



Nuestra misión es ayudar a las empresas a obtener valor de sus datos no estructurados

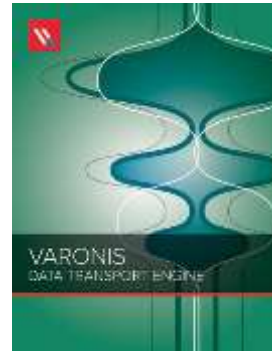
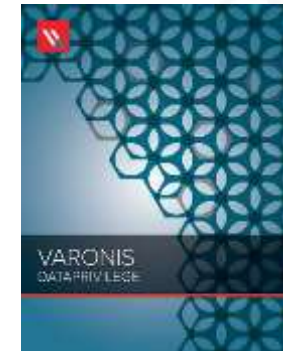
# Amenazas internas

**Andres Julian Marin**  
**Varonis Systems Engineer**

# ACERCA DE VARONIS

---

- Comenzó a operar el año 2005
- Más de **4000** Clientes
- Soluciones de software para datos generados por humanos



# AGENDA

---

- La anatomía de las brechas internas
- Brechas reales: estadísticas y ejemplos
- 6 consejos para disminuir las amenazas internas

# LOS PASOS

---



## Ingresar (si es que ya no está ahí)

- Realizado a través del phishing o de ingeniería social



## Husmear

- Enumerar el acceso actual; intentar elevar
- ¿Alguien quiere tarjetas Visa?



## Exfiltración

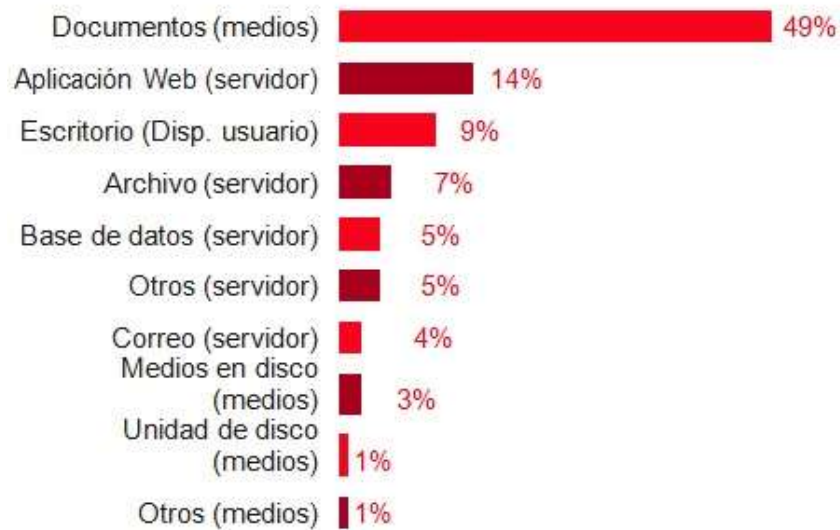
- Obtener los datos sin activar las alarmas

# LAS CIFRAS

Imagen 43. El top 10 de las amenazas provocadas por errores (n=558)

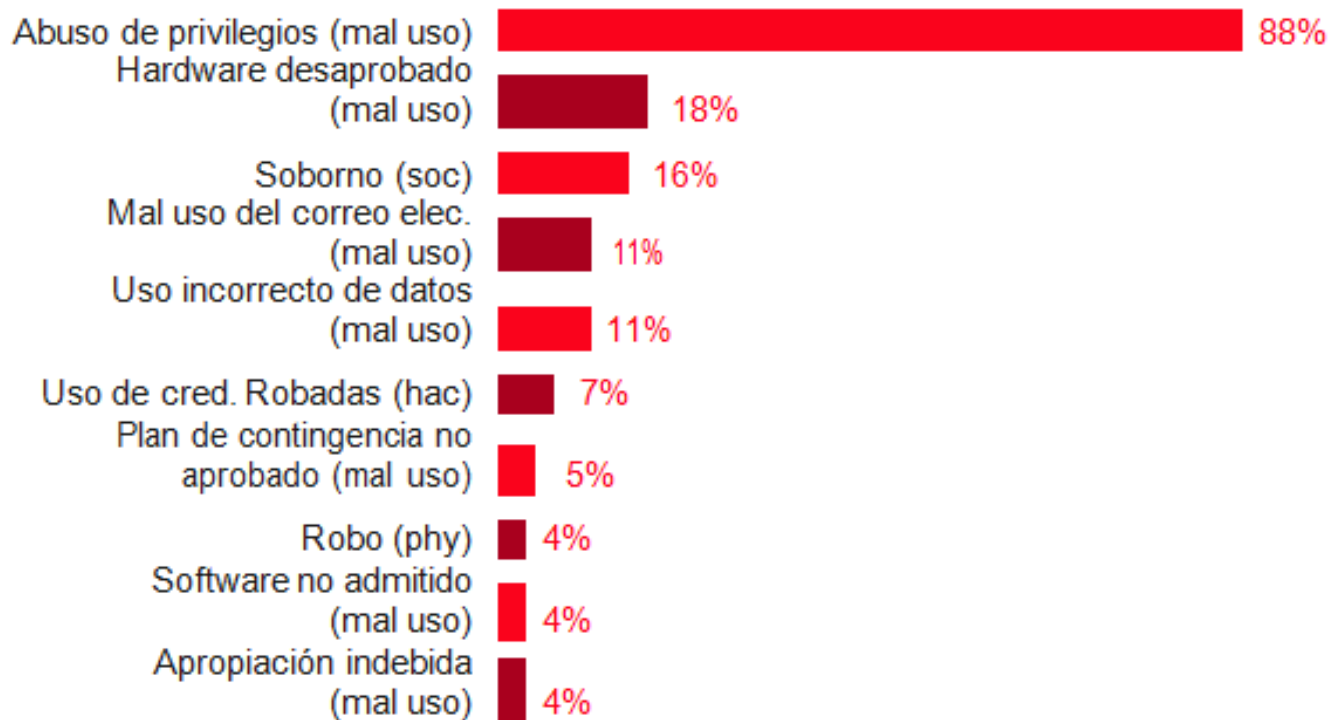


Imagen 44. El top de los activos afectados por errores (n=546)



# ABUSO DE PRIVILEGIO

Imagen 30. El top 10 de las amenazas provocadas por el mal uso interno (n=153)



□

# NUESTRO PEOR ENEMIGO



midnight memories

@GagasSwag



my new credit card! omg I'm so happy

5:12 PM - 4 Sep 2013

49 RETWEETS 22 FAVORITES



inurl:ftp filetype:config password

Web News Videos Images Shopping More Search tools

Page 2 of about 164 results (0.45 seconds)

## Web.config

[ftp://58.68.91.119/iMAAP/Demo%2007Oct12/maapcloud/Web.config](#) ▾  
SqlClientDriver Data Source=localhost\\sql2k8;Initial Catalog=maapcloud;User ID=  
=sa;Password=uc@n10gin; Connect Timeout=120; web maapcloud.dbo 250 ...

## access\_to\_oracle\_import\_matrix.exe.config

[ftp://206.191.66.248.dedicated.allstream.net/.../access\\_to\\_oracle\\_import...](#) ▾  
Data Source=matrix\_prod;User ID=cnt;Password=C4VFDuWx;Unicode=True DATA  
SOURCE=206.191.66.248/matrix;PERSIST SECURITY INFO=True;USER ...

## README.config

[ftp.vim.org/security/coast/firewalls/freestone/.../README.config](#) ▾ Vim ▾  
Note, we strongly suggest that you have in.telnetd call a one-time password login  
program like keylogin from S/Key. We also strongly suggest that you use an ...

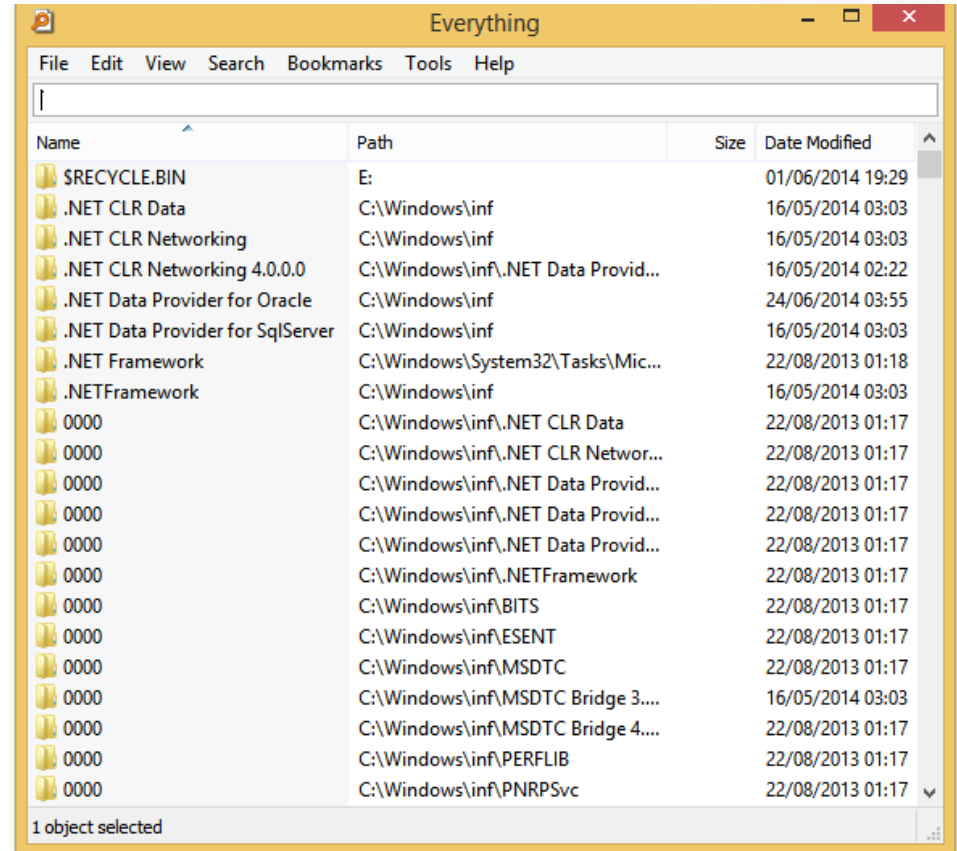
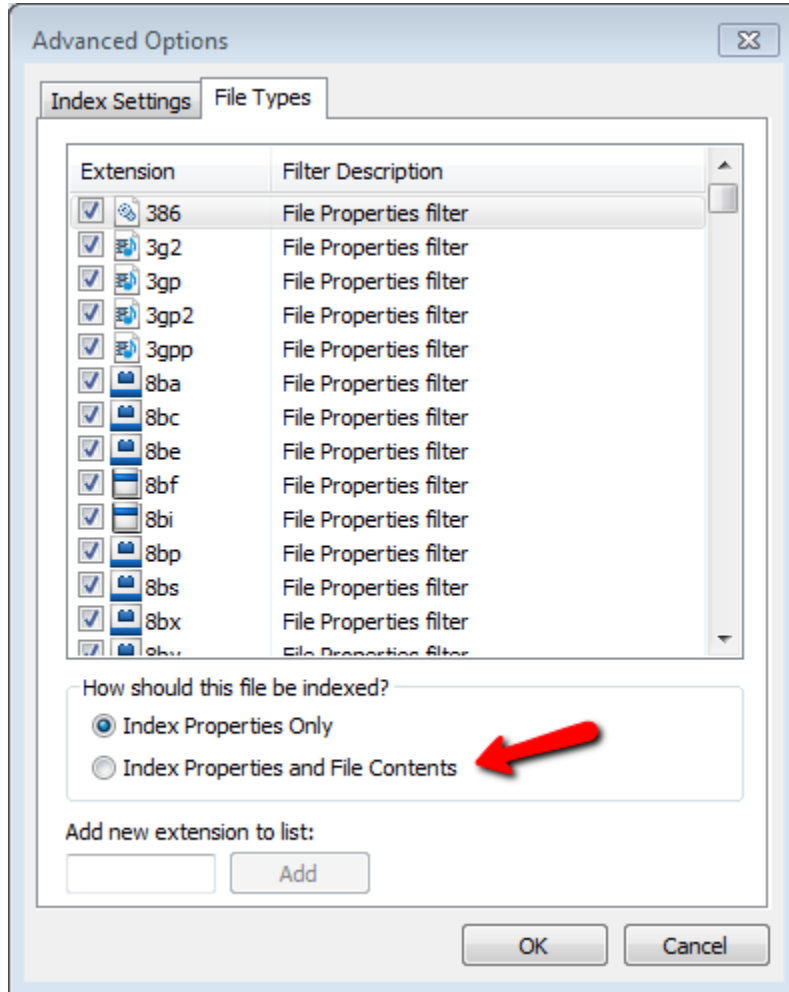
## [DOC] Automatically generated make config: don't edit # Busybo...

[ftp.belnet.be/ftp.slackware.com/...12.1/.../busybox.dot.config](#) ▾ BELNET ▾  
Apr 7, 2007 - Login/Password Management Utilities. #  
CONFIG\_FEATURE\_SHADOWPASSWDS=y. # CONFIG\_USE\_BB\_SHADOW is not  
set.

## TOne.RepricingService\_OLD.exe.config

[ftp://93.89.95.8/Service/Service/TOne.RepricingService\\_OLD.exe.config](#) ▾  
SqlClientDriver Server=192.168.110.185;Database=MVTSPProDemo;User ID=  
Development;Password=dev123 NHibernate.Dialect.MsSql2008Dialect TABS.

# HUSMEAR DETRÁS DEL FIREWALL





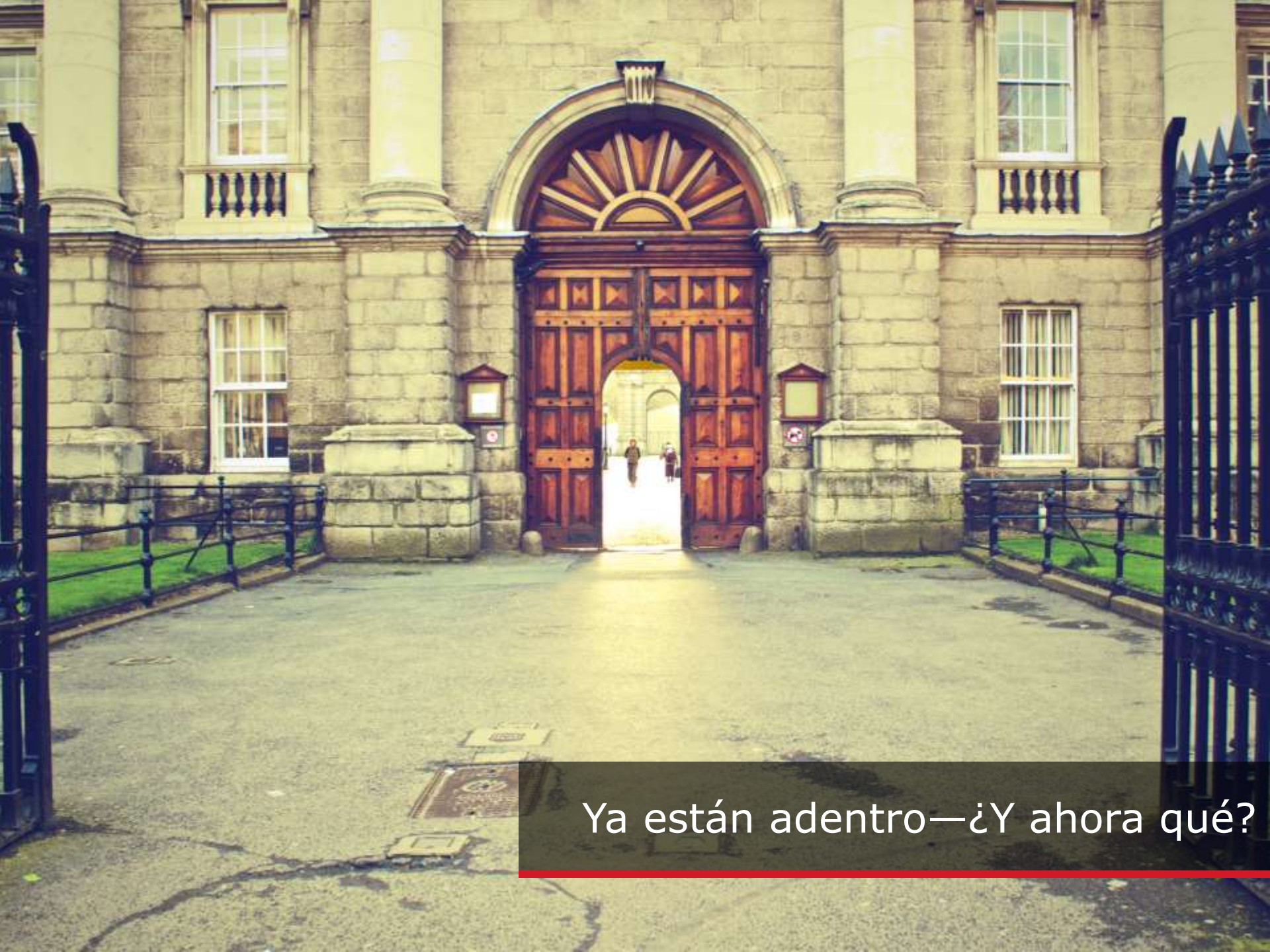
# TARGET COMO BLANCO

---

- 40,000,000 archivos perdidos
- Muchas herramientas sofisticadas vigilando el perímetro (síndrome del caramelo)
- “[...] la vocera, Molly Snyder, dice que los intrusos ganaron acceso al sistema utilizando credenciales robadas de un vendedor”



@Avivahl de Gartner dice que de haberse asesorado con analistas del comportamiento, se pudo haber prevenido una #Brechadedatos en Target



Ya están adentro—¿Y ahora qué?

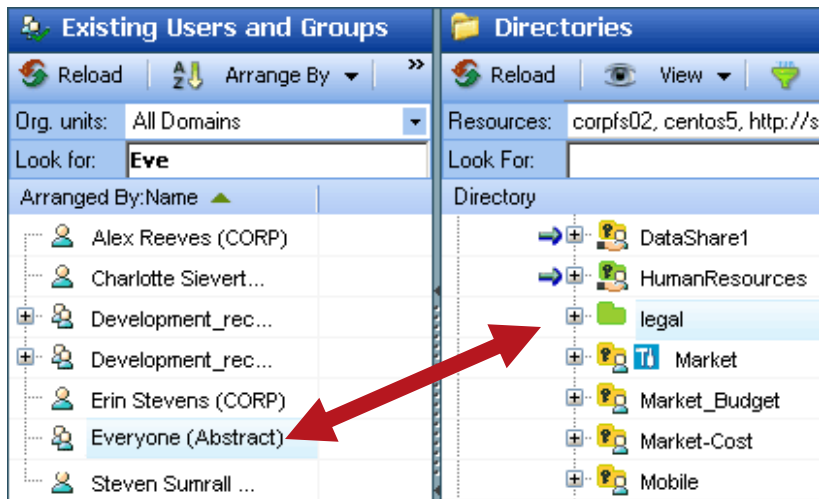
# 6 CONSEJOS DE MITIGACIÓN

---

1. Elimine el acceso global
2. Elimine los permisos excesivos
3. Alerta las escaladas de privilegios
4. Alerta las desviaciones de comportamiento
5. Instale ~~paneles de miel~~ trampas
6. Monitoree de cerca a las personas y los datos de alto riesgo

# CONSEJO #1: ELIMINE EL ACCESO GLOBAL







- Localice a grupos como "Todos" y "Usuario autenticado" y reemplácelos por grupos de seguridad más cerrada
- ¿Cómo evito cortar el acceso legítimo?



¡Alice Tanner perderá el acceso a los datos que ha estado utilizando!

# CONSEJO #2: ELIMINE LOS PERMISOS EXCESIVOS

- iGente y software!
- Descubra a qué información *prohibida* tiene acceso la gente
  - Recomendaciones como las de Amazon
- Acceso temporal de auto-expiración
- Revise los ~~derechos~~ permisos periódicamente

<input checked="" type="checkbox"/> Review only actionable objects			
<input type="checkbox"/> Review only entities that were not added by an automatic rule ?			
Status	Users	Permission	Decision And Explanation
	 <a href="#">Allison Schafer (CORP)</a>	Exe-Write	<input checked="" type="radio"/> Keep <input type="radio"/> Remove
	 <a href="#">Andrew Carlisle (CORP)</a>	Exe-Write	<input checked="" type="radio"/> Keep <input type="radio"/> Remove
	 <a href="#">Andrew Weirich (CORP)</a>	NA	<input type="radio"/> Keep <input checked="" type="radio"/> Remove
	 <a href="#">Andy Welch (CORP)</a>	Execute	<input checked="" type="radio"/> Keep <input type="radio"/> Remove
	 <a href="#">Anne Lampkin (CORP)</a>	Execute	<input checked="" type="radio"/> Keep <input type="radio"/> Remove

# CONSEJO #3: ALERTE LAS ESCALADAS DE PRIVILEGIOS

## ¿Sabe cuándo alguien tiene acceso a la raíz?

General

Who (Acting Object)

**Where (Affected Object)**

What (Event Details)

When (Event Time)

Alert Method

**Where (Affected Object)**

You can use filters or a Predefined Scope to define alerts for specific affected objects. Note that when using filters, the file server filter is mandatory and residing on the selected file server.

Select predefined scope: (None) Save as predefined scope

New Group New Filter Remove Selected

All of (AND):

<input type="checkbox"/> File server	Equals	DirectoryServices	...
<b>and</b>			
<input type="checkbox"/> Directory name (DirectoryServices)	Is equal to	corp.local\Users\Domain Admins	...

Search in child objects

General

Who (Acting Object)

Where (Affected Object)

**What (Event Details)**

When (Event Time)

Alert Method

**What (Event Details)**

Add filters to alert on specific event types and event status. If no filters are selected, an alert will be created for all events.

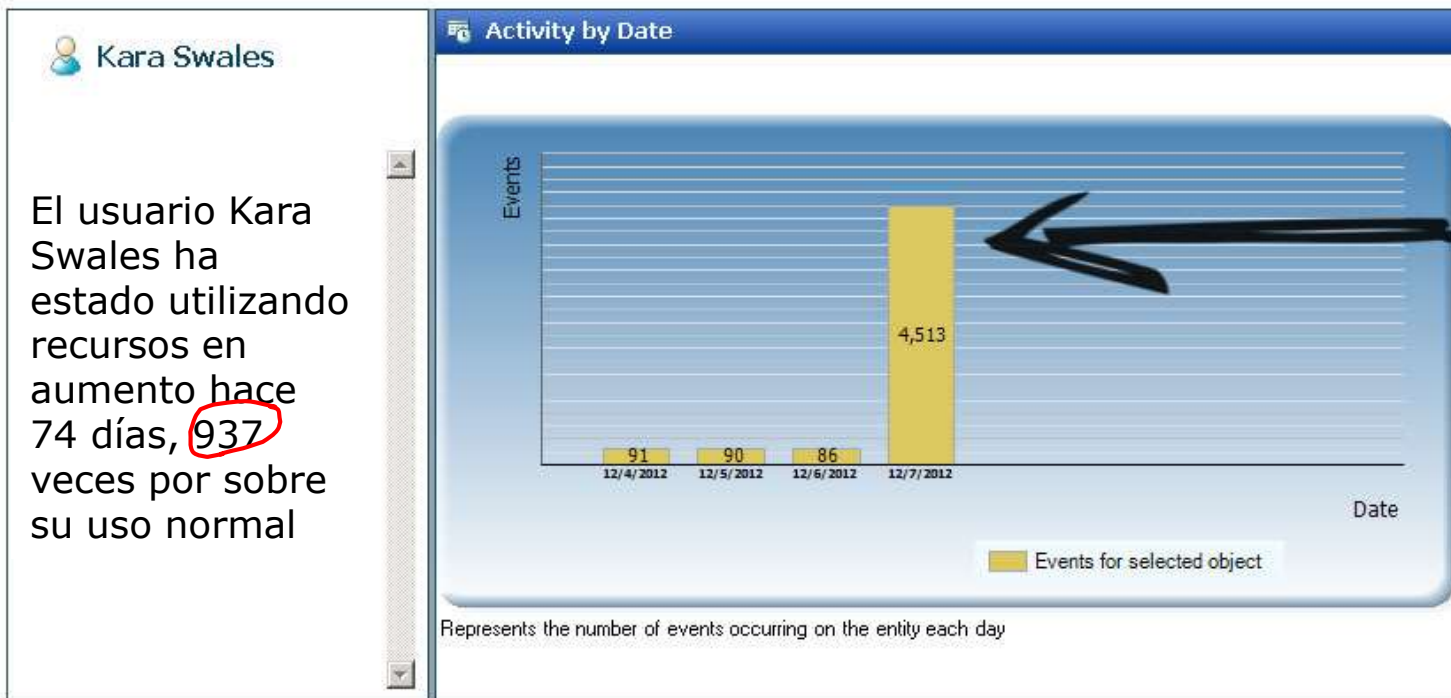
New Group New Filter Remove Selected Reset Import/Export Filter

All of (AND):

<input type="checkbox"/> Event type	Contained in	DS object membership added, DS object membership removed	...
-------------------------------------	--------------	--	-----

# CONSEJO #4: ALERTE LAS DESVIACIONES DE COMPORTAMIENTO

- Aumento de actividad de comportamiento (Correo elect., archivos, acceso denegado)
- Monitoree la actividad fuera del horario de trabajo



El usuario Kara Swales ha estado utilizando recursos en aumento hace 74 días, **937** veces por sobre su uso normal

Alerte la actividad anómala

# CONSEJO #5: INSTALE TRAMPAS ~~PANALES DE~~ MIEL

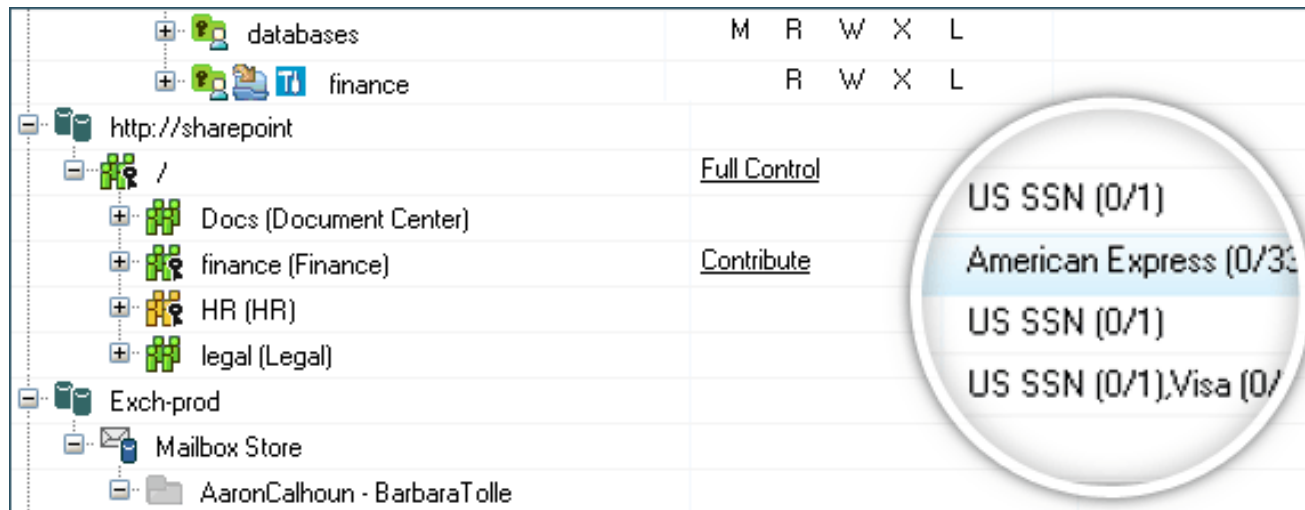
---

- Configure una carpeta compartida que esté abierta para todos los usuarios
  - X:\Share\Payroll
  - X:\Share\Confidential
  - X:\Share\CEO
- Vea quién comete abuso de dicha carpeta



# CONSEJO #6: MONITOREE A LAS PERSONAS Y DATOS DE ALTO RIESGO

- Alerte o envíe a cuarentena a los datos sensibles cuando aparezca en un lugar público
- Supervise a los administradores de raíz/dominio
- Supervise a los contratistas



+	databases	M	R	W	X	L
+	finance	R	W	X	L	
+	http://sharepoint					
+	/					<u>Full Control</u>
+	Docs (Document Center)					
+	finance (Finance)					<u>Contribute</u>
+	HR (HR)					
+	legal (Legal)					
+	Exch-prod					
+	Mailbox Store					
+	AaronCalhoun - BarbaraTolle					

US SSN (0/1)  
American Express (0/3)  
US SSN (0/1)  
US SSN (0/1), Visa (0/1)



¡Gracias!

Andres Julian Marin

Varonis Systems Engineer - Latin America  
and the Caribbean

[amarin@varonis.com](mailto:amarin@varonis.com)

Arturo Medina

Varonis Sales Rep ( Mexico y Puerto Rico)

[amedinaramos@varonis.com](mailto:amedinaramos@varonis.com)

Evaluacion de amenazas gratuita

<http://hub.varonis.com/evaluation-es>