales que hacen necesario un cuidado especial sobre la misma.

### Otras denominaciones:

- **Usuario de emergencia o firecall:** esta nomenclatura es conocida cuando existen situaciones de contingencia en los sistemas.
- **Cuenta de administración, cuenta de máximo privilegio, administrador o root:** esta nomenclatura es conocida cuando se habla de usuarios con amplios permisos.

Dada su criticidad, es necesario establecer procedimientos para efectuar un adecuado control, monitoreo y trazabilidad de su gestión.

# Usuarios sensitivos

## Ejemplos

---

Algunos ejemplos

- **en sistemas operativos**

- **root**: la cuenta de máximos privilegios en Unix / Linux.
- **Administrador**: la cuenta de máximos privilegios en Windows.
- **oracle**: la cuenta sobre la que se monta la base de datos en el sistema operativo.

- **en bases de datos**

- **sa**: la cuenta de administración del motor de base de datos Sql Server.
- **system**: la cuenta de administración del motor de base de datos Oracle.

- **en aplicaciones**

- **aplic** : la cuenta de instalación de aplicaciones.
- **emerg01** : la cuenta utiliza para dar soporte en entornos productivos.

- **etc.**

# Usuarios sensitivos Problemática

---

- Las cuentas privilegiadas y el control de cuentas administrativas compartidas son un área de continuo interés y preocupación para todas las empresas.
- El crecimiento de los requisitos a cumplir ha enfocado la atención en como la empresa gestiona y controla estas cuentas criticas.
- Las regulaciones pueden variar basándose en las industrias y mercados particulares:
  - SOX
  - ISO-IEC 27002
  - PCI
  - HIPAA
  - BCRA “A” 4609



# Usuarios sensitivos Problemática

---

El acceso a la información sensible es restringida por contraseñas de cuentas con altos privilegios, y se almacena en:

- Servidores
- Bases de datos
- Aplicaciones
- Correo electrónico

Al aumentar la infraestructura de TI, el número de cuentas con altos privilegios se incrementa considerablemente complejizando su administración.

# Usuarios sensitivos Problemática

---

## ¿Quiénes utilizan estas cuentas?

- Administradores de servidores
- Administradores de correo electrónico
- Mesa de ayuda de las aplicaciones
- Administradores de seguridad
- Etc

## ¿Quiénes controlan estas cuentas?

- Administradores de seguridad
- Auditores

## ¿Dónde se conservan las credenciales?

- Hojas de cálculos
- Archivos en texto plano
- Papeles impresos



# Usuarios sensitivos Problemática

---

Si el ID es compartido por múltiples usuarios, cambiar la contraseña es esencial para poder identificar unívocamente a la persona que accedió a los sistemas utilizando esa clave.

Este tipo de contraseña debe estar disponible rápidamente en caso de problemas con el sistema.

El cambio de la contraseña es un proceso administrativo tedioso y en muchos casos no es sencillo o posible cambiar la contraseña por lo tanto la misma es conocida por muchas personas en la organización.

# Usuarios sensitivos Problemática

---

Adicionalmente al cambio de la contraseña, otra tarea fundamental es efectuar un control estricto para:

- Permitir que sólo las personas autorizadas puedan acceder a las contraseñas de los usuarios sensitivos.
- Brindar acceso en todo momento (7x24) a las contraseñas de los usuarios firecalls.
- Identificar la persona que solicitó el acceso a esa contraseña del usuario firecall.
- Determinar exactamente el período de tiempo durante el cual una persona tuvo acceso a la contraseña del usuario firecall.
- Asignar contraseñas robustas a los usuarios sensitivos.
- Generar reportes de actividades de este tipo de usuarios.

# Usuarios sensitivos

## Solución histórica

---

Considerando que esta problemática existe ya hace muchos años, se han implementado soluciones históricas.

La más común es almacenar físicamente las contraseñas. En muchos casos, la contraseña es escrita en un papel, guardada dentro de un sobre cerrado y almacenado en una caja fuerte.

Este almacenamiento es luego controlado por la sala de Operaciones, cuya tarea es disponibilizar el sobre correcto cuando es necesario el acceso al sistema.

El Administrador de Seguridad es responsable de cambiar las contraseñas de las cuentas utilizadas.

# Usuarios sensitivos

## Solución histórica - Ejemplo



Surge una emergencia



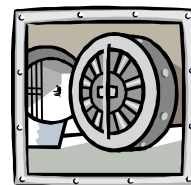
Solicita usuario sensitivo



Verifica si esa autorizado



Obtiene llaves de caja fuerte



Obtiene sobre cerrado



Obtiene usuarios y contraseña



Soluciona la emergencia



Cambia contraseña, almacena y genera reporte auditoria



Línea de tiempo

T0

T1

T2

T3

T4

T5

T6

T7

# Usuarios sensitivos

## Solución histórica

---

La deficiencia más evidente en el proceso de ensobrado manual es el volumen. Esto puede funcionar para 20 cuentas, pero no lo hace para 100 ó 5.000.

El proceso es a su vez, muy manual, necesitando un procedimiento que asegure el mantenimiento de un inventario exacto y certero. Las deficiencias pueden incluir:

- Escala: los procesos manuales rápidamente se vuelven inmanejables.
- Cambio:
  - Cuánto tiempo existe entre que una contraseña es utilizada y es cambiada?
  - Las contraseñas que están hardcodeadas son cambiables?
  - Con qué frecuencia y a qué costo?.
- Conocimiento: Considerando que una persona asigna una contraseña al usuario firecall, cómo nos aseguramos que esa persona no la utilice?.

# Usuarios sensitivos

## Solución actual

---

Las soluciones actuales se basan en la utilización de algún software que resuelva los problemas planteados.

Dada la criticidad de la información que manejan, estos software deben:

- Estar concebidos en base a las mejores prácticas de seguridad de la información.
- No permitir el acceso no autorizado.
- Permitir a una persona solamente acceder a las cuentas sensitivas a las que tiene permiso.
- Poseer alta disponibilidad.
- Contar con copias de respaldo seguras.

# Usuarios sensitivos

## Solución actual

---

Las soluciones actuales deberían permitir:

- Eliminar costos derivados del antiguo sistema de sobre cerrado.
- Administrar en forma más ágil y eficiente estas contraseñas.
- Generar en forma automática reportes de acceso y administración de contraseñas.
- Registrar detalladamente las operaciones de los administradores y usuarios del sistema de contraseñas, según roles específicos.
- Identificar problemas en los sistemas.
- Disponibilizar el acceso remoto 7x24.
- Asignar contraseñas mediante funciones aleatorias con alta seguridad.
- Reducir los tiempos de acceso a las contraseñas
- Generar de registros de actividades detallados.
- Proteger las contraseñas mediante un almacenamiento encriptado.
- Reducir el riesgo de acceso no autorizado o deducción de contraseñas sencillas o predecibles.

# Usuarios sensitivos

## Información de referencia

---

Algunos links donde pueden obtener mayor información al respecto:

- [http://en.wikipedia.org/wiki/Privileged\\_password\\_management](http://en.wikipedia.org/wiki/Privileged_password_management)
- [http://searchfinancialsecurity.techtarget.com/tip/0,289483,sid185\\_gci1325290,00.html](http://searchfinancialsecurity.techtarget.com/tip/0,289483,sid185_gci1325290,00.html)
- <http://www.scmagazineus.com/Six-simple-steps-to-managing-privileged-passwords/article/34643/>
- [http://www.securitypark.co.uk/security\\_article.asp?articleid=260337&Categoryid=1](http://www.securitypark.co.uk/security_article.asp?articleid=260337&Categoryid=1)
- <http://www.bjhcim.co.uk/features/2008/802002.htm>
- [http://www.accessmylibrary.com/coms2/summary\\_0286-29792656\\_ITM](http://www.accessmylibrary.com/coms2/summary_0286-29792656_ITM)

# Usuarios sensitivos Demostración

---



# Usuarios sensitivos

## Beneficio – Pitbull KeyHolder

---

**Pitbull KeyHolder ® brinda una solución definitiva a la gestión de contraseñas de emergencia bajo el sistema de sobre cerrado, contribuyendo a una gestión de IT más profesional y confiable.**

Los principales beneficios de Pitbull – KeyHolder son:

- Reducción de costos
- Monitoreo, control y trazabilidad de gestión
- Flexibilización
- Optimización de procesos
- Seguridad mejorada





**SEGURINFO  
2009**

**Quinto Congreso Argentino de Seguridad de la Información  
19 de marzo de 2009 - Hotel Sheraton Buenos Aires**

## **Penta Security Solutions SRL**

**Ing. Silvana Colasurdo ([scolasurdo@pentass.com](mailto:scolasurdo@pentass.com))**

**Ing. Agustín Zorgno ([azorgno@pentass.com](mailto:azorgno@pentass.com))**

