



# Gestión de vulnerabilidades

Preparado por:

Astrid Pereira Sierra

[Astrid@Creangel.com](mailto:Astrid@Creangel.com)





## Agenda

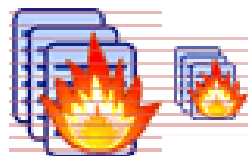
- Introducción
  - Definiciones
  - Identificación de problemática
- Gestión de vulnerabilidades
- Bibliografía y referencias

Astrid@creangel.com

## Definiciones

- Vulnerabilidad: error de software que usa un intruso para ganar acceso a un sistema de información de forma manual o mediante el uso de exploits.
- Exploit: programa informático malicioso que aprovecha una vulnerabilidad para realizar acciones no autorizadas por el usuario.
- Intruso: individuo que intenta aprovechar una vulnerabilidad para beneficio propio o daño ajeno.

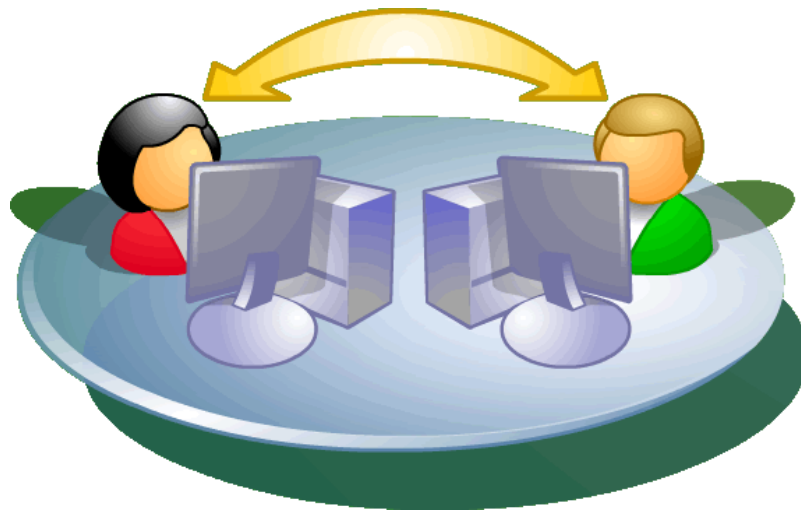




## Problemática alrededor de las Vulnerabilidades

- Existen grupos de personas y organizaciones que encuentran vulnerabilidades en S.O y Aplicaciones.
- La publicación de las vulnerabilidades expone los sistemas afectados y las organizaciones.
- Exploits e intrusos que aprovechan las existencia de las Vulnerabilidades.
- Vulnerabilidades de día 0
- Se estima que por cada 1000 líneas de código existen entre 5 y 20 fallas\*

\* <http://www.ocio.usda.gov>

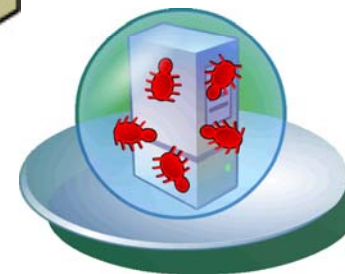


## Publicaciones sobre Vulnerabilidades

- CVE
- NIST
- SANS
- CERT
- Fabricantes Ej: “Patch Tuesday”

## A qué se expone por no gestionar vulnerabilidades

- Ingresos no autorizados a la infraestructura de red y los sistemas de información
- Acceso y divulgación de información privilegiada
- Violación de privacidad, legislación o regulaciones
- Incumplimiento de estándares
- Detención o entorpecimiento de la operación



# VIII Jornada Nacional de Seguridad Informática



## A qué se deben las vulnerabilidades?

- Fallas de software
- Fallas de configuración
- Configuraciones por defecto
- Errores humanos

Astrid@creangel.com

## Algunos tipos de vulnerabilidades

- Desbordamiento de Buffer
- Cross Site Scripting.
- Inyección SQL
- Denegación de Servicio (DoS) (DDoS).

0	0	0	0	0	0	0	0	0	3
Buffer A								Buffer B	
'd'	'e'	'm'	'a'	's'	'i'	'a'	'd'	'o'	0
Buffer A								Buffer B	

```
<A HREF="http://www.instisec.com/comentarios.asp?texto='<SCRIPT>Código Malicioso</SCRIPT>'">Información sobre agujeros</A>
```

```
CONSULTA := "SELECT * FROM usuarios WHERE nombre = " + nombreUsuario + "';"
```

```
SELECT * FROM usuarios WHERE nombre = 'Usuario1';
```

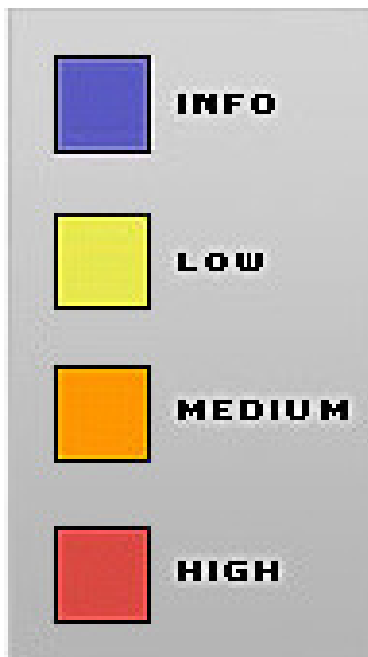
```
Usuario1'; DROP TABLE usuarios; SELECT * FROM datos WHERE nombre LIKE '%
```

```
SELECT * FROM usuarios WHERE nombre = 'Alicia';
```

```
DROP TABLE usuarios;
```

```
SELECT * FROM datos WHERE nombre LIKE '%';
```

Astrid@creangel.com



## Categorías de Vulnerabilidades

- **Altas:** Un atacante puede ganar acceso privilegiado (Root, Administrador) remotamente.
- **Medias:** Un atacante puede ganar acceso No-privilegiado (User) remotamente.
- **Bajas:** Permiten revelación de información para elaborar ataques de mas riesgo.
- **Informativas:** Revelan información menos valiosa que las Bajas, en muchos casos son inherentes al funcionamiento de la red.

Astrid@creangel.com

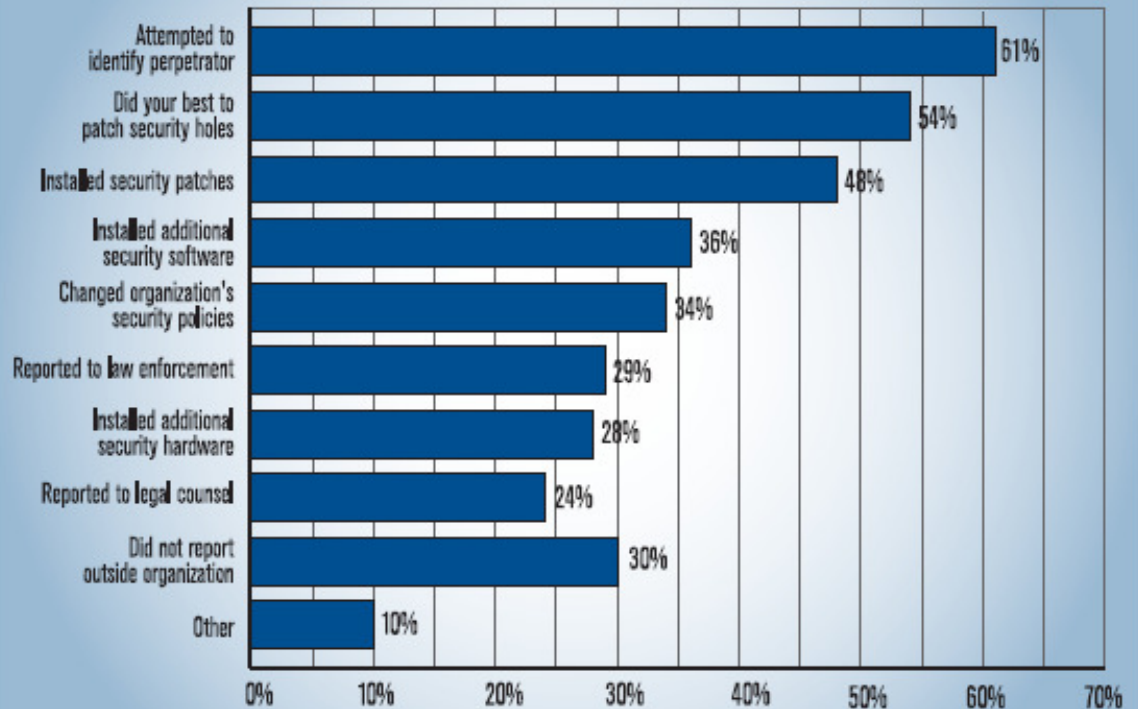


# VIII Jornada Nacional de Seguridad Informática



¿Qué acciones se suelen tomar ante un incidente?

**Figure 24. Actions Taken Following an Incident**  
By Percent of Respondents



CSI 2007 Computer Crime and Security Survey  
Source: Computer Security Institute

2007: 274 Respondents



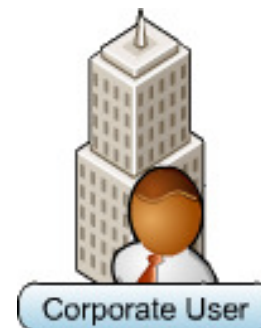
## Agenda

- ✓ Introducción
  - ✓ Definiciones
  - ✓ Identificación de problemática
- **Gestión de vulnerabilidades**
- Bibliografía y referencias

Astrid@creangel.com

## GV – Gestión de vulnerabilidades

- Es diferente de detección de vulnerabilidades
- Es diferente de Ethical Hacking
- Es una de las medidas básicas de seguridad
- Implica la detección, remoción y control del riesgo generado por las vulnerabilidades mediante el uso de herramientas y workflows que ayudan a minimizar los riesgos de explotación



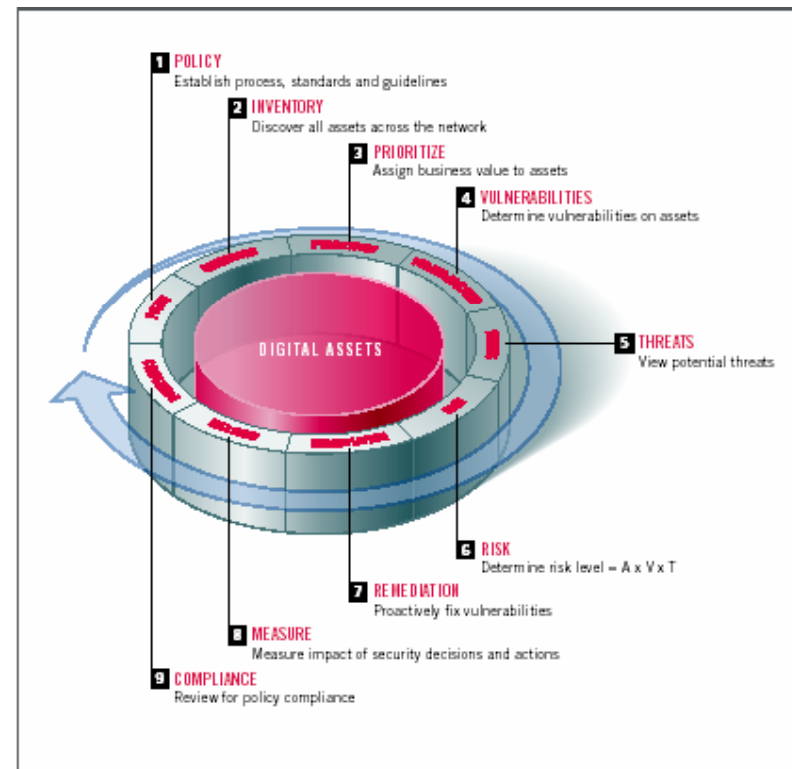
## Objetivos base de GV

- Alinearse con la gestión de riesgo de la organización
- Ir más allá de un Ethical hacking o una prueba de vulnerabilidades
- Identificar y corregir fallas de software o configuraciones
- Verificar que los correctivos no afecten funcionalidad y/o rendimiento de los sistemas
- Identificar amenazas
- Identificar falencias que no pueden ser corregidas y ofrecer alternativas para la minimización del riesgo
- Identificar e implementar las mejores alternativas para remediar las vulnerabilidades
- Permitir documentar y seguir las labores de remediación
- Permitir verificar el estado de seguridad para labores de auditoría y cumplimiento



## Elementos básicos

- Políticas
- Inventario
- Priorización
- Búsqueda de vulnerabilidades
- Identificación de amenazas
- Métricas de riesgo
- Remediación
- Revisión de impacto
- Cumplimiento de políticas



# VIII Jornada Nacional de Seguridad Informática



## GV y políticas de seguridad

- Deben estar alineados porque GV busca de manera sistemática encontrar y remediar vulnerabilidades.
- Esto implica el uso de tecnología pero asociada a la organización y sus procesos
- Las políticas determinan la naturaleza de los controles
- Las políticas y controles se aplican sobre cada uno de los activos
- Las políticas ayudan a la priorización

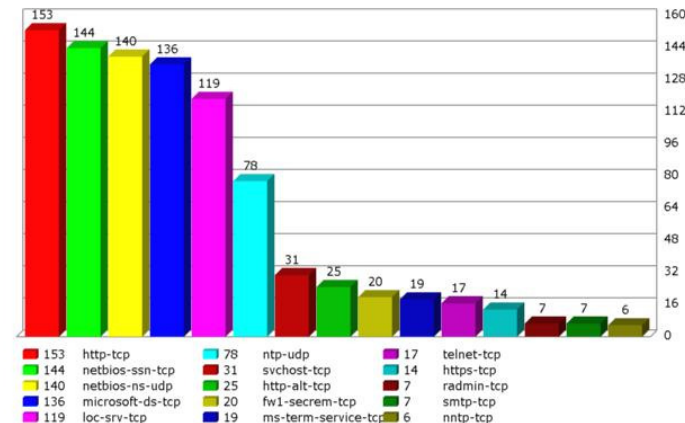
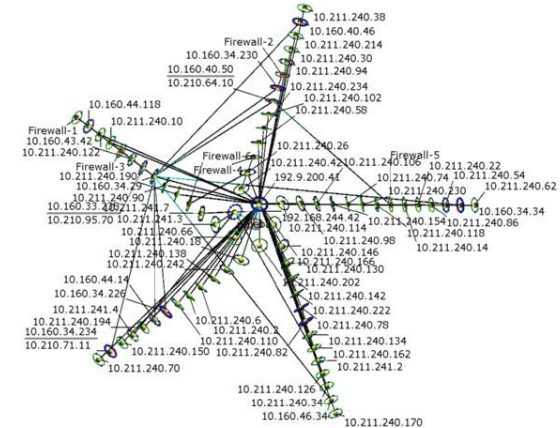
Astrid@creangel.com

# VIII Jornada Nacional de Seguridad Informática



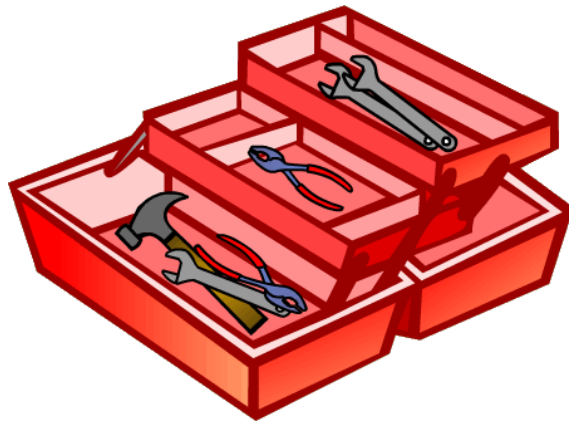
## Inventario

- Activos
  - Que activos serán incluidos en la gestión
  - Ancho de banda disponible
  - Segmentos de red dónde están ubicados los activos
  - Cómo llegar a revisar los activos incluidos
  - Cuándo es conveniente efectuar revisiones
- Servicios
  - Identificar y proveer el mínimo suficiente



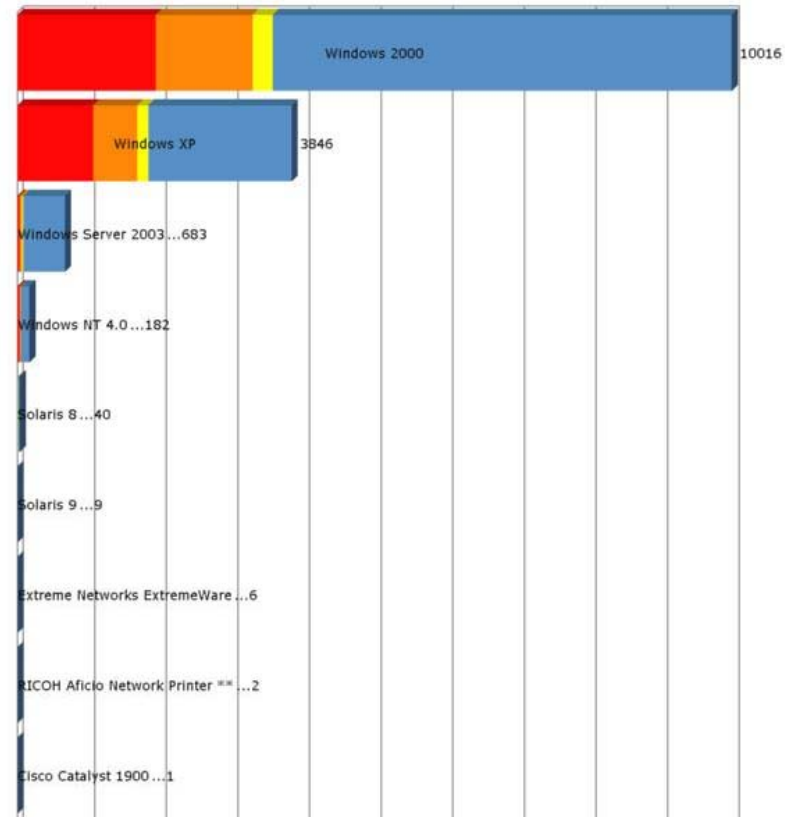
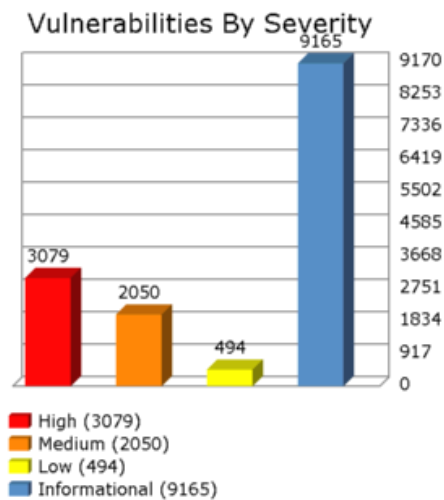
## Priorización

- Clasificación de activos
- Clasificación de información
- Por unidades de negocio
- Por procesos productivos
- Por uso



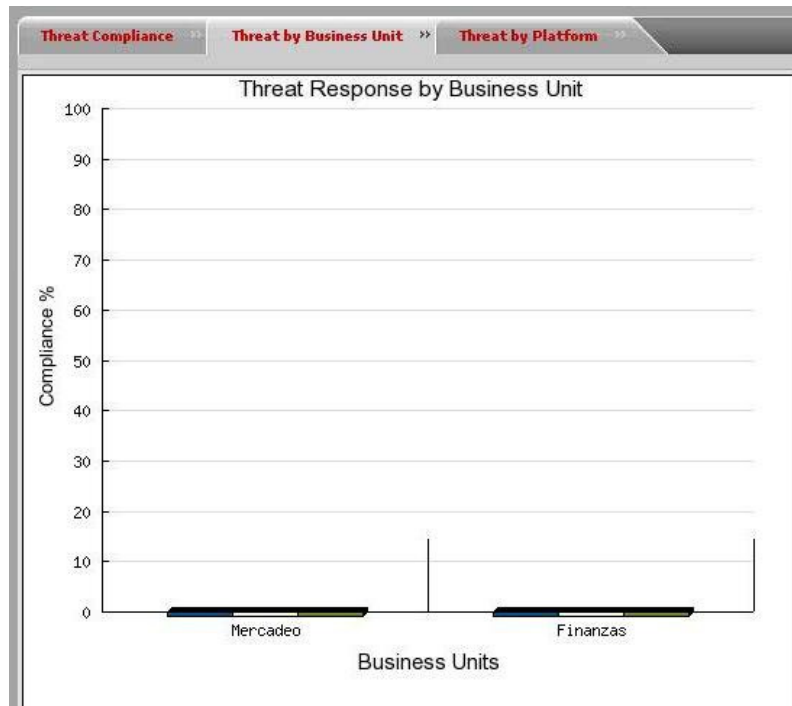
## Búsqueda de vulnerabilidades

- Por severidad
- Por sistemas operativos



## Identificación de amenazas

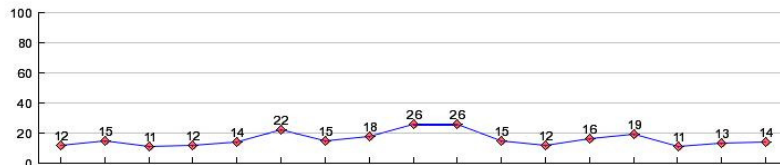
- Cuáles son las amenazas más relevantes para la organización en función de:
  - Aplicativos y su criticidad
  - Los servicios ofrecidos por los activos
  - Uso
  - Unidades de negocio
  - Criticidad de los activos



# VIII Jornada Nacional de Seguridad Informática



## Métricas de riesgo



- Las medidas tomadas han disminuido la exposición al riesgo?
- Relación costo/beneficio
- Esfuerzo horas/hombre
- $R = \text{Activo} \times \text{Vulnerabilidad} \times \text{Amenaza}$

Astrid@creangel.com

## Remediación

- NO se reduce a aplicar parches
- Pruebas
  - Algunas de las medidas pueden impactar el ambiente productivo
  - Falsos positivos
  - Quién, cómo, cuándo, por dónde empezar
  - Comprobar que efectivamente se remedió
  - La mejor solución viable
  - Ofrecer alternativas a lo “irremediable”

HIGH

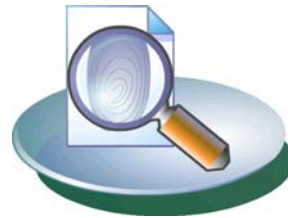
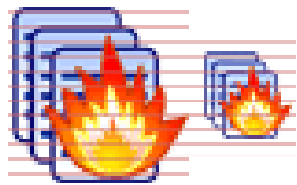
<a href="#">(MS03-031) Microsoft SQL Server 2000 Named Pipe Hijacking</a>	1	<a href="#">10.210.112.20</a>
---	---	-------------------------------

MEDIUM

<a href="#">Password file accessible via anonymous FTP</a>	1	<a href="#">10.210.90.8</a>
--	---	-----------------------------



- **Revisión de impacto**



- Por área de negocio
- Por gestión efectuada
- La curva de aprendizaje puede ser larga y dolorosa, evalúe si puede abreviarla utilizando servicios expertos

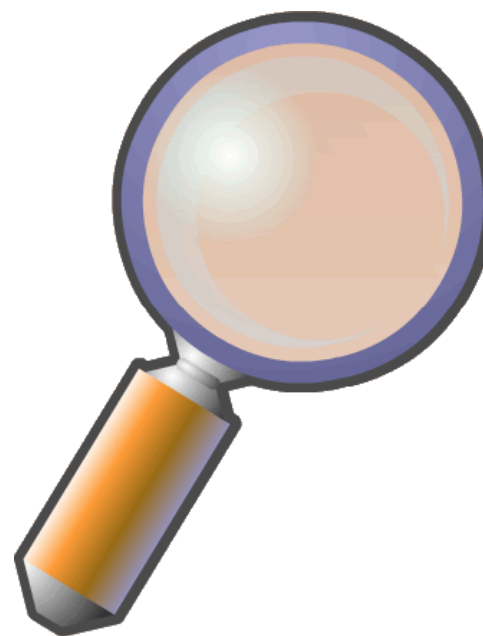
## Cumplimiento de políticas

- ISO 27001
- SOX
- HIPAA
- Sarbanes-Oxley
- FISMA
- PCI
- COBIT
- ITIL



## Buenas prácticas en GV

- Descubra sus activos
- Clasifíquelos
- Revise todos los segmentos de red
- Efectúe revisiones constantes y detalladas
- Revise los reportes técnicos y gerenciales
- Priorice, ejecute de manera continua las medidas de remediación





## Se recomienda implementar la gestión de vulnerabilidades porque:

1. Permite reducir el riesgo de exposición de la organización debido al uso de tecnología
2. Ayuda a reducir los ataques exitosos contra la organización.
3. Identifica y colabora en remediar fallas de software que afecten la seguridad.
4. Busca complementar las herramientas de seguridad implementadas Antivirus, Firewall, IPS/IDS o VPN.
5. Permite mejorar el cumplimiento con Normas/Políticas.
6. Refuerza la postura de seguridad de la información
7. En 1000 activos de una infraestructura bien gestionada es fácil encontrar 500000 vulnerabilidades
8. El centro de coordinación del CERT (CC)3 (<http://www.cert.org>) estima que el 95% de todas las intrusiones de red podrían ser evitadas manteniendo al día los sistemas en parches e implantando las mejores prácticas de seguridad provistas por los fabricantes

Astrid@creangel.com

## Agenda

- ✓ Introducción
  - ✓ Definiciones
  - ✓ Identificación de problemática
- ✓ Generalidades sobre gestión de vulnerabilidades
- Bibliografía y referencias



## Bibliografía y referencias

- <http://www.cert.org>
- NIST: Creating a Patch and Vulnerability Management Program, <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>
- <http://www.ocio.usda.gov>: USDA Vulnerability Scan Procedures
- Curing the Patch Management Headache: Felicia M Nicastro
- Integrated Risk and Vulnerability Management Assisted by Decision Support Systems: Relevance and Impact on Governance (Topics in Safety, Risk, Reliability and Quality) : Adrian V. Gheorghe



- Gracias por su Atención

Astrid Pereira Sierra

[Astrid@creangel.com](mailto:Astrid@creangel.com)

