Tecnológico de Monterrey

Mecanismos detección y recuperación

Roberto Gómez Cárdenas

rogomez@itesm.mx

http://cryptomex.org

@cryptomex

Tecnológico de Monterrey

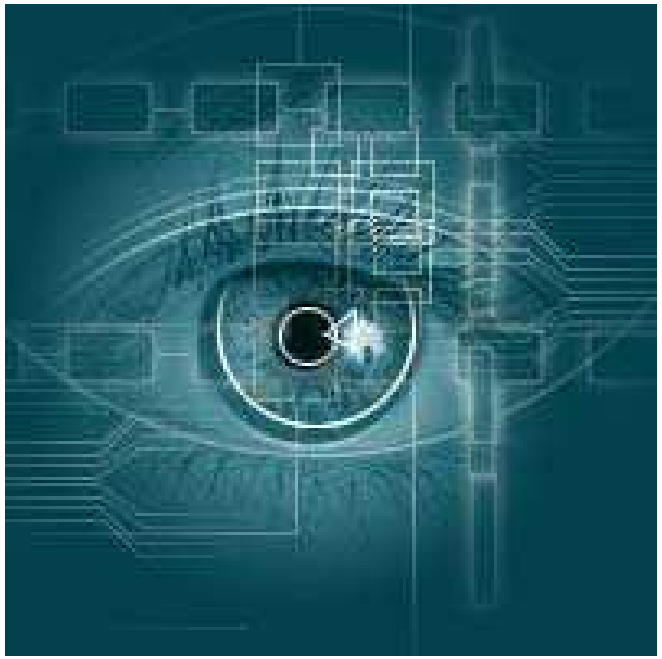
Detección

- Busca descubrir incidentes al momento en que ocurren o lo antes posible.
- Debe permitir detectar eventos para reducir el daño.
- Permite identificar y perseguir culpables.
- Revela vulnerabilidades.

Tecnológico de Monterrey

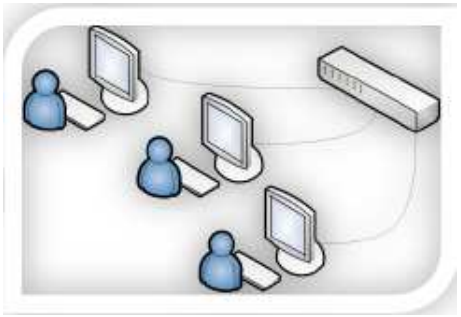
Mecanismos detección

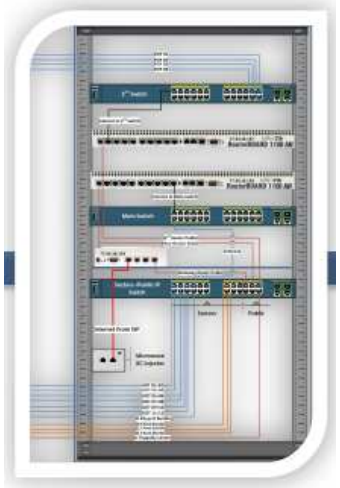
- Son aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación.
- Ejemplos de estos mecanismos
  - IDS
    - Tripwire
    - Snort
  - Detectores de vulnerabilidades
    - Nessus
    - ISS
    - Rapid7

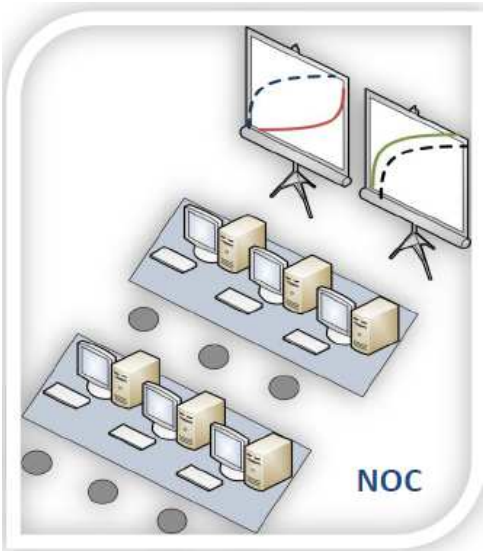


NOC: Network Operation Centers

- Administra los sistemas NMS (network management systems) monitorea fallas y eventos, da seguimiento al desempeño de la red y atiende problemas que se presentan de primera mano.
- Como su nombre implica, el principal propósito de un NOC es administrar la red.





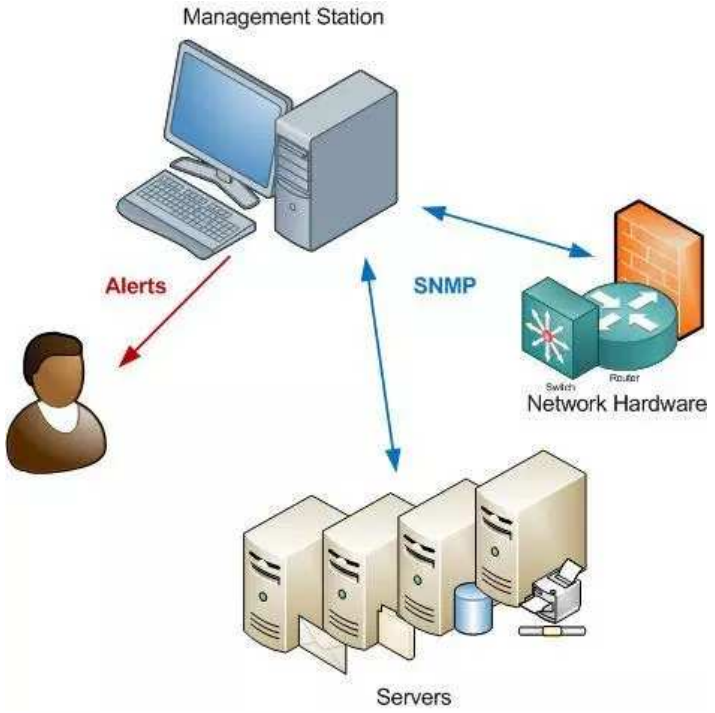


Tecnológico de Monterrey

NOC de Namibia y la India

SNMP

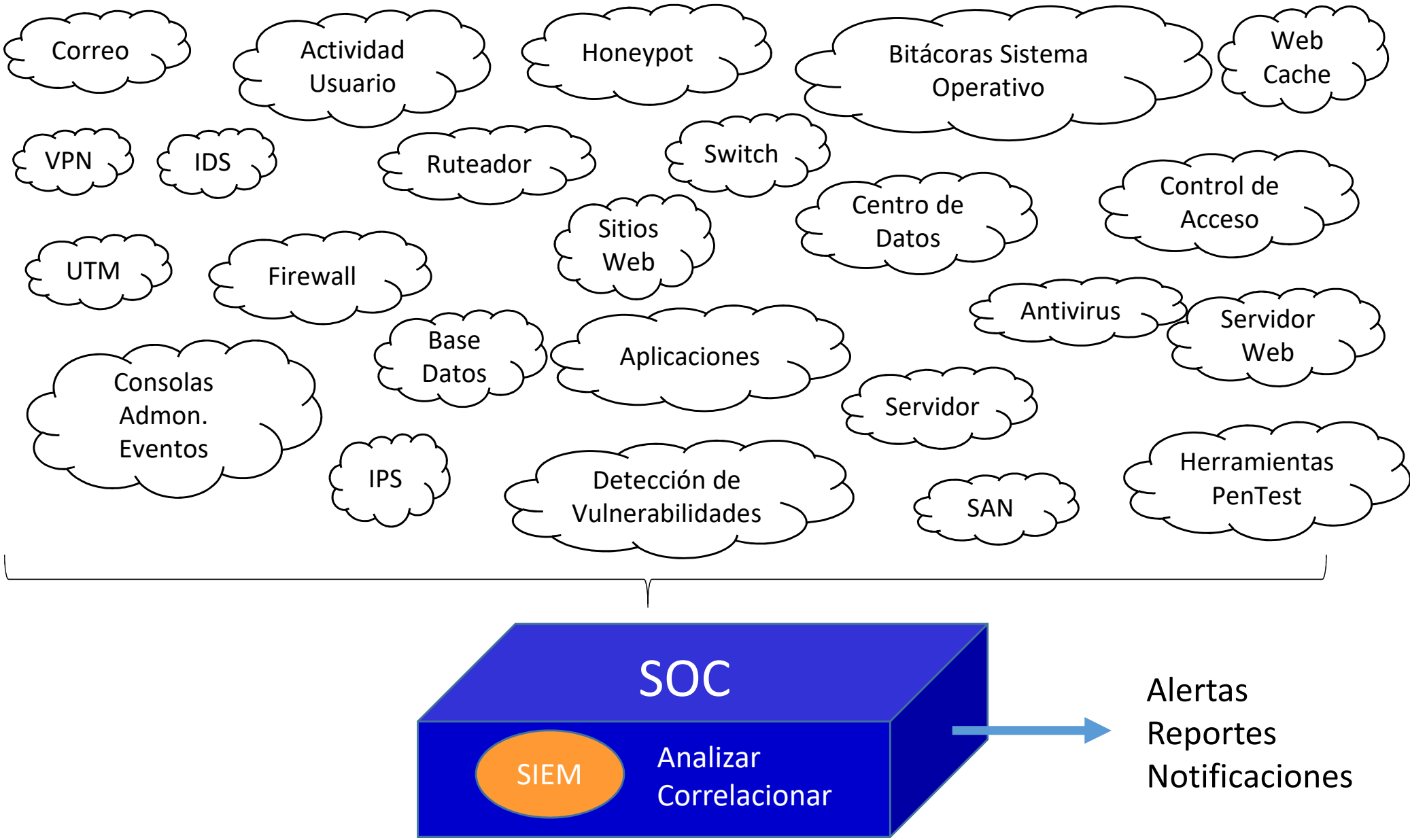
- Simple Network Management Protocol
- Protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.
- Los dispositivos que normalmente soportan SNMP incluyen routers, switches, servidores, estaciones de trabajo, impresoras, bastidores de módem y muchos más.
- Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.



SOC: Security Operation Center

- Un centro de operaciones de seguridad (SOC) es una unidad centralizada en una organización que se ocupa de cuestiones de seguridad, en una organización y nivel técnico.
- Un SOC dentro de un edificio o instalación es una central ubicación desde donde el personal supervisa el sitio, usando datos tecnología de procesamiento.
- Típicamente, está equipado para el acceso.
- Monitoreo y control de iluminación, alarmas y barreras de vehículos.
- Puesto de mando, centro de monitoreo, Cx
  - Comando, Control, Comunicaciones y Cómputo

Entradas salidas SOC

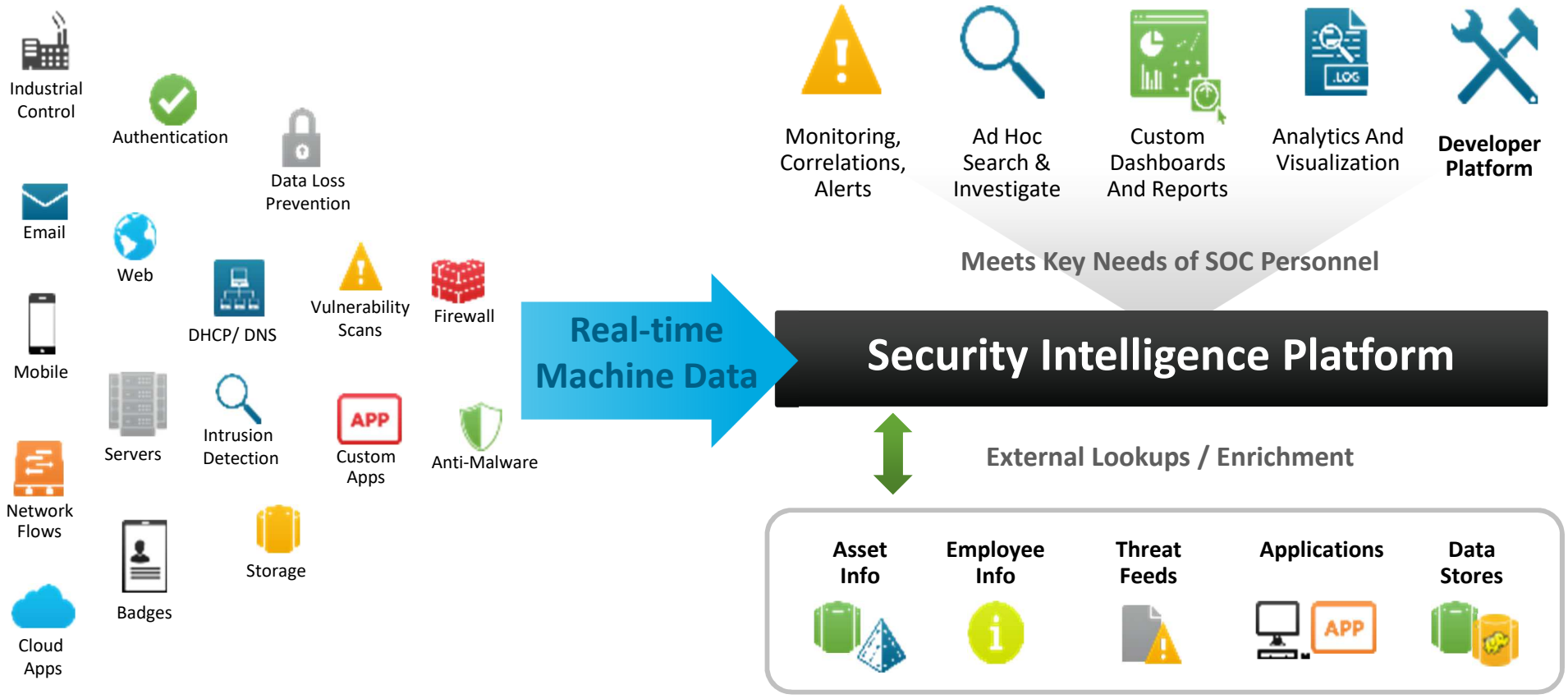


Tecnológico de Monterrey

Herramientas SIM/SIEM/SEM

- SIEM Security Information Event Management (SIEM)
  - Termino para software y servicios de productos que combina características de un SIM y un SEM
  - Recolectar, analiza y presenta información de
    - Red y dispositivos de seguridad;
    - Aplicaciones de identidad y acceso,
    - Herramientas de administración de vulnerabilidades y de cumplimiento de políticas.
    - Bitácoras de sistemas operativos, bases de datos y aplicaciones.
    - Datos de amenazas externa
- En algunas ocasiones los acrónimos SIEM, SIM y SEM se usan indistintamente.
  - SEM: Security Information Management, tiene que ver con monitoreo a tiempo real, correlación de eventos, notificaciones y vistas de consola.
  - SIM: Security Event Management, proporciona almacenamiento a largo tiempo, análisis y reporteo de datos de bitácoras

Necesidad de la plataforma de inteligencia de seguridad (SIEM + más)



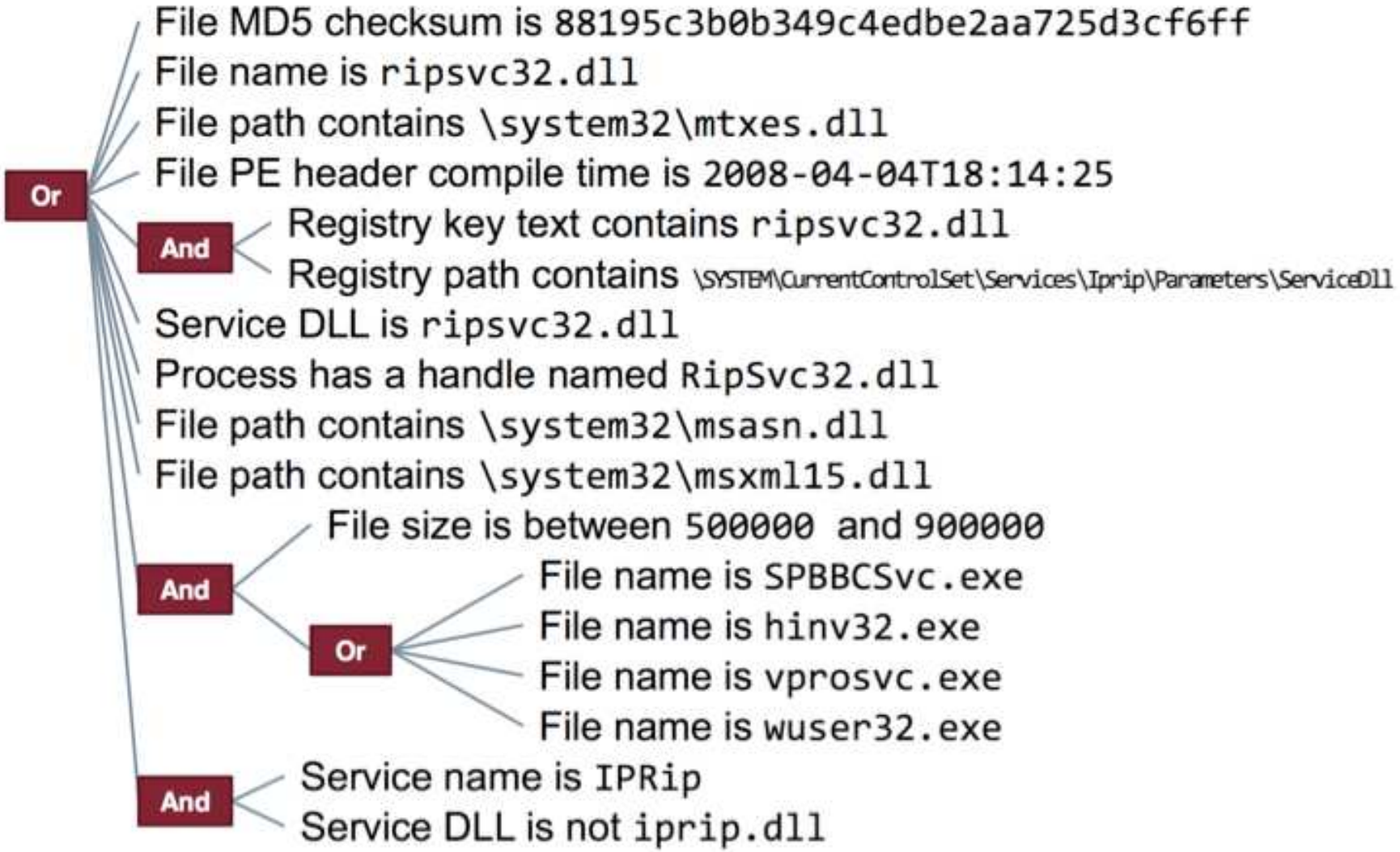
Tecnológico de Monterrey

Algunos términos relacionados

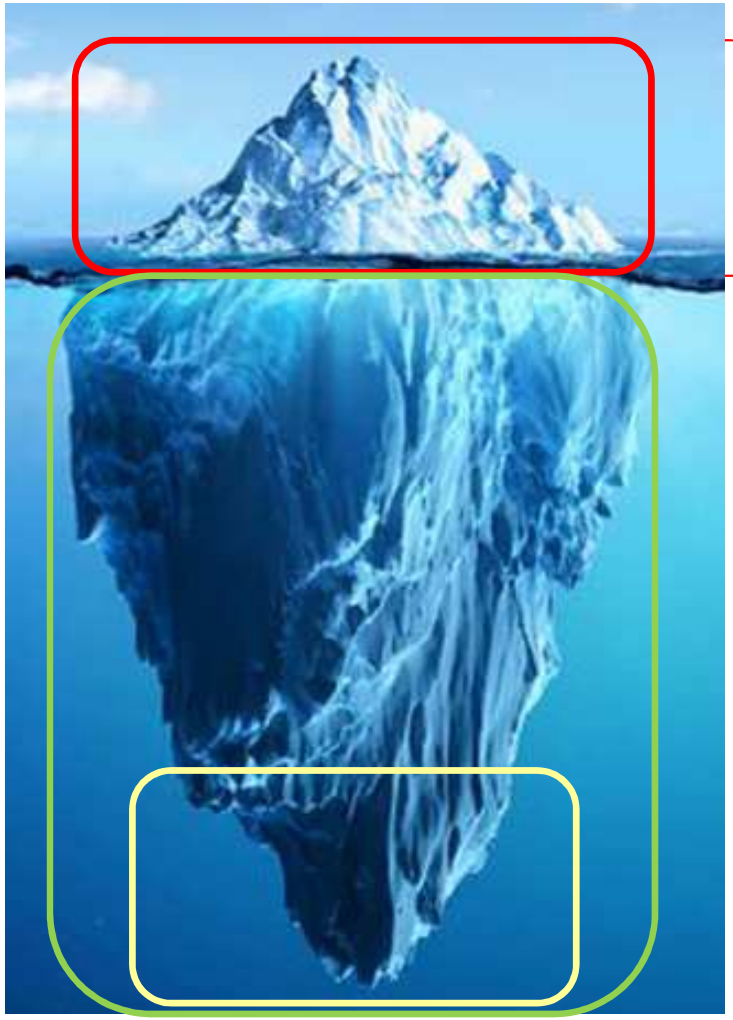
- APT
- Ciber Intelligence
- Threat Intelligence
- Threat Hunting
- Artifacts
- IoC
- Big Data
- Data Analysis
- I.A.
- Deep Web
- Dark Web

Tecnológico de Monterrey

Ejemplo IoC



Web, DeepWeb y DarkWeb



- 4% del contenido de la Web.
- De fácil acceso.
- Bajo supervisión gobierno.

- 96% del contenido de la Web (500x el tamaño del Surface Web).
- Puede incluir contenido inofensivo como resultados de búsqueda de sitios de viajes y catálogos de bibliotecas.
- También incluye el “Dark Web”.

- Clandestino.
- Intencionalmente oculto a la vista.
- Proporciona anonimato (tanto para editores como para usuarios).
- Difícil de navegar/monitorear.

Leyendas urbanas: Niveles Web

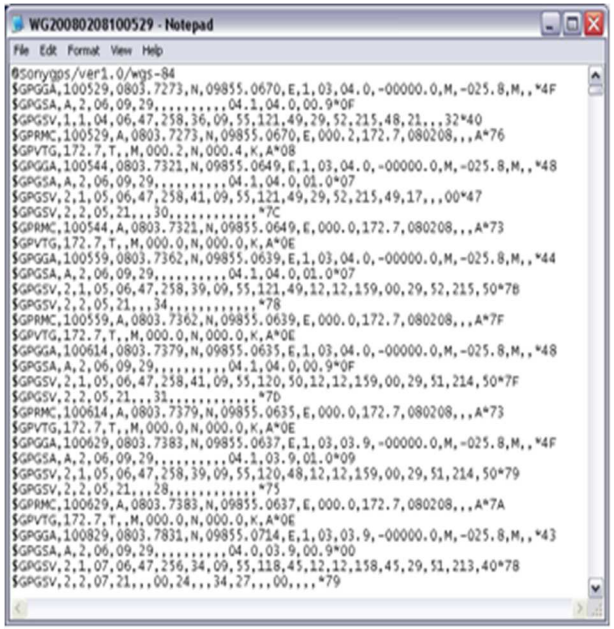
Nivel	Nombre	Descripción
1	Surface/Common Web	
2	Bergie Web	Este nivel es el último normalmente accesible: todos los niveles que siguen a este deben ser accedidos con un proxy, Tor o mediante la modificación de su hardware. En este nivel puede encontrar algunos sitios web "subterráneos" pero aún indexados, como 4chan.
3	Deep Web	Requiere de un proxy para acceder (CP, gore, hacking websites)
4	Charter Web P1	Accesible vía TOR Charter Web (drug trafficking, human trafficking, banned movies, books and black markets.)
	Charter Web p2	Se puede acceder a través de una modificación del hardware: "Closed Shell System". Contiene sitios web como Hardoce CP, websites such as Hardcore CP, experimental hardware information and some darker information such as world war 2 experiments and even location of Atlantis.
5	Marianas Web	Aquí las cosas se ponen más oscuras y serias, no se puede acceder a esta área ni siquiera utilizando el navegador TOR o VPN, Proxy. Hay muy pocas personas que pueden acceder a la documentación gubernamental secreta. El día que llegas aquí, oficialmente ya no eres un maricón
6	INTERMEDiARIO ENTRE MARIANA Y FOG/VIRUS SOUP	
7	Fog/Virus Soup,	La zona de guerra. Estan intentando acceder al nivel 8, conocido como The Fog o Virus Soup, ya que todo esto está lleno de tantos códigos para intentar arruinar a otras personas que están en la capa 7 y que intentan llegar a la capa 8.
8	The Primarch System	Todo aquí es una locura. El Sistema Primarca (DIOS DEL SISTEMA) es lo que controla Internet.

Mecanismos de recuperación

- Son aquellos que se aplican cuando una violación del sistema se ha detectado, para retornar a éste su funcionamiento correcto.
- Ejemplos
  - Respaldos
  - Redundancia
  - Bitácoras
  - BCP
  - DRP
- Subgrupo
  - Mecanismos de análisis forense

Accountabilty: bitácoras

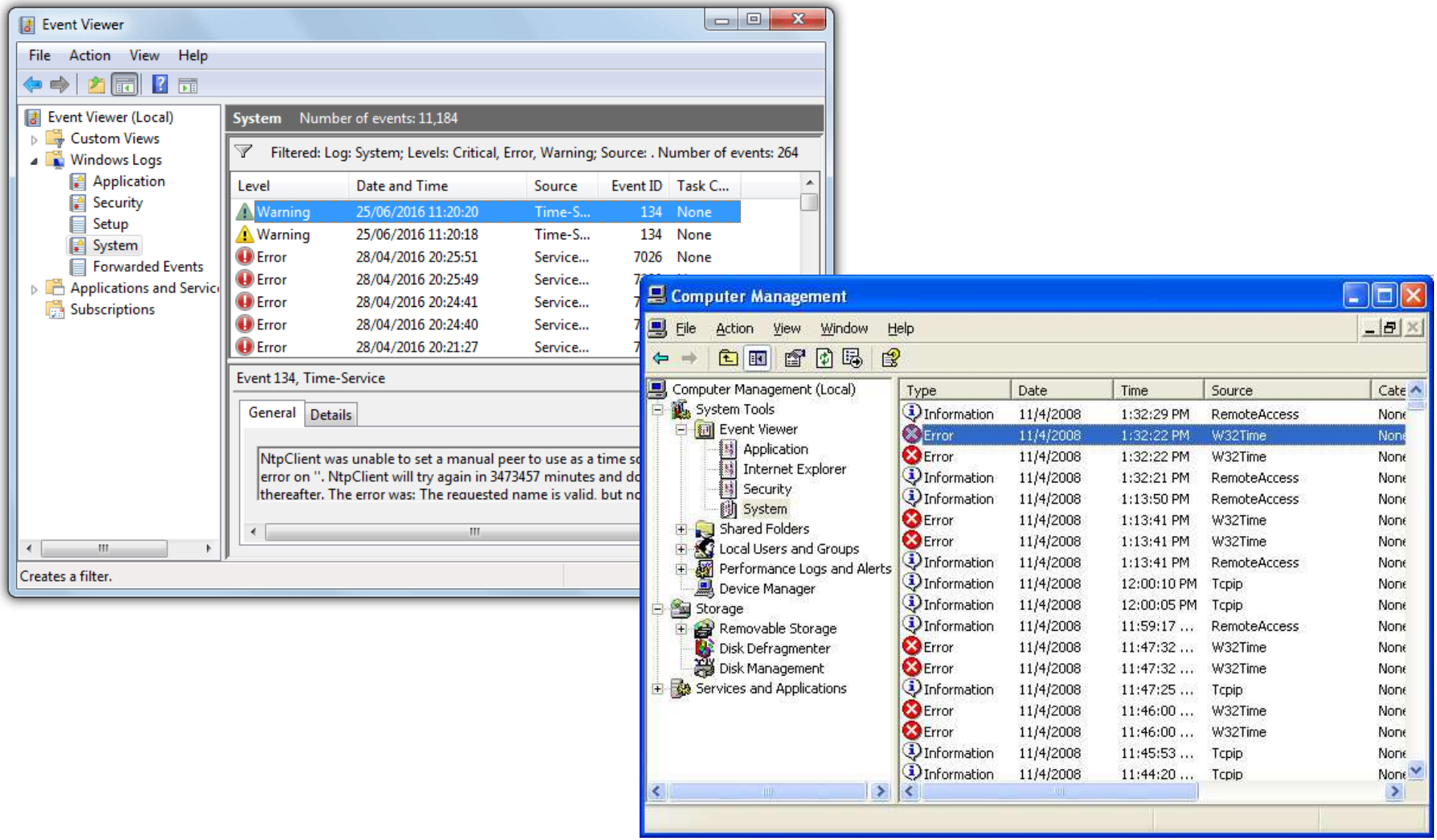
- Se refiere al procedimiento a través del cual un sistema operativo registra eventos conforme van ocurriendo y los preserva para un uso posterior.
- Bitácora:
  - Registro de datos sobre quien, que, cuando, donde y por que (W5: who, what, when, where y why, W5) un evento relacionado con un dispositivo o aplicación en particular tiene lugar.
- La mayoría de las bitácoras son almacenadas o desplegadas en el formato estándar ASCII




```
[2011.09.27 10.12.15 ]  product_version: DMO
[2011.09.27 10.12.15 ] [AutoOsDetection()] - Entered
[2011.09.27 10.12.15 ]  [Param] ProductInfo:DMO
[2011.09.27 10.12.15 ]  [Param] OSInfo:Red Hat Enterprise Linux Server release 5.5 {32-bit}
[2011.09.27 10.12.15 ]  [Param] CPU Arch:Kernel=i686
[2011.09.27 10.12.15 ]  Finding product code in product.cfg
[2011.09.27 10.12.15 ]  product code found :
[2011.09.27 10.12.15 ]  Found DMO code in product.cfg
[2011.09.27 10.12.15 ]  Finding OS Arch and CPU Type
[2011.09.27 10.12.15 ]  Found OS Arch = 32-bit, CPU Type=
[2011.09.27 10.12.15 ]  Calling config_parser.sh...
[2011.09.27 10.12.15 ] [config_parser.sh] - Entered
[2011.09.27 10.12.15 ]  [Param] OSInfo:Red Hat Enterprise Linux Server release 5.5 {32-bit}
[2011.09.27 10.12.15 ]  [Param] ProductCode:DMO
[2011.09.27 10.12.15 ]  [Param] OSArch:Arch=32-bit
[2011.09.27 10.12.16 ]  [Param] CPUArch:CPU=
[2011.09.27 10.12.16 ]  [Param] Version:version=
[2011.09.27 10.12.16 ]  [Param] XXX:Kernel=i686
[2011.09.27 10.12.16 ]  Forming parse array...
[2011.09.27 10.12.16 ] [Form_Parse_String] - Entered
[2011.09.27 10.12.16 ]  [Param] OSInfo:Red Hat Enterprise Linux Server release 5.5 {32-bit}
[2011.09.27 10.12.16 ]  [Param] ProductCode:DMO
[2011.09.27 10.12.16 ]  [Param] OSArch:Arch=32-bit
[2011.09.27 10.12.16 ]  [Param] CPU:CPU=
[2011.09.27 10.12.16 ]  [Param] CPUArch:Kernel=i686
```

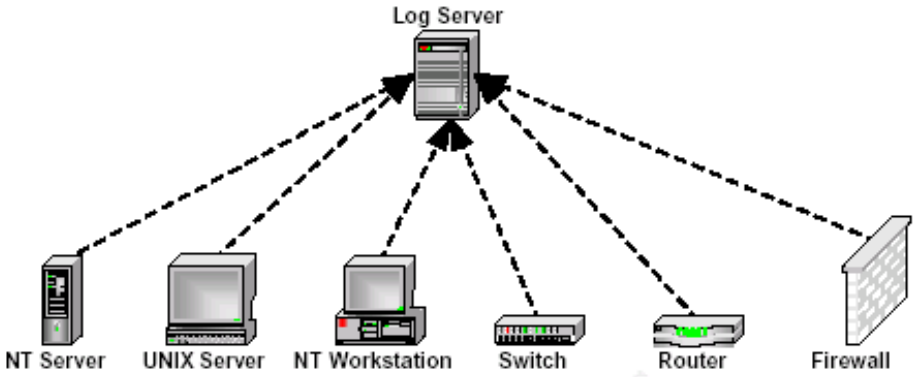
Tecnológico de Monterrey

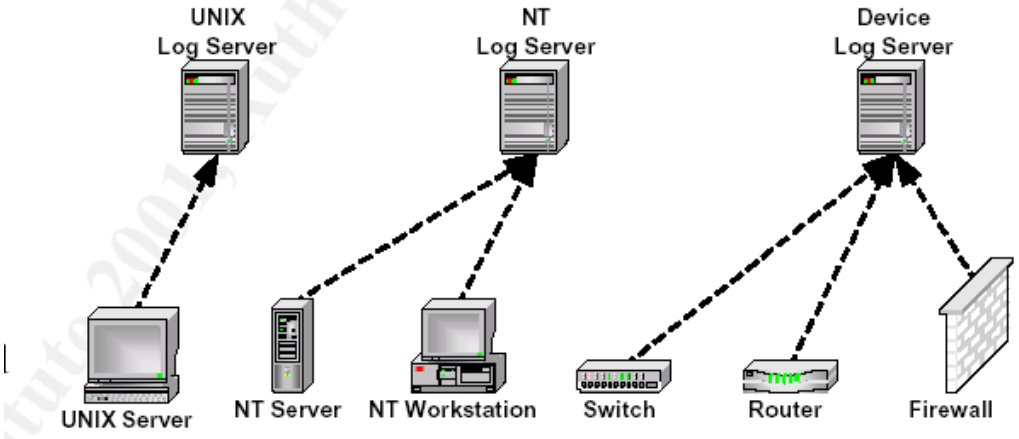
Event Viewer



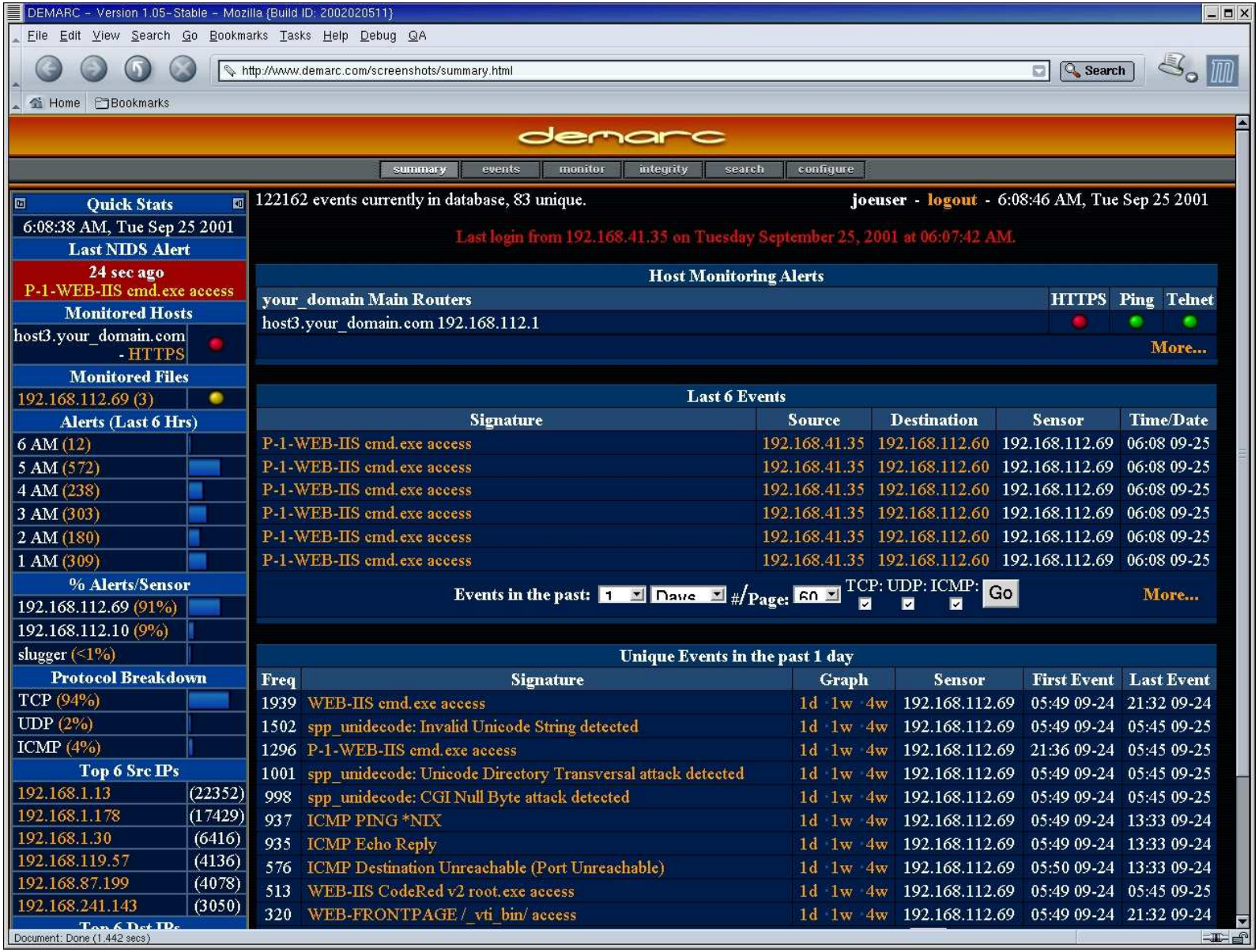
Consolidación de bitácoras

- Todos los dispositivos envían sus archivos de bitácoras a un único común servidor de bitácoras.
- todos los dispositivos similares envían sus archivos de bitácoras a un único servidor designado.

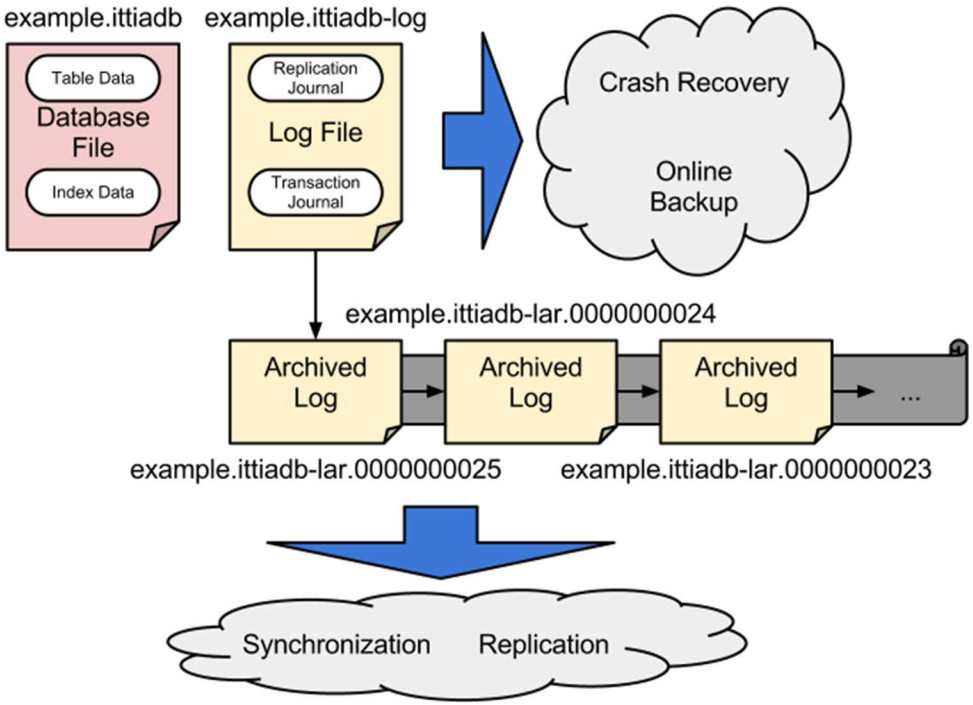


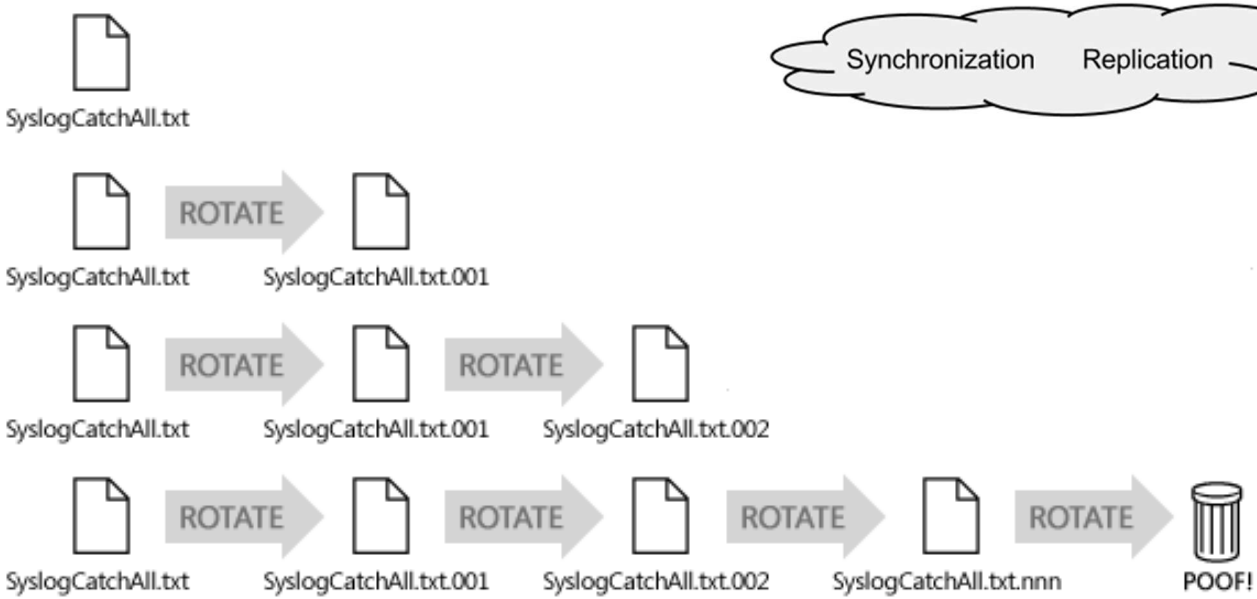


Ejemplo consolidación

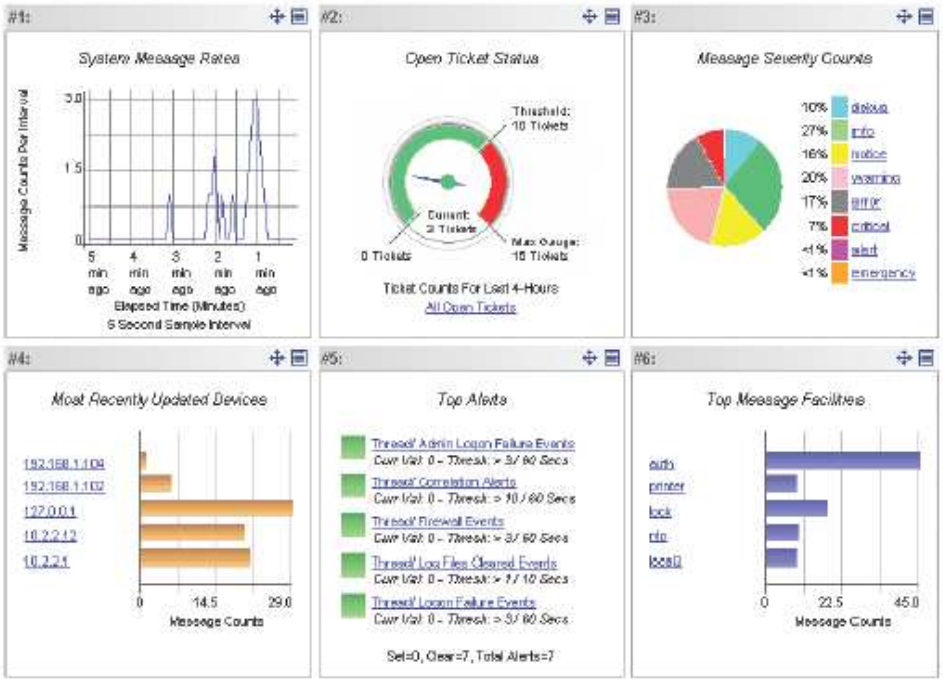


Rotación de bitácoras





Correlación de bitácoras



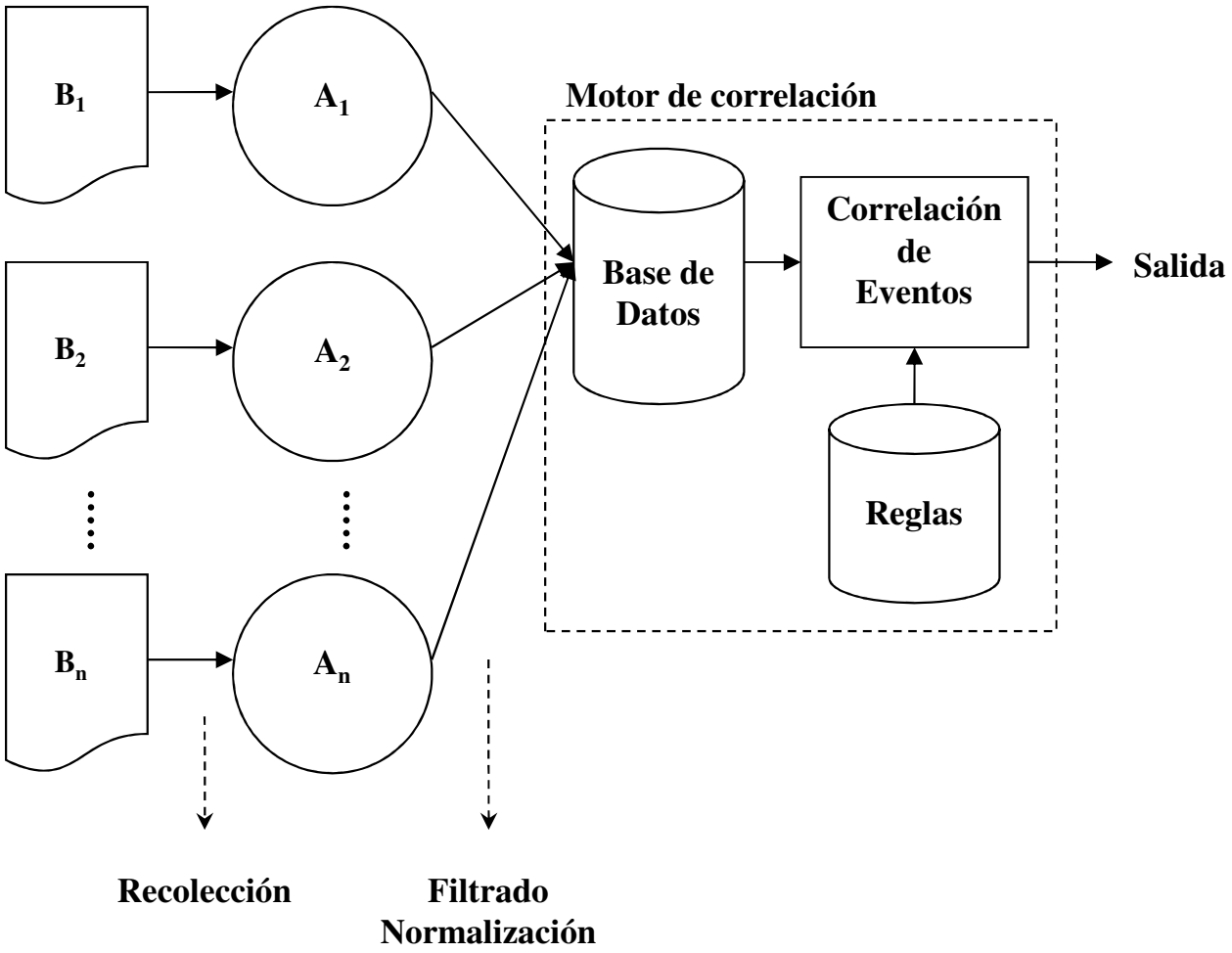
Tecnológico de Monterrey

Algunos aspectos a considerar

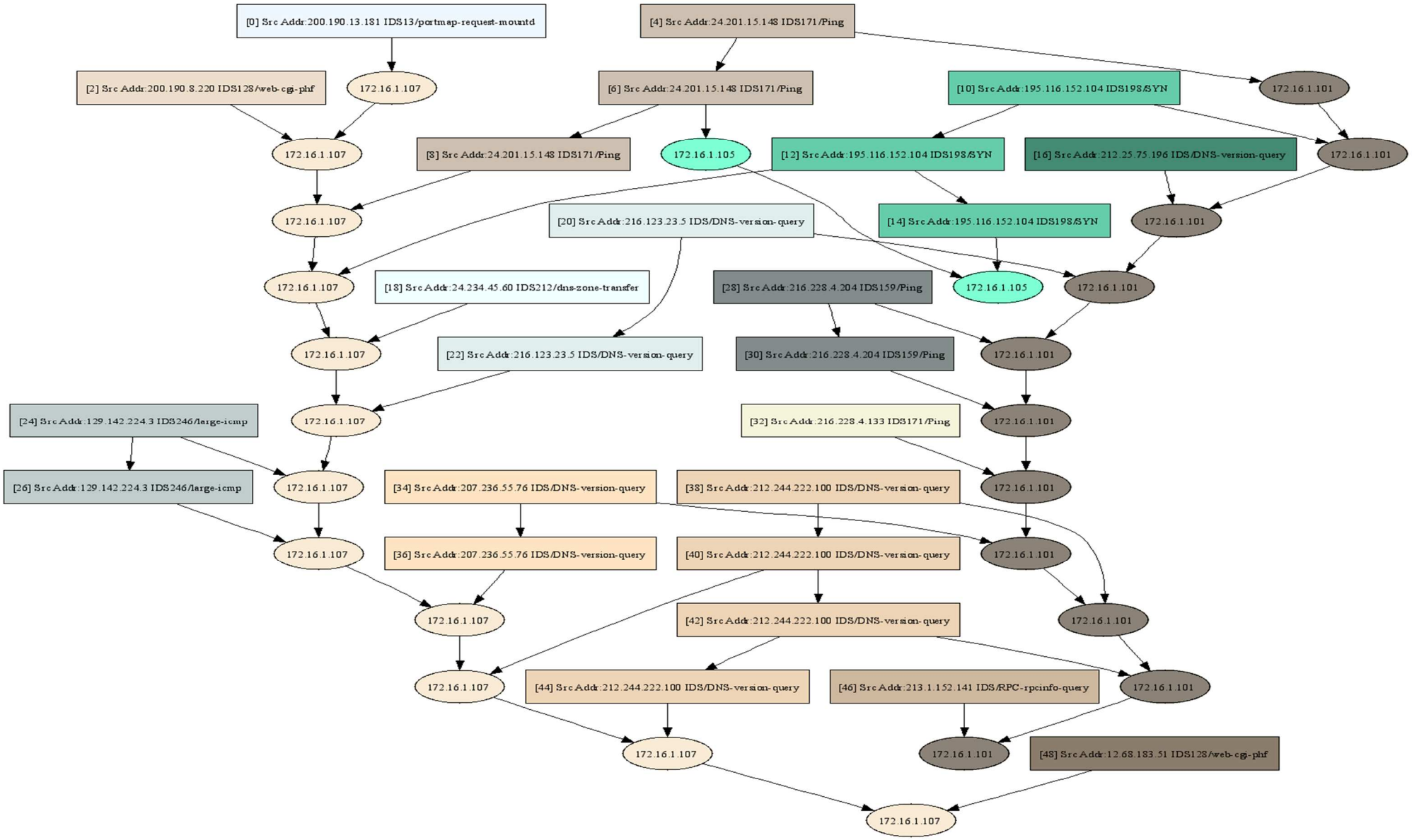
- Es posible configurar los sistemas de tal forma que los eventos:
  - Se escriban en uno o en distintos archivos,
  - Se envíen a través de la red a otra computadora,
  - Se transmitan a algún dispositivo.
- Principales desventajas
  - Espacio disco
  - Desempeño del sistema
- Confidencialidad e integridad de las bitácoras.
- Sincronización de relojes de las fuentes de las bitácoras.

http://www.bipm.org/

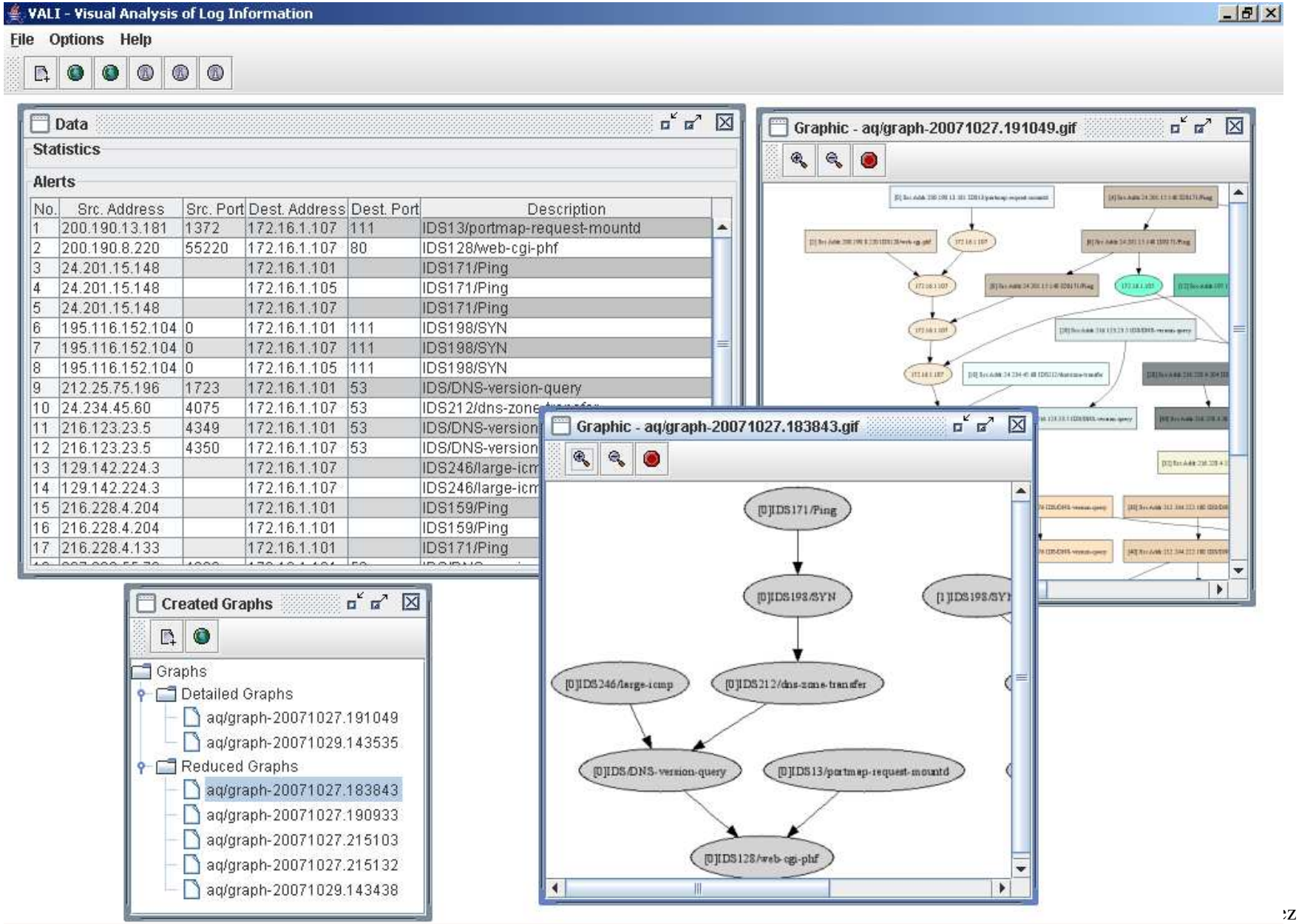
Uniendo todo



Visión gráfica de las bitácoras



El sistema VALI (Visual Analysis of Log Information)



Tecnológico de Monterrey

Los respaldos

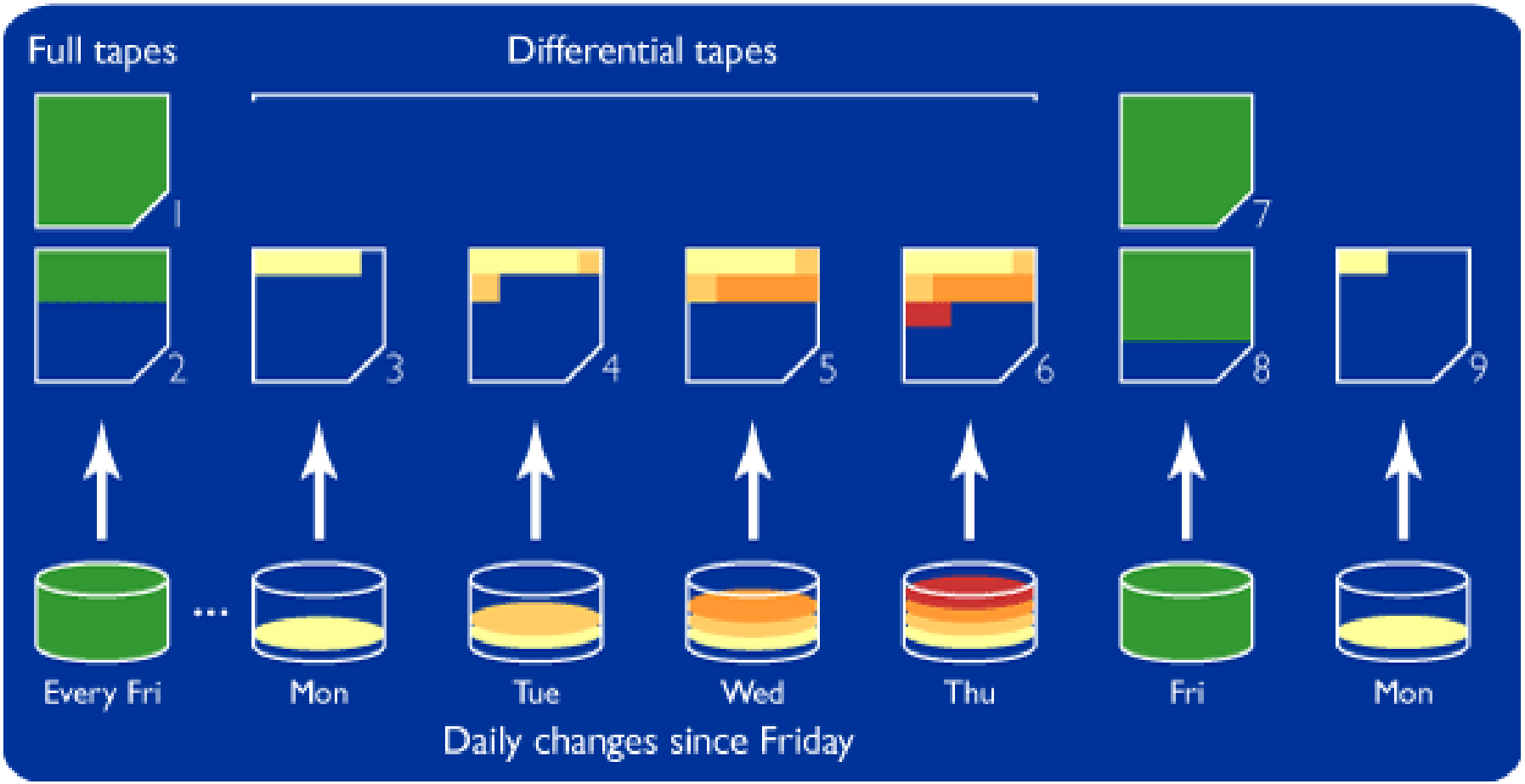
- Es una copia de los datos escrita en cinta u otro medio de almacenamiento duradero.
- De manera rutinaria se recuerda a los usuarios de computadoras que respalden su trabajo con frecuencia.
- Los administradores de sitios pueden tener la responsabilidad de respaldar docenas o incluso cientos de máquinas

Tecnológico de Monterrey

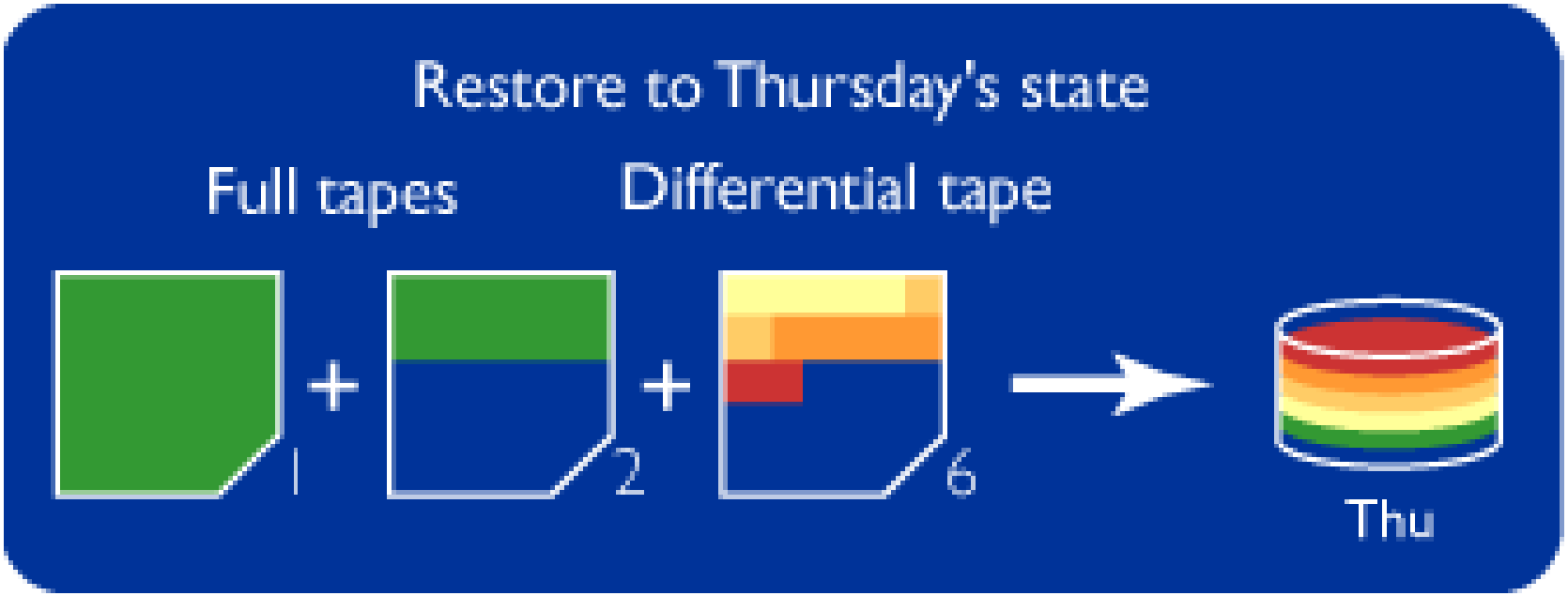
Tipos de respaldos

- Respaldo completo (full backup)
  - Se respaldan todos los archivos, contenidos en el dispositivo protegido en el medio de respaldo.
- Respaldo diferencial (differential backup)
  - Se respaldan **todos los archivos** que han sido modificados desde más reciente respaldo completo.
- Respaldo incremental (incremental backup)
  - Se respaldan **solo aquellos archivos** que han sido modificados desde el más reciente respaldo completo o incremental.

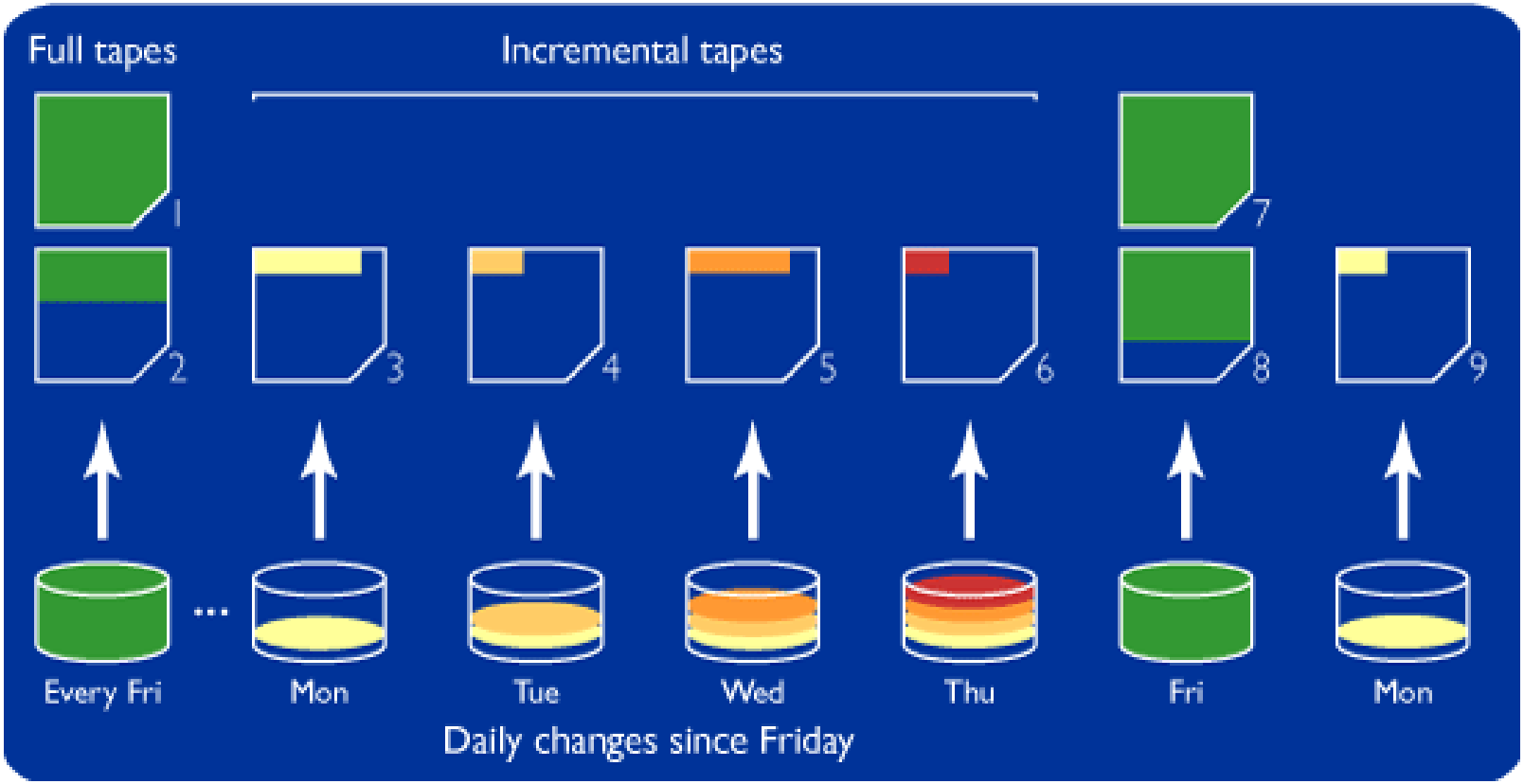
Ejemplos de respaldos completos y diferenciales.



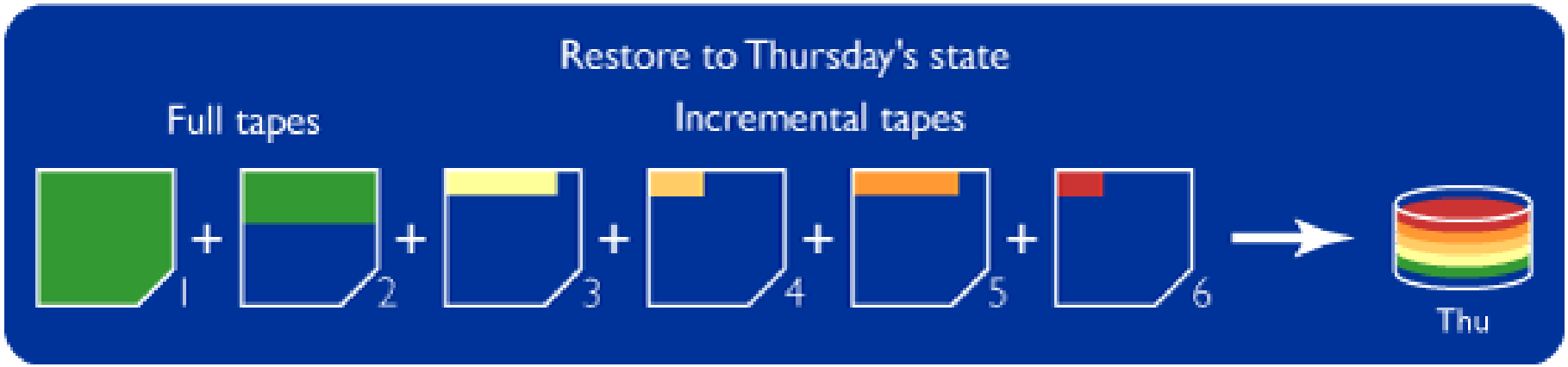
Ejemplo de una restauración diferencial



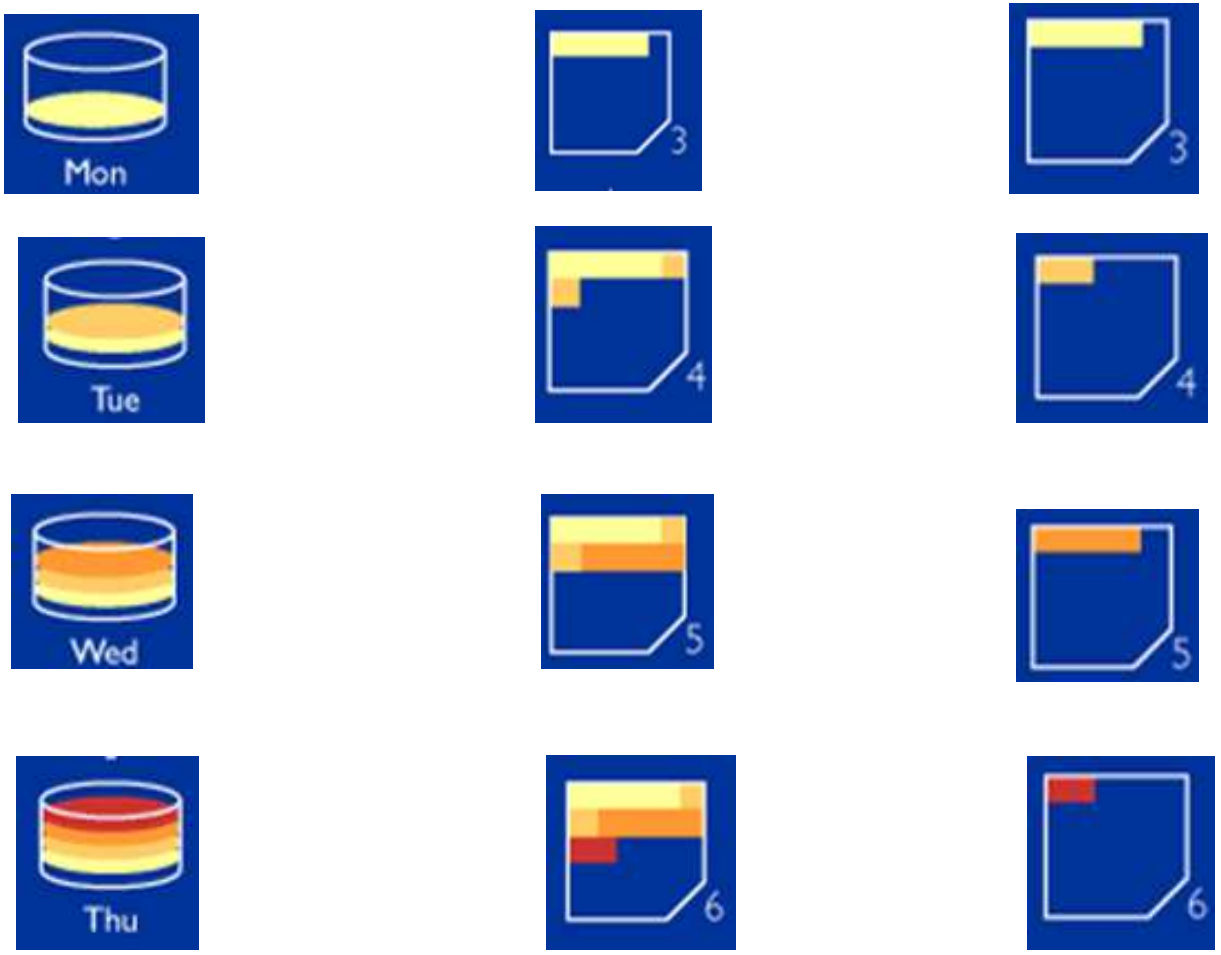
Ejemplo de un respaldo incremental



Ejemplo de un restablecimiento incremental



Diferencial vs incremental



Archivos modificados

Respaldo Diferencial

Respaldo Incremental

Tecnológico de Monterrey

Comparativo

Estrategia respaldo	Base del respaldo	Velocidad del respaldo	Espacio ocupado	Similaridad	Medio requerido para recuperación
Completo	Respaldo completo	Bajo	Grande	/	Solo el respaldo más reciente
Diferencial	Respaldo completo	Medio	Grande	Solo se respaldan archivos modificados	Respaldo completo más reciente y más reciente diferencial.
Incremental	Ultimo respaldo de cualquier tipo	Rápido	Pequeño	Solo se respaldan archivos modificados	Respaldo completo más recuente y todo los respaldos incrementales desde el respaldo completo.

Tecnológico de Monterrey

Concluyendo

- Comparado con el respaldo completo, el respaldo incremental toma menos tiempo de respaldo y produce un archivo de imagen más pequeño.

- Comparado con un respaldo diferencial el respaldo incremental ahorrará espacio de una mejor forma.
  - Esa es la razón principal por la que la mayoría de las personas optan por realizar respaldos incrementales.

Tecnológico de Monterrey

Planes de contingencia

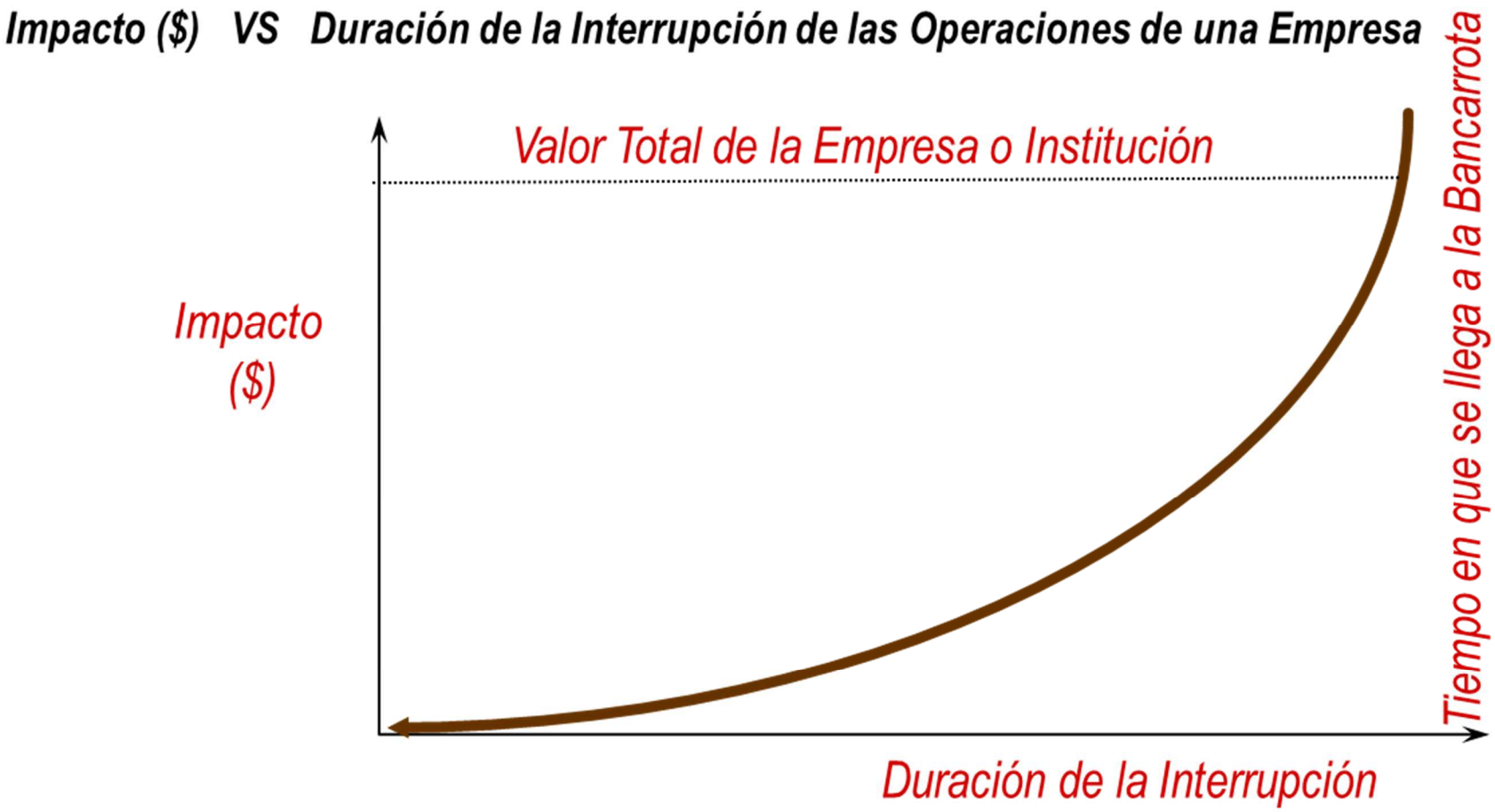
- Consiste en un análisis pormenorizado de las áreas que componen una organización para establecer una política de recuperación ante un desastre.
  - es un conjunto de datos estratégicos de la empresa y que se plasma en un documento con el fin de protegerse ante eventualidades.
- Además de aumentar su seguridad la empresa también gana en el conocimiento de fortalezas y debilidades.
- Si no lo hace, se expone a sufrir una pérdida irreparable mucho más costosa que la implantación de este plan.

Tecnológico de Monterrey

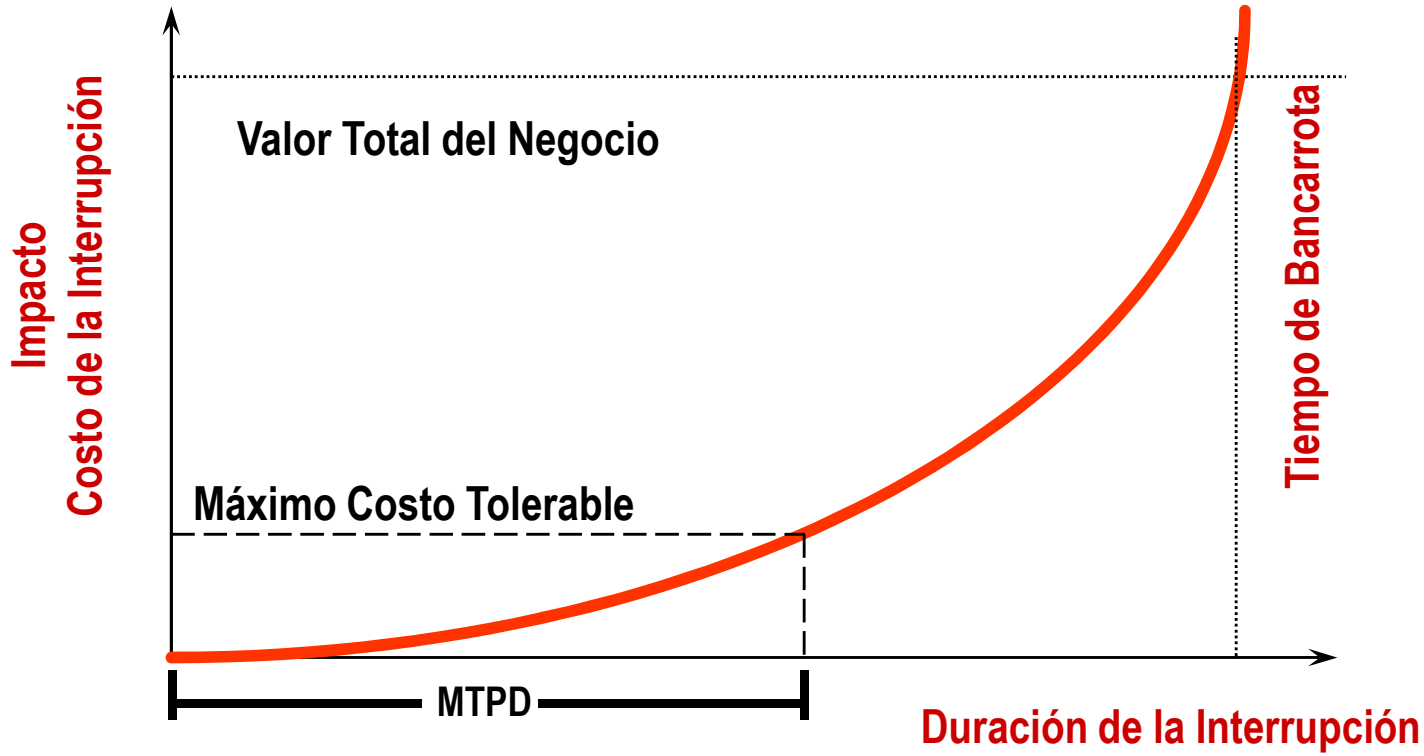
DRP y BCP

- DRP (Disaster Recovery Planning)
  - Recuperar la operación de los **servicios computacionales y de telecomunicaciones** después de un desastre.
- BCP (Business Continuity Planning)
  - Capacidad para mantener la continuidad de las operaciones.
- Business Continuity Management
  - Establecer la administración de la continuidad del negocio como un programa continuo, el cual incluye procedimientos para la ejecución, prueba, actualización y mantenimiento de todos los planes de recuperación y continuidad del negocio.

Impacto desastre en la organización



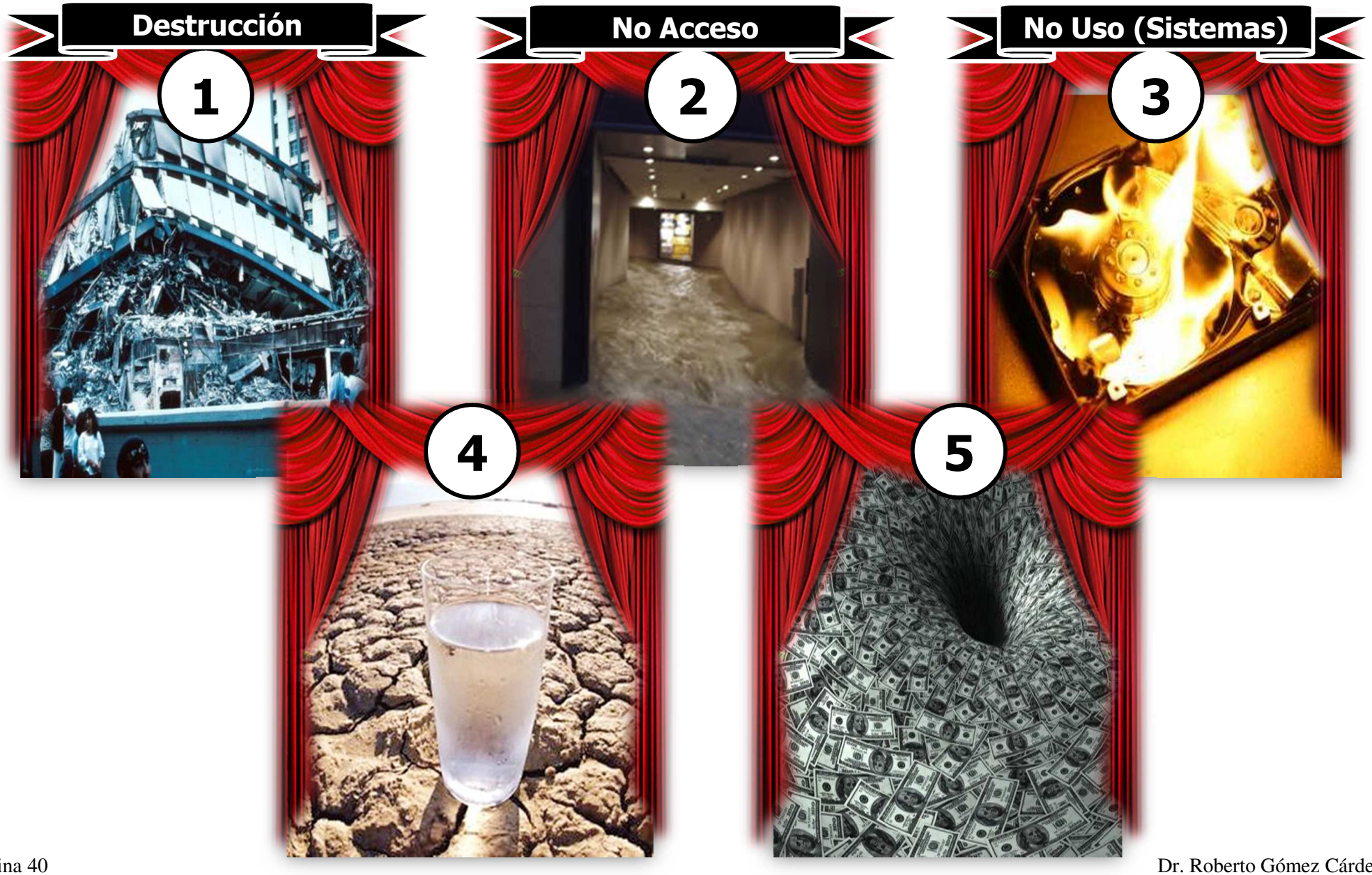
MTD: Maximum Tolerable Period of Disruption



¿Desastre?

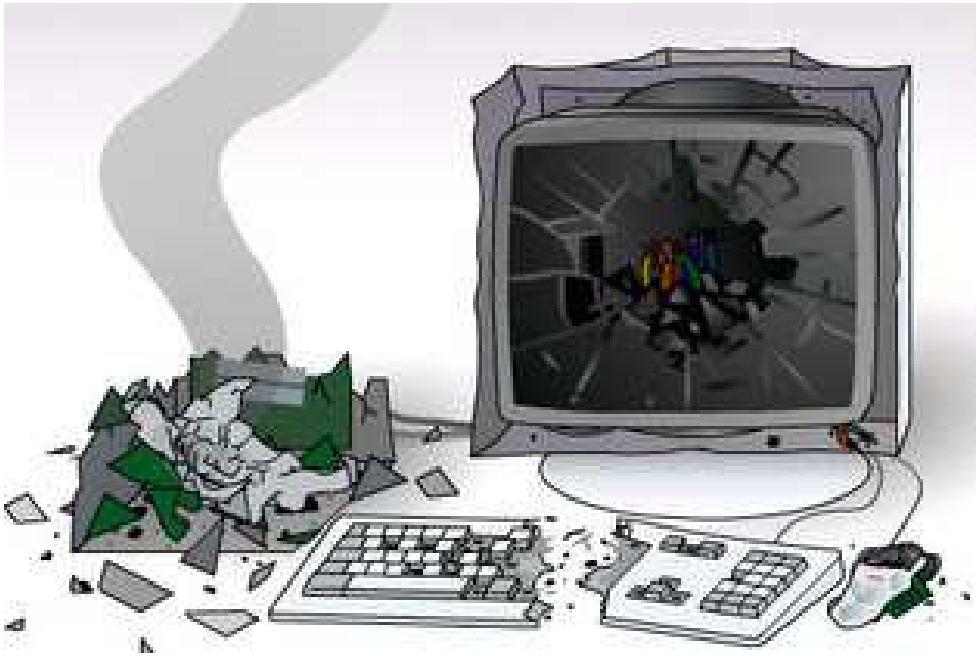
- Desastre es un evento no planeado que ocasiona la “no disponibilidad” de los servicios informáticos por un periodo de tiempo tal que, para restablecer estos servicios, es necesario utilizar facilidades alternas de cómputo y telecomunicaciones en otra localidad.
- Los planes están dirigidos a situaciones catastróficas (no problemas rutinarios).

Una posible clasificación de desastres



Tecnológico de Monterrey

¿Cuál es la causa de desastre más frecuente?



La Causa más frecuente de Interrupciones No Planeadas, Prolongadas y No Tolerables del Servicio Informático en México es:

!!!! Fallas de Hardware !!!

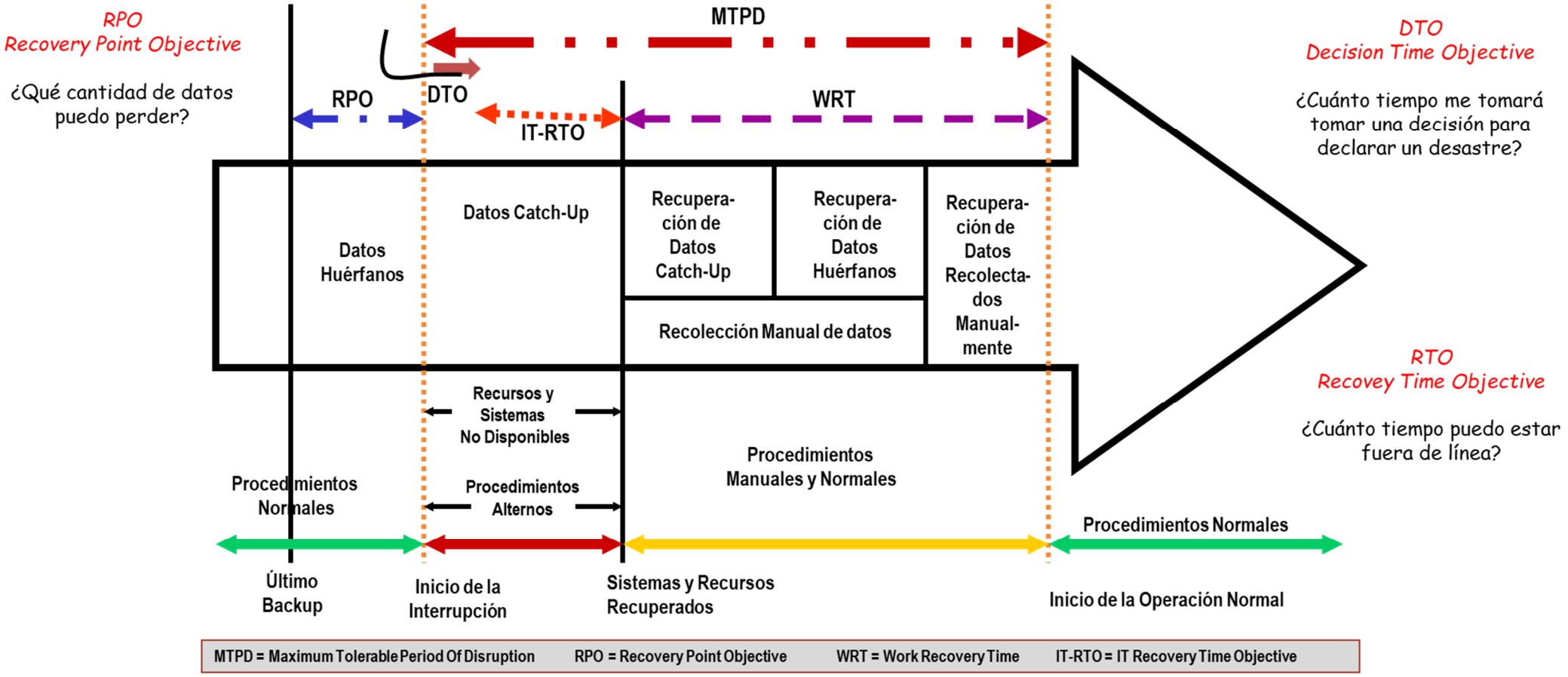
Análisis de Impacto al Negocio (BIA)

- Elemento utilizado para estimar la afectación que podría padecer una organización como resultado de la ocurrencia de algún incidente o un desastre.
- Objetivos:
  - Identificar las Funciones y Procesos Críticos del Negocio, y determinar el impacto de una interrupción significativa del servicio (desastre) en las Unidades Funcionales.
  - Estos impactos pueden ser Financieros en términos de Pérdida de Dinero, o pueden ser de naturaleza Operacional, tal como perder la capacidad para atender a los Clientes y/o Usuarios y no poder proporcionar un servicio de calidad.

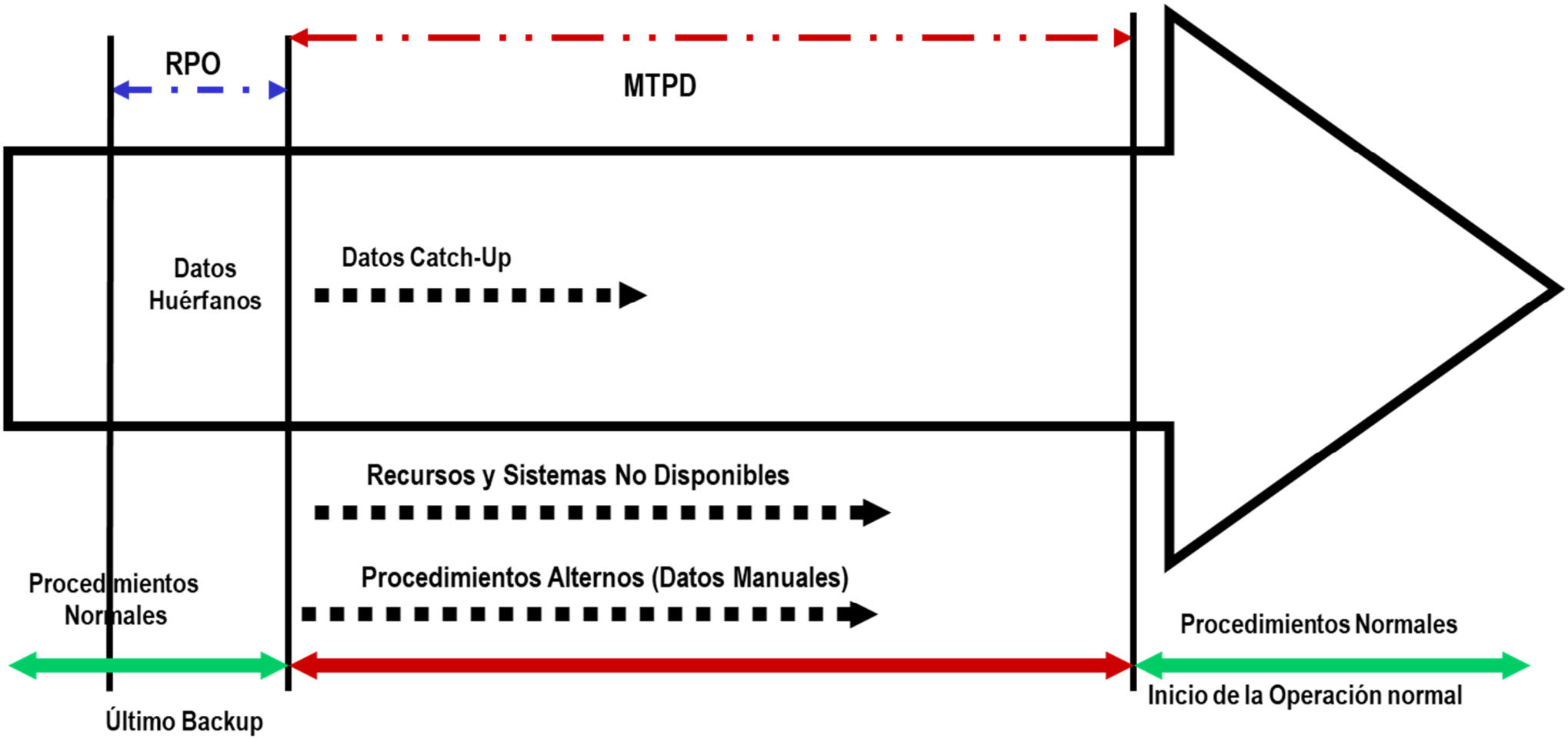
Análisis de Impacto al Negocio (BIA)

- Elemento utilizado para estimar la afectación que podría padecer una organización como resultado de la ocurrencia de algún incidente o un desastre.
- Objetivos:
  - Identificar las Funciones y Procesos Críticos del Negocio, y determinar el impacto de una interrupción significativa del servicio (desastre) en las Unidades Funcionales.
  - Estos impactos pueden ser Financieros en términos de Pérdida de Dinero, o pueden ser de naturaleza Operacional, tal como perder la capacidad para atender a los Clientes y/o Usuarios y no poder proporcionar un servicio de calidad.

Objetivo de Tiempo para Declaración de Desastre (DDTO = Disaster Declaration Time Objective)



Determinación RPOs



Tecnológico de Monterrey

Elementos BCP

- BIA
  - Análisis de Impacto al Negocio
  - Identificar las Funciones y Procesos Críticos del Negocio, y determinar el impacto de una interrupción significativa del servicio (desastre) en las Unidades Funcionales.

- RTO (Recovery Time Objective)
  - Define el límite de tiempo máximo tolerable dentro del cual se recuperan los datos. Si se produce un desastre y los sistemas deben estar disponibles inmediatamente, pero se permite que haya alguna pérdida de datos, el RTO es cero.
  - Sin embargo, si se tolera una hora de recuperación de datos, el RTO es una hora

Tecnológico de Monterrey

Site Producción

Tecnológico de Monterrey

Disponibilidad

ICREA

Nivel	Porcentaje	Tiempo Caída
1	90	876 horas
2	99.0	87 horas
3	99.9	8 horas
4	99.99	58 minutos
5	99.999	5 minutos

Uptime Institute

Nivel	Porcentaje	Tiempo Caída
1	99.671	28.8 horas
2	99.741	22 horas
3	99.982	1.6 horas
4	99.995	0.8 horas

$$\frac{\text{(Tiempo Total) – (Tiempo Caída)}}{\text{(Tiempo Total)}} \text{ X 100}$$

Tecnológico de Monterrey

Sites Alternos

- Hot site
- Warm Site
- Cold site

Tecnológico de Monterrey

Hot Site

- Una sala o instalación de cómputo alterna la cual tiene instalado el equipo de cómputo, las telecomunicaciones, y la infraestructura ambiental requerida para recuperar los sistemas, aplicaciones y servicios que soportan los procesos de la organización.

Warm Site

- Una sala o instalación de cómputo alterna con acondicionamiento eléctrico y ambiental la cual tiene preinstalado algún equipo periférico e interfaces de comunicaciones mas no el procesador central o servidores, los cuales, normalmente son los equipos más caros y que son indispensables para poder realizar la recuperación de los sistemas, aplicaciones y servicios que soportan los procesos de la organización

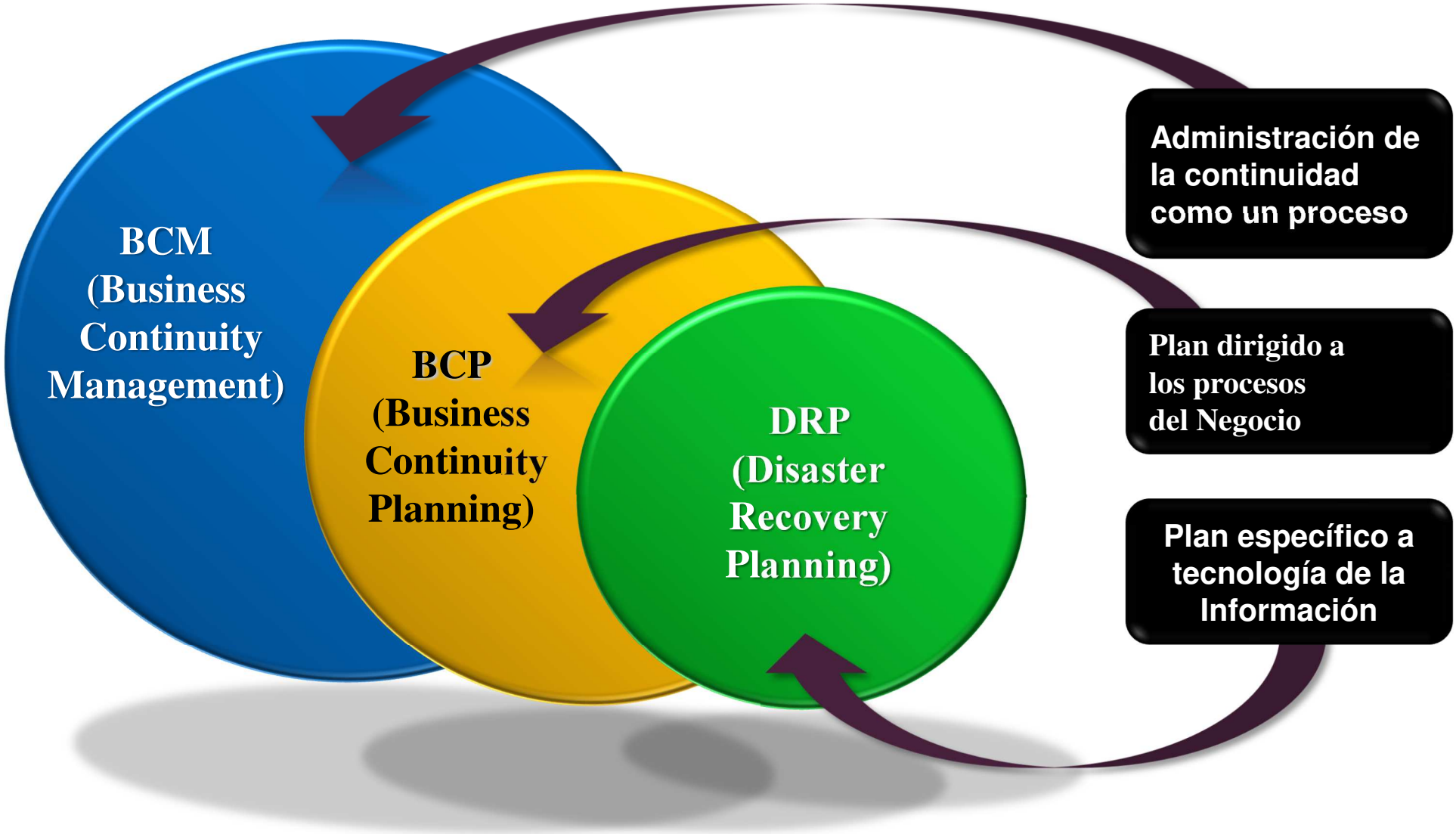
Tecnológico de Monterrey

Cold Site

Una sala o instalación de cómputo alterna que cuenta con la infraestructura ambiental requerida para recuperar los sistemas, aplicaciones y servicios que soportan los procesos de la organización, pero que **no tiene preinstalado ningún equipo de cómputo, equipo de telecomunicaciones ni Red, los cuales deberán ser proporcionados e instalados en la etapa del desastre.**

Tecnológico de Monterrey

BCM vs BCP vs DRP



Tecnológico de Monterrey

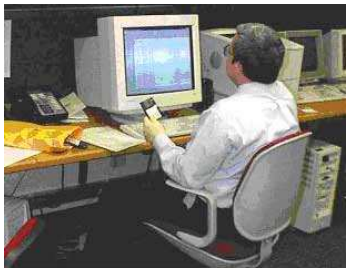
El computo forense

- Se refiere al proceso de aplicar técnicas científicas y analíticas a infraestructura de cómputo, para identificar, preservar, analizar y presentar evidencia de manera que sea aceptable en un procedimiento legal
- ¿Que clase de evidencia ?
  - La computadora involucrada de forma directa.
  - La computadora involucrada de forma indirecta.
- Meta: reconstrucción de eventos pasados
  - Reconstruir que pasó, que lo ocasionó y deslindar responsabilidades

El proceso forense

Identificar evidencia

Preservar evidencia



Analizar evidencia

Presentar evidencia

Tecnológico de Monterrey

Los dos primeros pasos

- Identificar evidencia
  - Identificar la información que se encuentra disponible.
  - Determinar la mejor manera de recolectarla.

- Preservar la evidencia
  - Con la menor cantidad de cambios (contaminación).
  - El forense debe poder demostrar su responsabilidad en cualquier cambio que tenga la evidencia.
  - ¿Cómo demostrar que lo que se tiene como evidencia es exactamente igual a lo que originalmente se recolectó?

Tecnológico de Monterrey

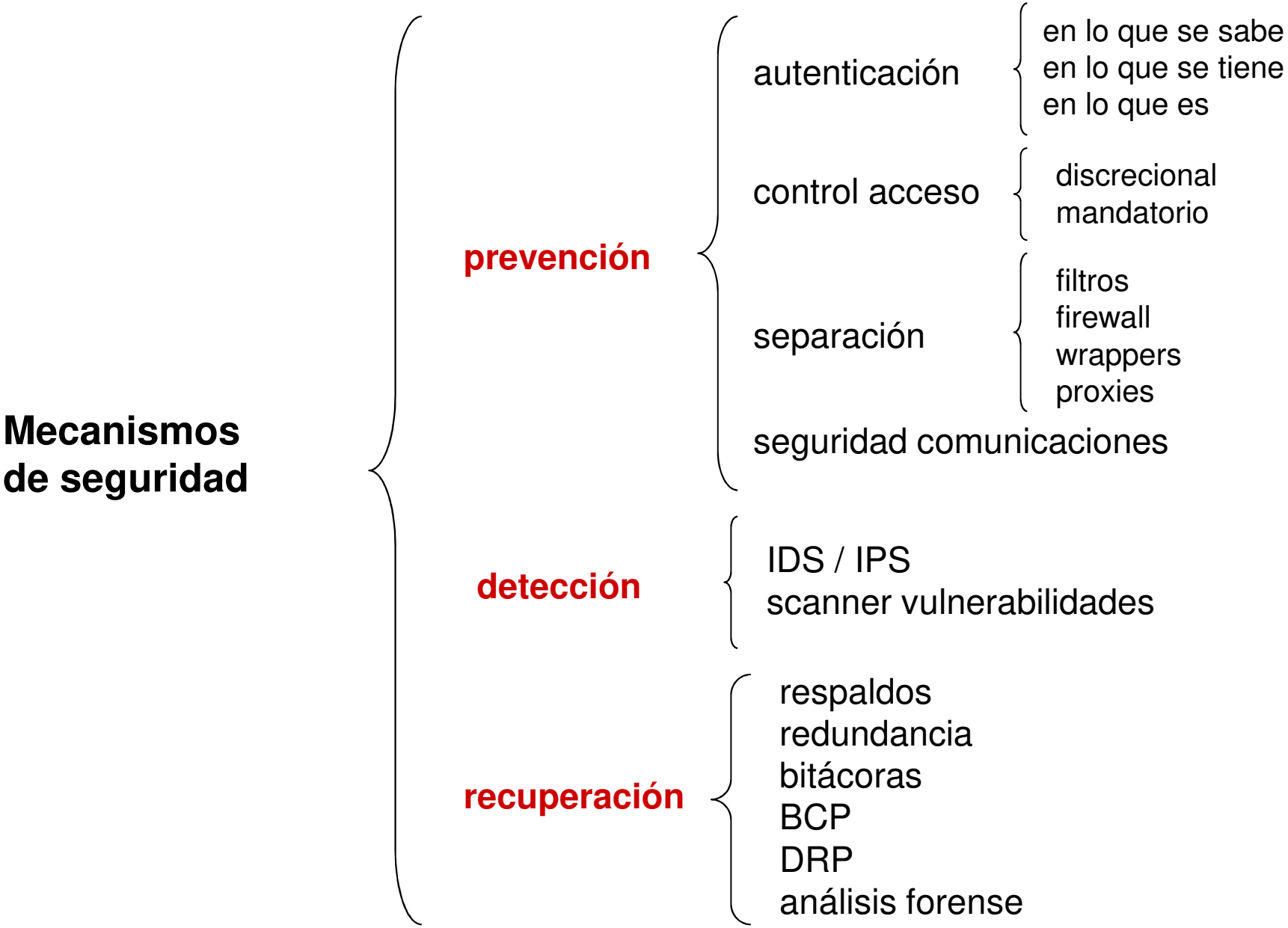
Paso 3: Analizar la evidencia

- Extraer, procesar e interpretar.
- La extracción puede obtener solo imágenes binarias, que no son comprendidas por los humanos.
- La evidencia se procesa para poder obtener información que entiendan los investigadores.
- Para interpretar la evidencia se requiere conocimiento profundo para entender como embonan las piezas.
- El análisis efectuado por el forense debe de poder ser repetido.

Paso 4: Presentar la Evidencia

- Abogados, fiscales, jurado, etc.
- La aceptación dependerá de factores como:
  - La forma de presentarla (¿se entiende?, ¿es convincente?)
  - El perfil y credibilidad del expositor.
  - La credibilidad de los procesos usados para preservar y analizar la evidencia.
    - Aumenta si se pueden duplicar el proceso y los resultados.
- Especialmente importante cuando la evidencia se presenta en una corte.

Clasificación mecanismos seguridad



Tecnológico de Monterrey

Algunos principios de Seguridad

- Propuestos por la OECD en 1992
  - Organisation for Economic Co-operation and Developmen
- Entre los más importantes encontramos
  - Accountability (Responsabilidad / Rendición de Cuentas)
  - Awareness (Sensibilización)

Accountability

- Propiedad que asegura que las acciones de una entidad deben llevar unicamente a dicha entidad (ISO 7498-2)
- La propiedad que habilita actividades en un sistema ADP que conducen (trace) a individuos que pueden ser declarados responsables de dichas actividades (DOE 5636.2A)

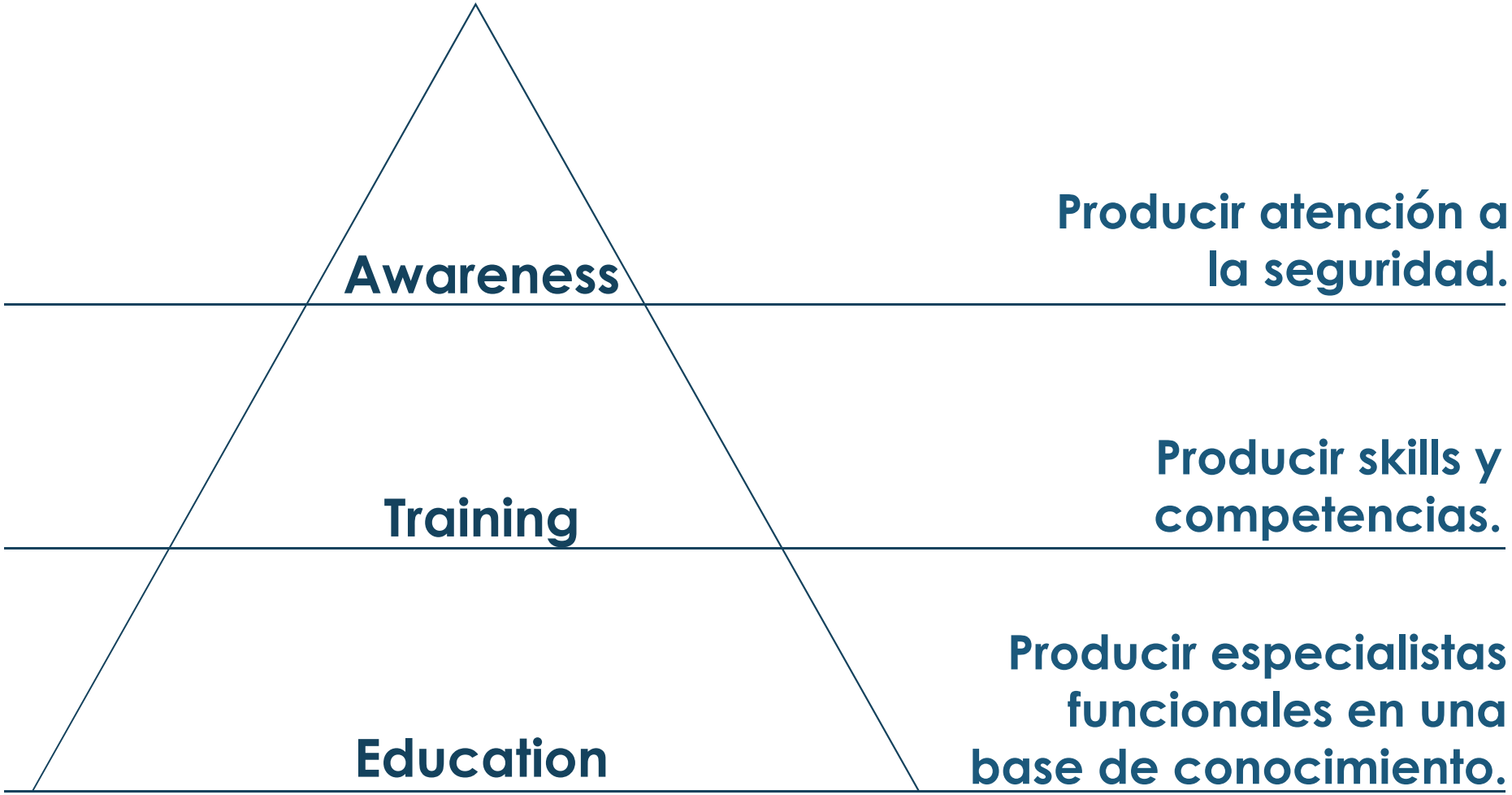
Awareness

- Lograr que los usuarios comprendan su rol y responsabilidad en la protección de la integridad, confidencialidad y disponibilidad de la información y los activos de su organización.
- Que los usuarios entiendan que la seguridad de la información es responsabilidad de todos, no sólo del Departamento de TI.
- Lograr que los usuarios comprendan que sus acciones pueden impactar de forma adversa en la seguridad de la organización.

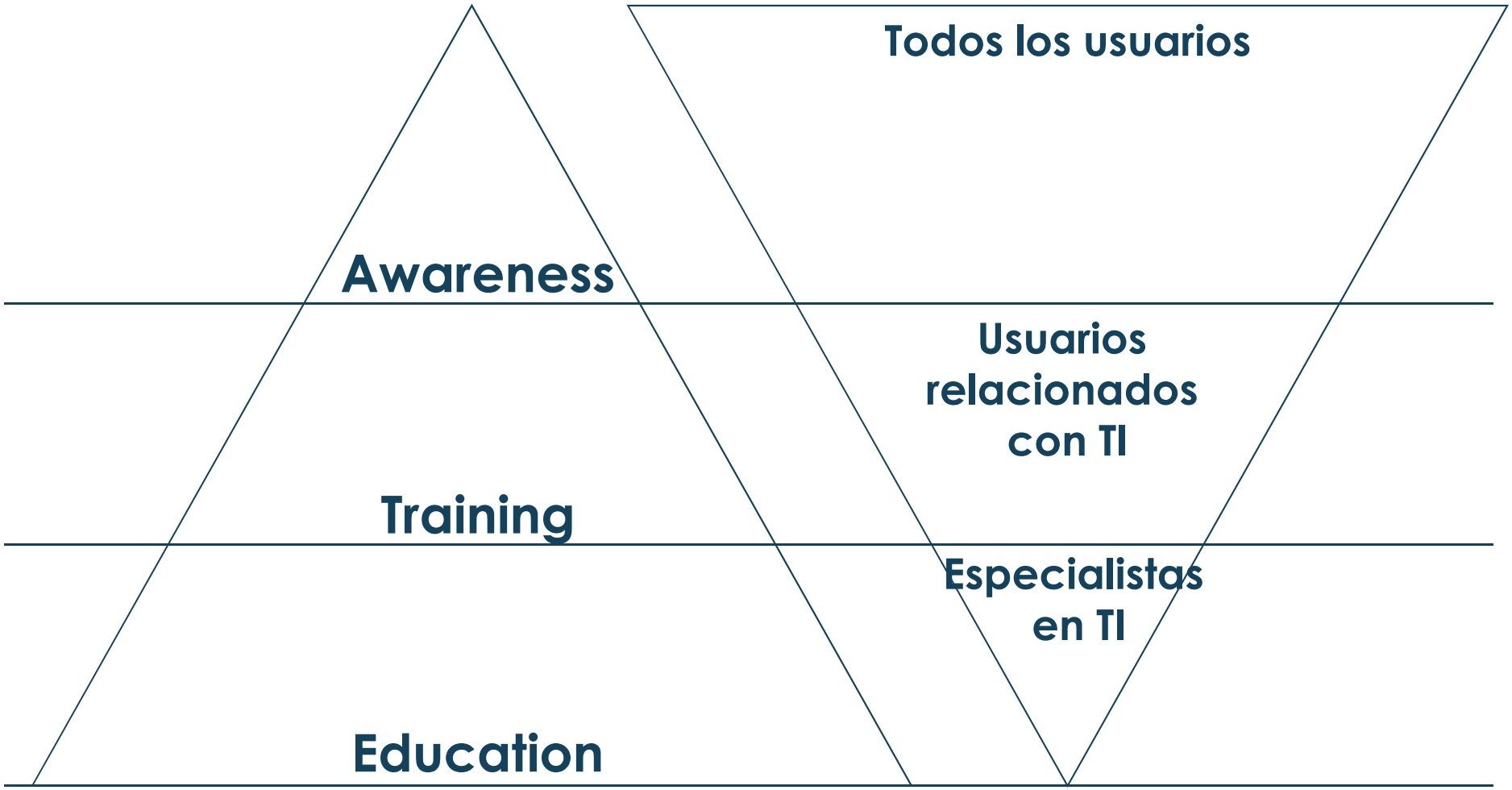
Awareness, Training, Education

- Awareness:
  - Está enfocado a lograr conciencia de la importancia de la seguridad.
  - Los mensajes deben ser simples, claros y presentados en un formato fácil de entender para la audiencia.
- Entrenamiento:
  - Está enfocado a lograr un mejor nivel de entendimiento de las prácticas de seguridad.
  - Las técnicas pueden incluir clases formales, entrenamiento personalizado y paquetes de educación.
- Educación:
  - Está enfocado a lograr competencias específicas y especialistas.
  - Las técnicas incluyen capacitaciones especializadas y cursos de propósito específico.

Triangulo del conocimiento organizacional



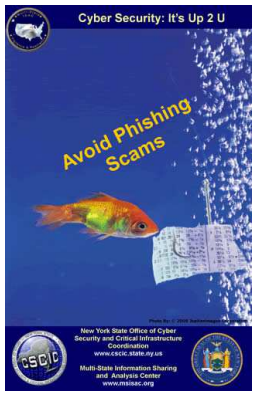
Triangulo del conocimiento organizacional

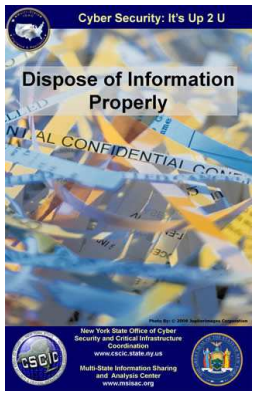


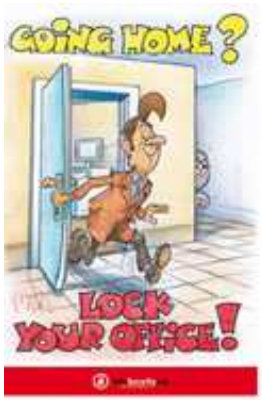
Ejemplos awareness

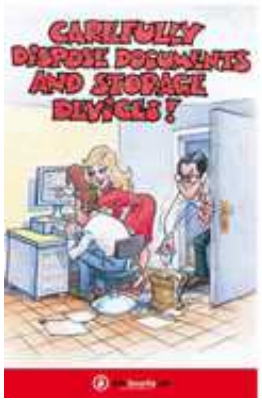
Tips de Seguridad para el uso de Internet

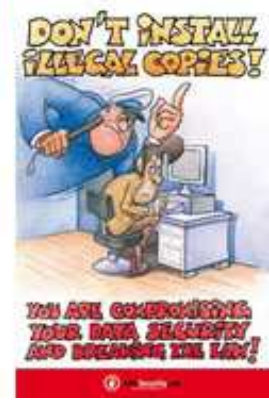
- **No concretes** una cita con un "**amigo**" en línea, ya que es un desconocido
- **No facilites** información **personal** cuando navegues por Internet en comunidades, chat o mensajería instantánea
- **No llenes** formularios de registro, perfiles **personales**, ni participes en concursos en línea
- **No olvides** que hay **riesgos** al descargar programas, ya que pueden bajar accidentalmente software espía o un virus informático
- **Si algo** o alguien en línea te hace sentir **incómodo** o amenazado da aviso a las autoridades competentes
- **Evita sitios** que muestren **violencia** y/o pornografía, ya que son sitios de alto riesgo
- **No te conectes** a sitios de descarga de música gratuita, pueden **dañar** tu computadora e infringes las leyes de autor
- **En Internet** sigues siendo tú y tu comportamiento debe ser **responsable**
- **No debes** utilizar Internet para **propagar** rumores, molestar, ni amenazar a otros
- **Acepta** y actualiza de forma **periódica** tu sistema operativo











Top 10 Reasons Computers Don't Have Security.

10. I just use my computer for email and web browsing.
9. I've never had any virus problems.
8. Well, I did have some security, but it kept popping up all the time.
7. It might crash my system.
6. My subscription kept expiring.
5. It slows down my system.
4. I thought it came with the computer.
3. It's too expensive.
2. Macs don't need security.
1. I don't know what to buy or how to install it.

Fuente: SANS: Ouch! Newsletter

Servicios propuestos por OSI

Norma 7498-2

- Autentificación.
  - autenticación del cliente
  - autenticación del servidor
- Control de Acceso
  - se aplica a los usuarios y procesos que ya han sido autentificados
- Confidencialidad.
  - principal mecanismo: criptologia
- Integridad de Datos
  - CRCs y huellas digitales.
- No Repudiación.

Tecnológico de Monterrey

No Repudiación.

- Permite comprobar las acciones realizadas por el origen o destino de los datos.
  - con prueba de origen.
  - con prueba de entrega.
- Los mecanismos principales son los certificados y las firmas digitales.
- Dos objetivos, garantizar:
  - que alguien que haya recibido un pago no pueda negar este hecho.
  - que alguien que haya efectuado un pago no pueda negar haberlo hecho.

Tecnológico de Monterrey

AAA

Authentication, authorization, y accounting

Tecnológico de Monterrey

La AAA

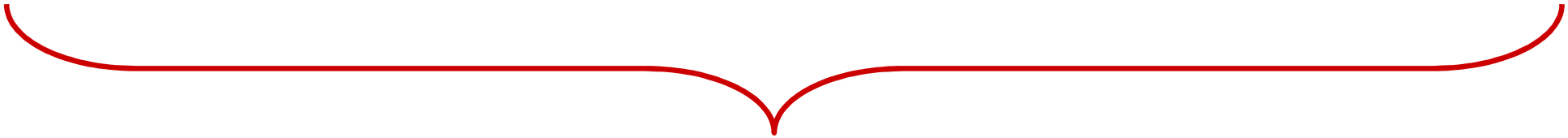
- Authentication, authorization, y accounting
  - consiste de un framewok que proporciona los tres servicios
- El objetivo del grupo de trabajo AAA es definir un protocolo que implemente autenticación, autorización y accounting lo suficientemente general para ser usado en aplicaciones diferentes.
- Definición de la arquitectura
  - de Laat, C. & Gross, G. & Gommans, L. & Vollbrecht, J. & Spence, C., Generic AAA architecture, Internet Draft (work in progress), January 2000.

Esquema general

proporcionar un método para identificar un usuario. p.e. login/password

autorización para llevar a cabo ciertas tareas

mide y/o almacena los recursos que un usuario consume durante su acceso



Servidor AAA

Tecnológico de Monterrey

Evaluación

- Como evaluar que un sistema es seguro o no
- Tres mecanismos
  - la auditoría de seguridad (security audit),
  - la evaluación de la seguridad (security assessment)
  - las pruebas de penetración (penetration testing o PEN TEST).

Tecnológico de Monterrey

Auditoría

- Proceso formal utilizado para medir aspectos de alto nivel de la infraestructura de seguridad desde la perspectiva organizacional (Ray Kaplan)
- Auditores limitan el alcance y no incluyen detalles técnicos de bajo nivel:
  - fallas en protocolos de comunicación.
- Posible encontrar auditorias con mayor nivel de profundidad y alcance, con datos y recomendaciones técnicas detalladas.
- Generalmente se lleva a cabo por auditores EDP (Electronic Data Processing) certificados bajo las directrices de un comité

Evaluación Seguridad Informática

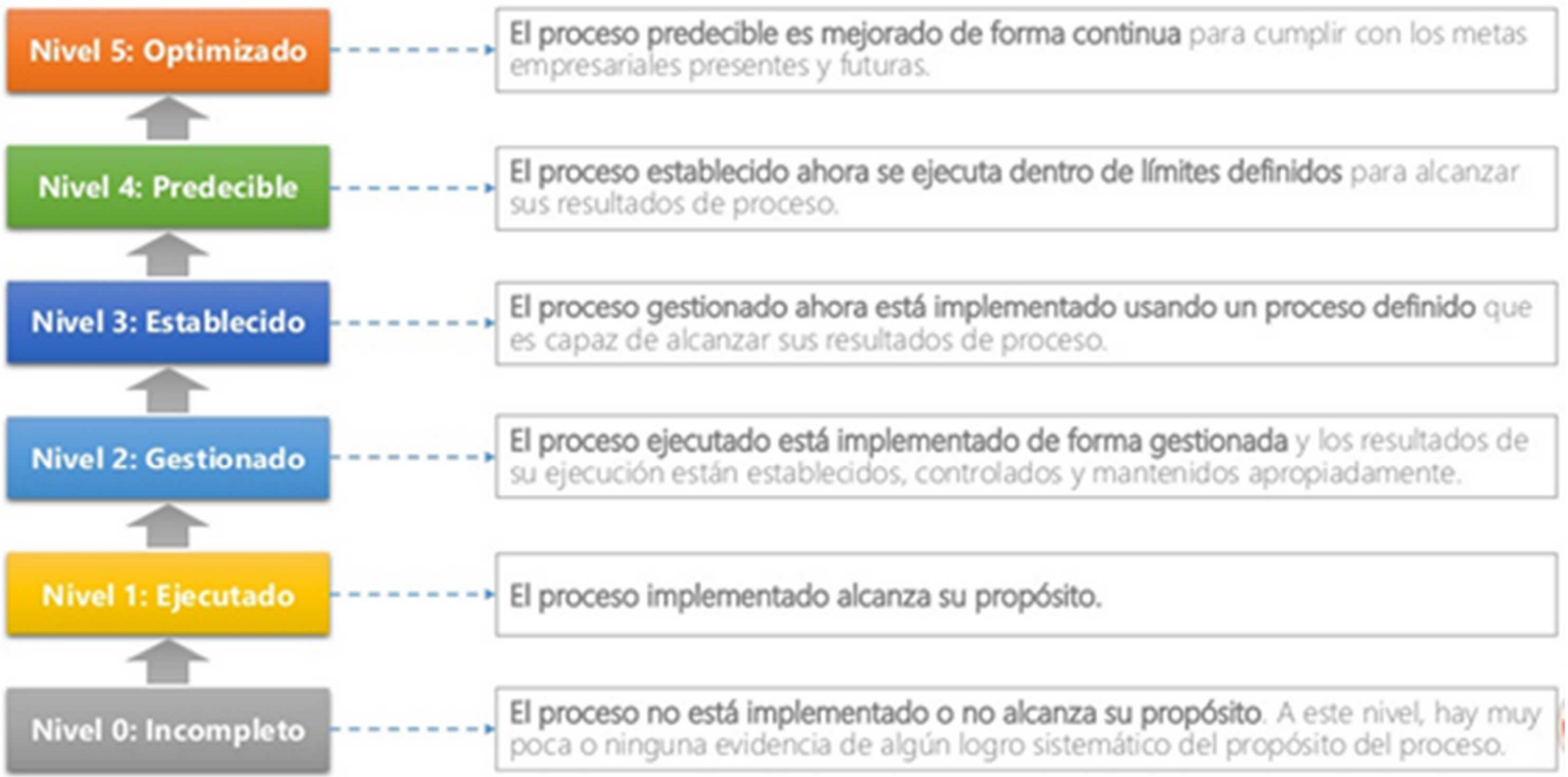
- Método detallado y sistemático para utilizados para evaluar la efectividad de los controles de seguridad cibernética en un sistema digital.
- En particular, los métodos y procedimientos de evaluación se utilizan para determinar si los controles de seguridad se implementan correctamente, funcionan según lo previsto y producen el resultado deseado con respecto al cumplimiento de los requisitos de seguridad del propietario del activo.

Tecnológico de Monterrey

Etapas

1. Análisis situación actual
   - Evaluación controles de seguridad de la información en los aspectos de personas, procesos y herramientas de una organización.
   - Alcance evaluación se puede personalizar para incluir solo ciertas áreas temáticas.
   - La metodología de evaluación se basa en estándares de la industria.
2. Definición del estado objetivo
   - Recomendaciones para mejorar seguridad información en áreas identificadas.
   - Posible seleccionar solo recomendaciones que se adapten a sus aspiraciones de madurez de seguridad de la información.
3. Roadmap
   - Un enfoque para priorizar las inversiones en las áreas de mejora identificadas en función de los objetivos comerciales, de TI y de seguridad de la información de su organización.
   - Propuesto a corto, mediano y largo plazo.

Niveles madurez Cobit

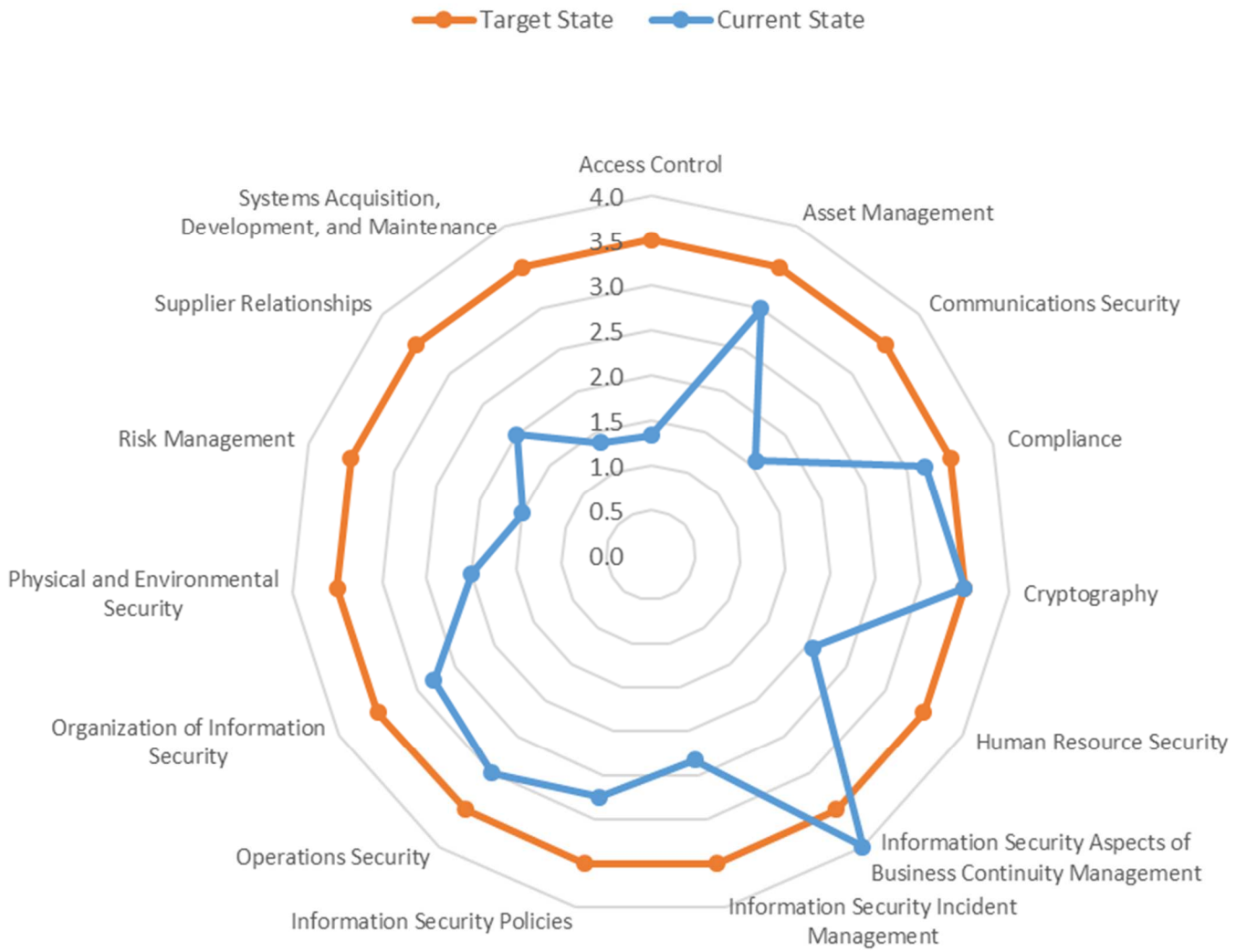


Fuente: http://gesegtic.blogspot.com/2014/09/analisis-de-madurez-y-capacidad-de.html

Los niveles y status

Fuente: Modelos de Madurez de Seguridad de la Información, Roberto Arbeláez

Ejemplo entregable CMM (Capability Maturity Model)



Fuente: http://blog.calanceus.com/3-steps-to-a-successful-cyber-security-assessment

Tecnológico de Monterrey

Pruebas de penetración

- Conjunto de metodologías y técnicas, que se llevan a cabo para proporcionar una evaluación integral de las debilidades de los sistemas informáticos.
- Consiste en reproducir intentos de acceso, a cualquier entorno informático, de un intruso potencial desde los diferentes puntos de entrada que existan, tanto internos como externos a la organización.
- El objetivo final es determinar el grado de acceso a la infraestructura informática que tendría un atacante con intenciones maliciosas.
- Reportan a comité seleccionado por la organización

Tecnológico de Monterrey

Tipos pruebas de penetración

- Formales e informales
- Externas o internas
- Cajas blancas, negras o grises

Pruebas de penetración formales e informales

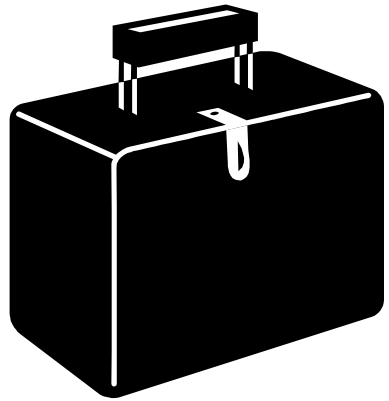
- Informales
  - Orientadas por objetivos técnicos de la infraestructura de comunicaciones, en un esfuerzo por penetrar tan rápido como se pueda dicha infraestructura.
- Formales
  - Orientadas a verificar debilidades en las políticas de seguridad, soportadas en procedimientos y prácticas que pueden comprometer la información sensible de la organización.

Pruebas de penetración internas y externas

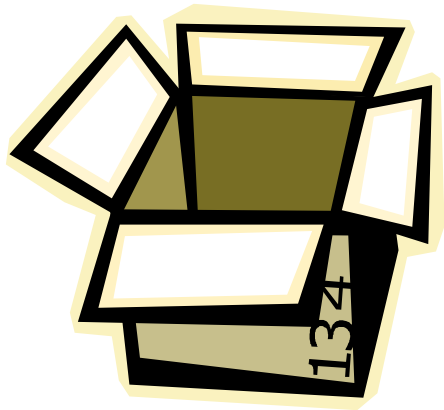
- Externas
  - El objetivo es acceder en forma remota a los equipos de la organización y posicionarse como administrador del sistema.
  - Se realizan desde fuera del Firewall y consisten en penetrar la Zona Desmilitarizada para luego acceder a la red interna.
- Internas
  - Trata de demostrar cual es el nivel de seguridad interno.
  - Se deberá establecer que puede hacer un usuario interno a la organización y hasta donde será capaz de penetrar en el sistema siendo un usuario con privilegios bajos.

Pruebas de penetración: cajas negras, blancas y grises

- Caja negra (blind)
  - No se cuenta con ninguna información del sistema y/o red que se va a analizar.

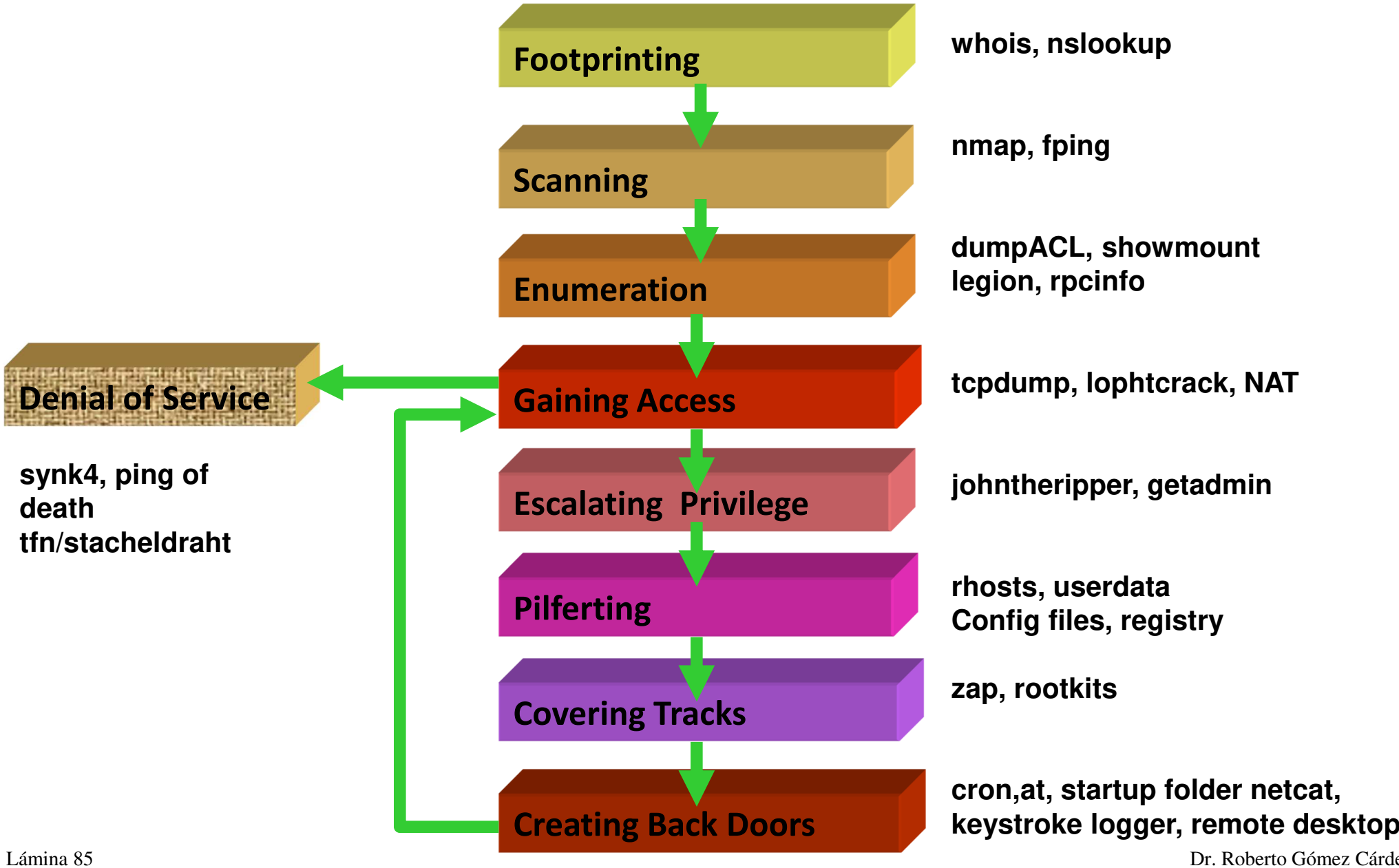


- Caja blanca (full disclosure)
  - Se tiene acceso a toda la información (datos internos, código fuente, etc.) del sistema y/o red que debe analizar.



- Caja gris (partial disclosure)
  - Caso intermedio a los anteriores.
  - El consultor cuanta con un mapa de la red y los segmentos de direcciones relevantes, pero no con el código fuente de los aplicativos disponibles.

Pasos en una prueba de penetración



Tecnológico de Monterrey

Metodologías

- El éxito de una buena prueba de penetración depende de capacidad y la experiencia del que la lleva a cabo, es bueno apoyarse en una metodología
- Ejemplos metodologías
  - Wardoc . Rhino9 y Neonsurge
    - Recopilación de información (NetBIOS e IIS)
    - Penetración (NetBIOS e IIS)
  - NIST 800-42 (Guía para evaluar la seguridad en red)
    - Planeación
    - Descubrimiento
    - Ataque (nuevamente descubrimiento)
    - Reporte (análisis causas raíz)

Tecnológico de Monterrey

La metodología OSSTMM

- Open Source Security Testing Methodology Manual
  - Autor: Pete Herzog
- Metodología dividida en secciones, módulos y tareas.
- Mapa de Seguridad (6 secciones)
  - Seguridad de la Información
  - Seguridad de los Procesos
  - Seguridad de las Tecnologías de Internet
  - Seguridad de las Comunicaciones
  - Seguridad Inalámbrica
  - Seguridad Física
- Base: Valores de Evaluación de Riesgos
  - solo aplicación efectiva de los controles y no solo su existencia.
- Cada sección se compone de varios módulos y estos a su vez de tareas.

Tecnológico de Monterrey

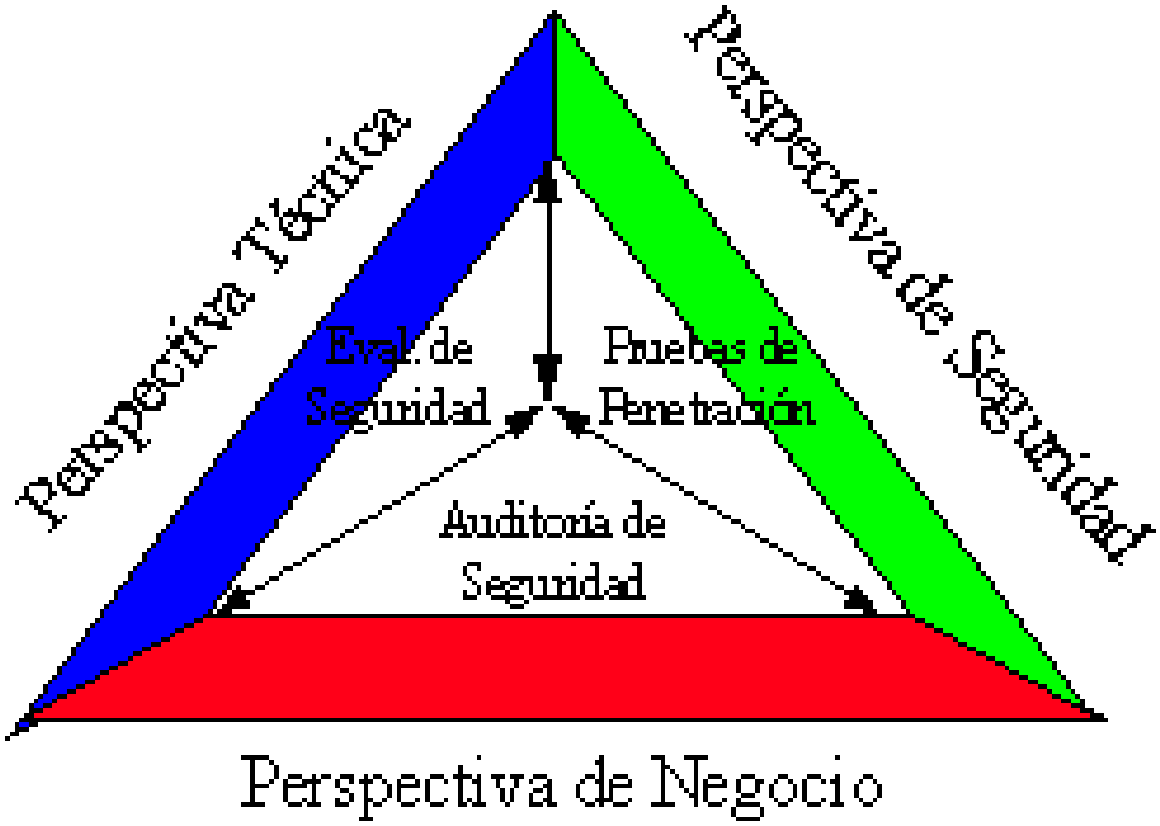
Otras metodologías

- Breaking into computer networks form the Internet, Roelof Temming (sensepost)
- An approach to systematic network auditing - Mixter (TFN)
- Impoving the security of your site by breaking into it . Dan Farme y Wietse Venema
- Managing a Network Vulnerability Assessment . Peltier y Blackley
- Hack I.T. . T.J. Klevinsky
- Hacking Exposed . McClure, Scambray, Kurtz

Reporte prueba penetración

- Se debe explicar paso a paso cómo se llevó a cabo la actividad hasta alcanzar y penetrar la infraestructura de comunicaciones.
- Así mismo, documenta cómo se aprovecharon las debilidades de los programas o deficiencias en las configuraciones del hardware para ingresar de manera no autorizada al perímetro de comunicaciones de la empresa.
- Dos reportes: técnico y ejecutivo

¿Cuál de las tres usar?



Tecnológico de Monterrey

Mecanismos detección y recuperación

Roberto Gómez Cárdenas

rogomez@itesm.mx

http://cryptomex.org

@cryptomex

Tecnológico de Monterrey

Arquitectura de seguridad

- Vista total de la arquitectura del sistema desde un punto de vista de seguridad.
- Da a conocer recomendaciones de donde, dentro del contexto general de la arquitectura del sistema, se deben colocar los mecanismos de seguridad.
- Proporciona una percepción de los servicios de seguridad, mecanismos, tecnologías y características que pueden ser usados para satisfacer requerimientos de seguridad del sistema.

Tecnológico de Monterrey

Ejemplo arquitectura