Tecnológico de Monterrey

Introducción a la Seguridad Informática

Roberto Gómez Cárdenas

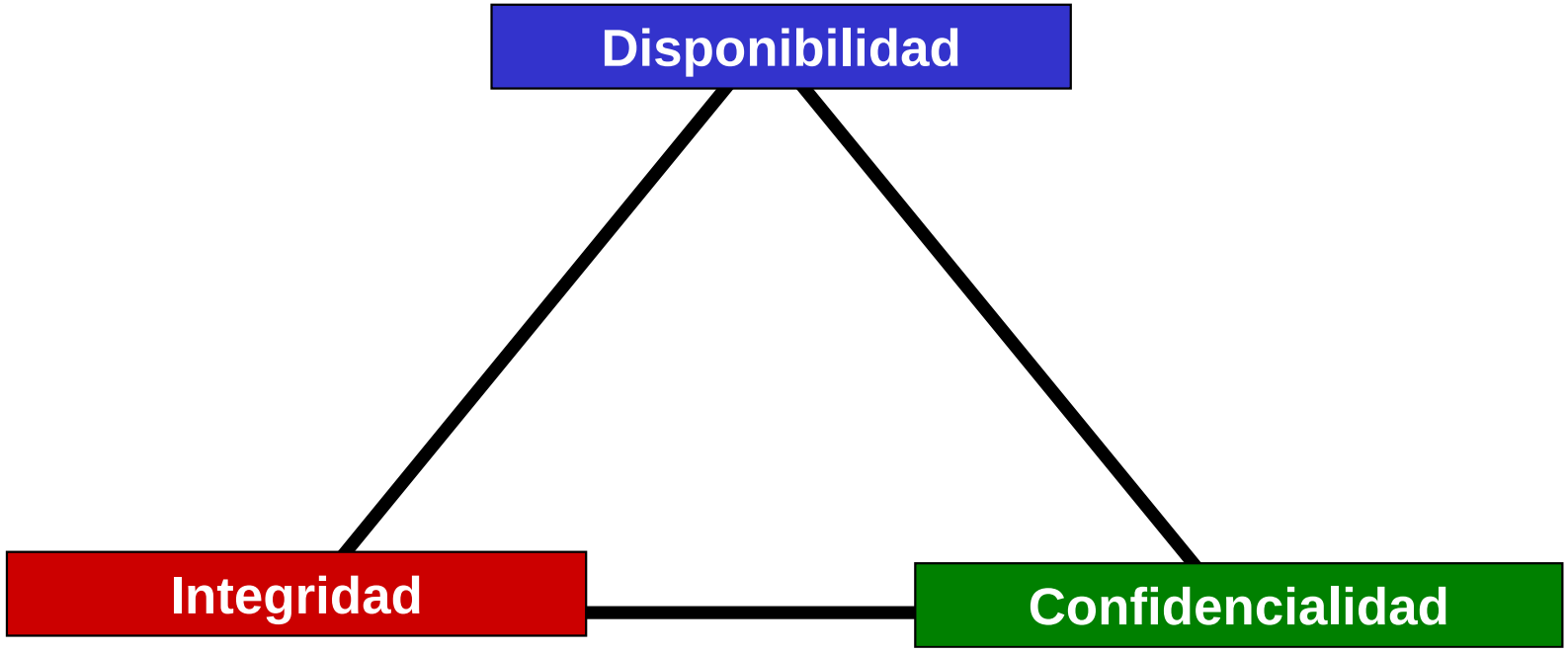
rogomez@itesm.mx

http://cryptomex.org

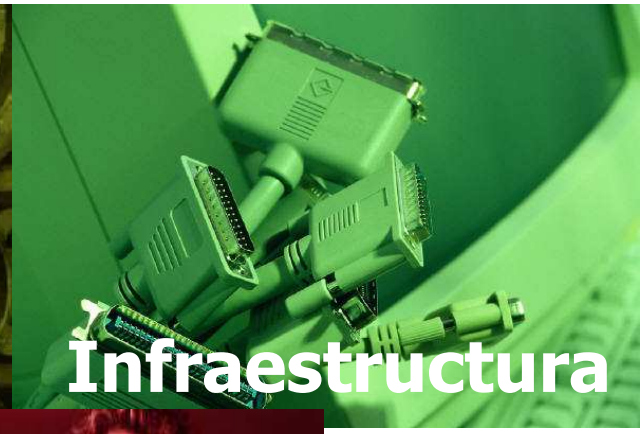
@cryptomex

Seguridad Computacional

El conjunto de políticas y mecanismos que nos permiten garantizar la ***confidencialidad***, la ***integridad*** y la ***disponibilidad*** de los recursos de un sistema.



La seguridad involucra 3 dimensiones (no sólo una)



Diseñar pensando en la seguridad

Roles y responsabilidades

Auditar dar seguimientos y rastrear

Mantenerse al día con el desarrollo de seguridad

Falta de conocimiento

Falta de comrpomiso

Falla humana

Los productos no cuentan con funciones de seguridad

Demasiado difícil mantenerse al día

Muchos problemas no se ven abordados por estándares técnicos (BS 7779)

Los productos tienen problemas

Activos de informacion

- Cualquier recurso de SW, HW, Datos, Administrativo, Físico, de Personal de Comunicaciones, etc.
- Activos intangibles
  - Imagen, propiedad intelectual, etc
- Ejemplos
  - Servidores
  - Bases de Datos
  - Redes
  - Usuarios
  - Aplicaciones
  - Sistemas Operativos
  - Dinero
  - Información
  - etc

Tecnológico de Monterrey

Amenaza

- Circunstancia o evento que puede causar daño violando la confidencialidad, integridad o disponibilidad
- El daño es una forma de destrucción, revelación o modificación de datos.
- Frecuentemente aprovecha una vulnerabilidad

Tecnológico de Monterrey

La amenaza

- Fuentes de la amenaza
  - Naturales
  - Ambientales
  - Humanas
    - Accidentales
    - Deliberadas
- Algunos ejemplos
  - Naturales:
    - Terremotos que destruyan el centro de cómputo.
  - Humanos
    - Fraude realizado al modificar los saldos de cuentas por cobrar.
  - Software
    - Cambios no autorizados al sistema que realicen cálculos incorrectos.

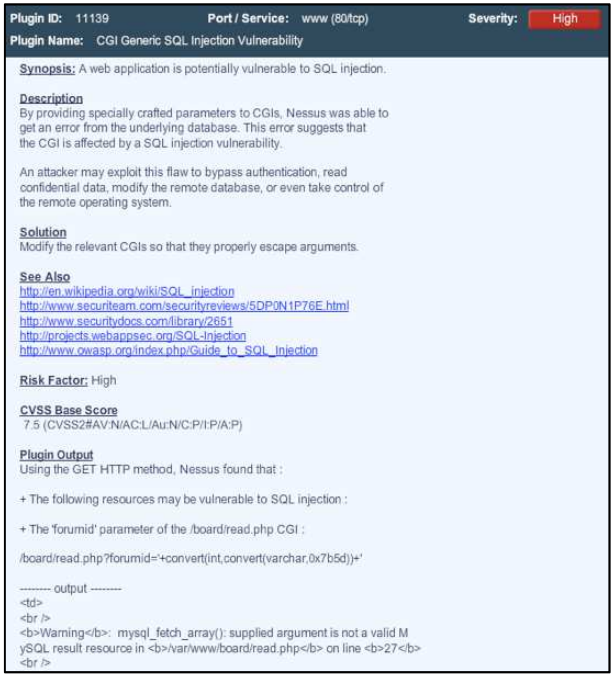
Tecnológico de Monterrey

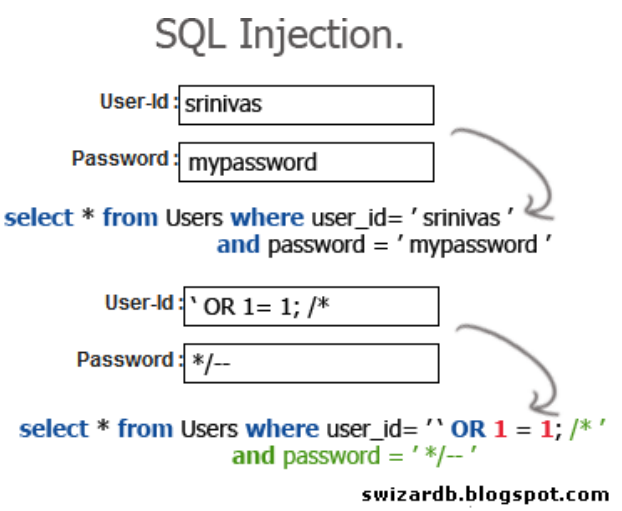
Vulnerabilidad

- Falta y/o debilidad o falla de seguridad, posibilita la materialización de una amenaza.
- Son aspectos que influyen negativamente en un activo y que posibilita la materialización de una amenaza.
- Indica que el activo es susceptible a recibir un daño a través de un ataque.
- La debilidad puede originarse en el diseño, la implementación o en los procedimientos para operar y administrar el sistema.
- En el argot de la seguridad computacional una vulnerabilidad también es conocida como un *hoyo*.

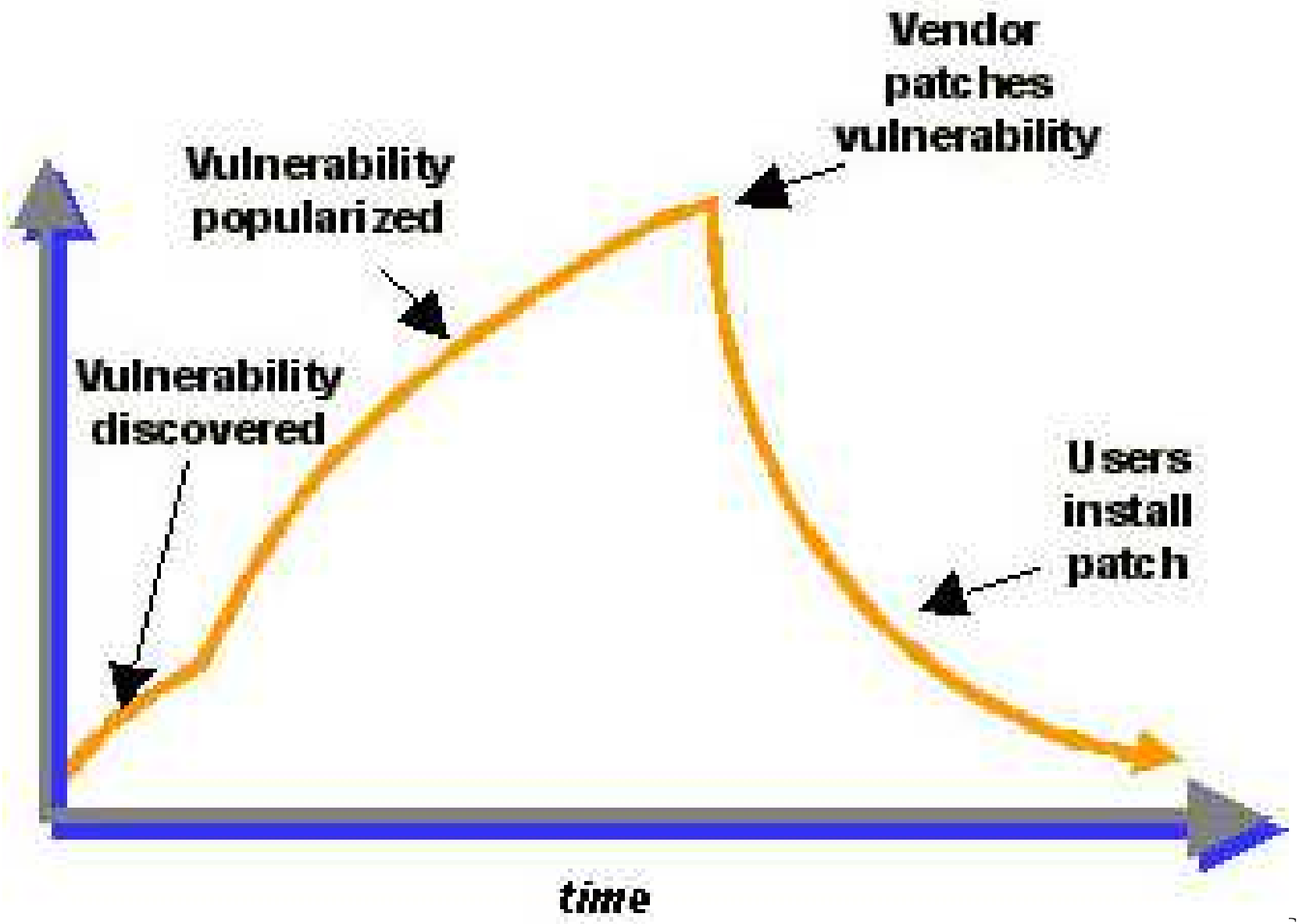
Ejemplos vulnerabilidades

- Cuentas de usuarios sin contraseña.
- El personal externo no registra su entrada y salida a las instalaciones.
- Falta de lineamientos para la construcción de contraseñas.
- No contar con un plan de recuperación de desastres.
- Un programa que no valida los datos que introduce un usuario.





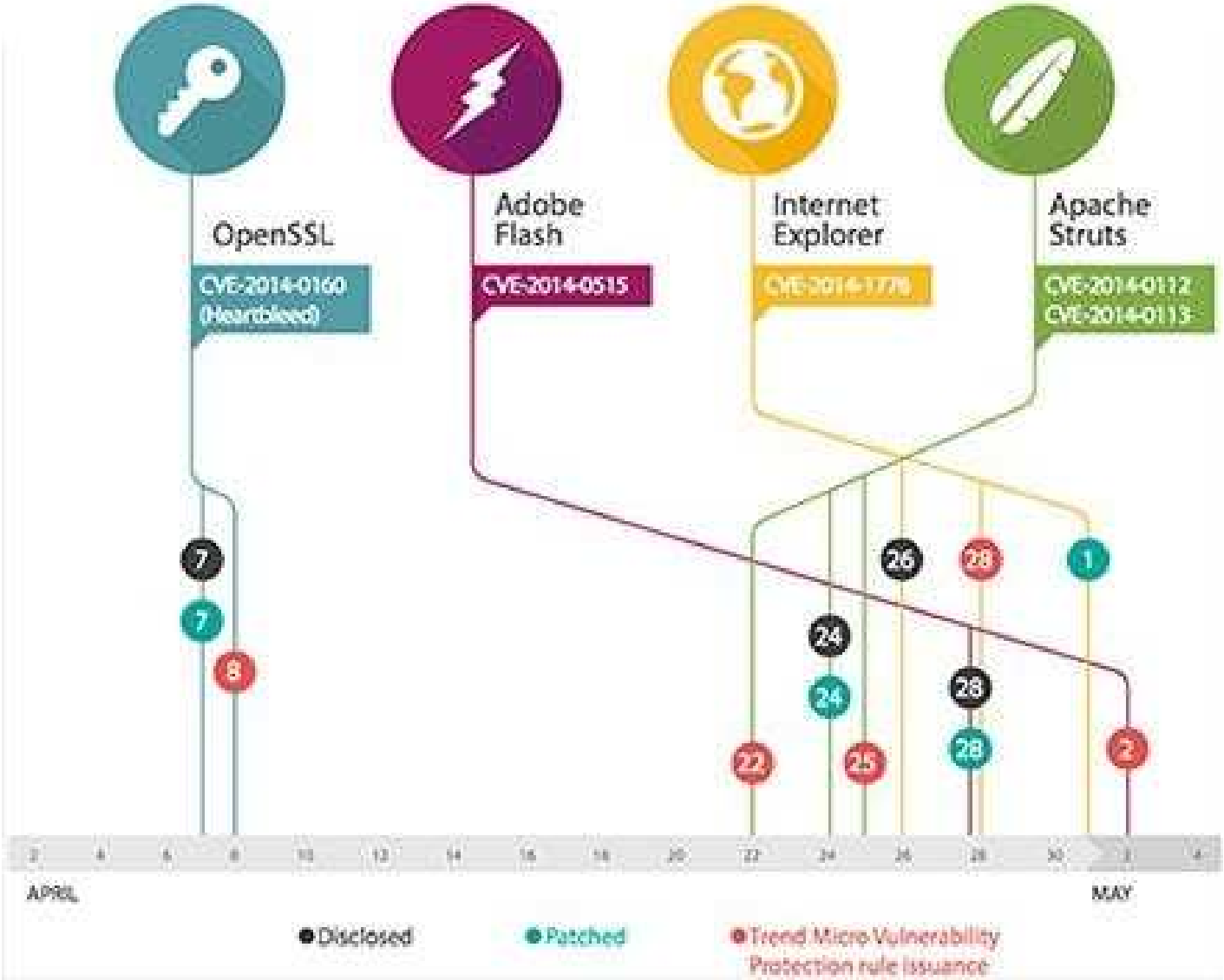
Tiempo vida vulnerabilidad



Common Vulnerabilities and Exposures: CVE

- Diccionario de nombres comunes (identificadores CVE) de vulnerabilidades conocidas públicamente.
- CCE: Commun Configuration Enumeration proporciona identificadores para aspectos de configuraciones de seguridad.
- Página: cve.mitre.org
- Otras referencias:
  - National Vulnerability Database
  - Open Source Vulnerability Database CERT Coordination Center of Vulnerability Database
  - Security Focus web site
  - Secunia
  - IBM X-Force Vulnerability Database
  - Scip VulDB

Línea tiempo de vulnerabilidades críticas, 2Q 2014



Tecnológico de Monterrey

El exploit

- Se refiere a la forma de explotar una vulnerabilidad
  - termino muy enfocado a herramientas de ataque, sobre equipos de computo).
- Aprovechamiento automático de una vulnerabilidad
  - generalmente en forma de un programa/software que realiza de forma automática un ataque aprovechandose de una vulnerabilidad

Bases de datos

- The Exploit Database
- Metasploit Auxiliary Module & Exploit Database (DB)
- Packetstorm
- 1337day
- Secunia

Venta exploits

New Java Security Flaw Uncovere Exploit on Sale for $5,000

By DAVID GILBERT: Subscribe to David's RSS feed
January 16, 2013 5:09 PM GMT

Only days after the last security flaw was patched by Oracle, a zero-day vulnerability has been found and put up for sale for $

Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits

8 comments, 5 called-out + Comment Now + Follow Comments

This story accompanies a profile of the French exploit-selling firm Vupen in the April 9th issue of Forbes magazine.

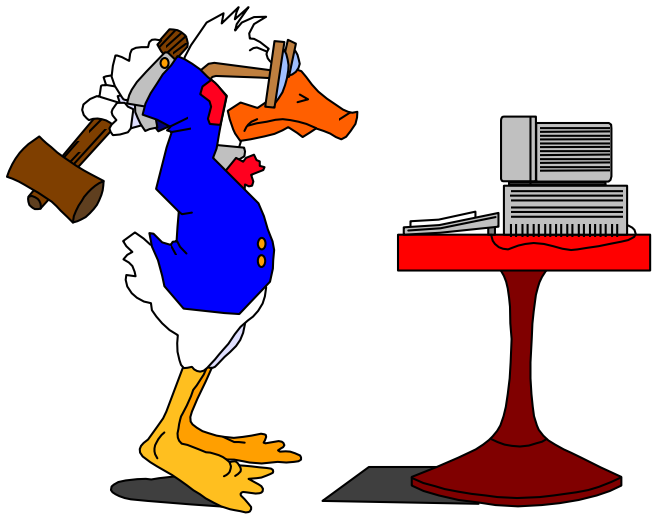
A clever hacker today has to make tough choices. Find a previously unknown method for dismantling the defenses of a device like an iPhone or iPad, for instance, and you can report it to Apple

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

Fuente: Forbes Marzo 2012

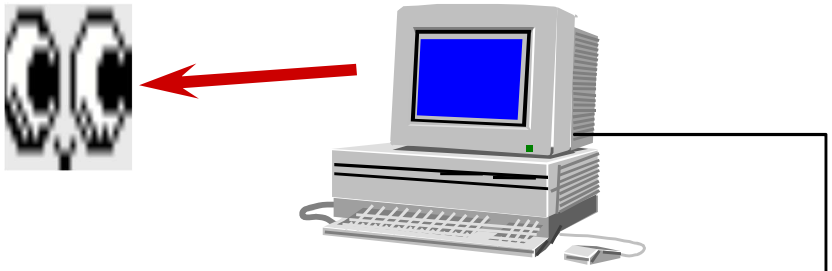
Ataque informático

- Es la consumación de una amenaza
- No es un ataque físico (aunque puede ser).
- Un ataque no se realiza en un solo paso.
- Depende de los objetivos del atacante.
- Puede consistir de varios pasos antes de llegar a su objetivo.



Tipos de Ataques (1)

Ataques Pasivos.



Ataques Activos.

Tecnológico de Monterrey

Tipos ataques activos

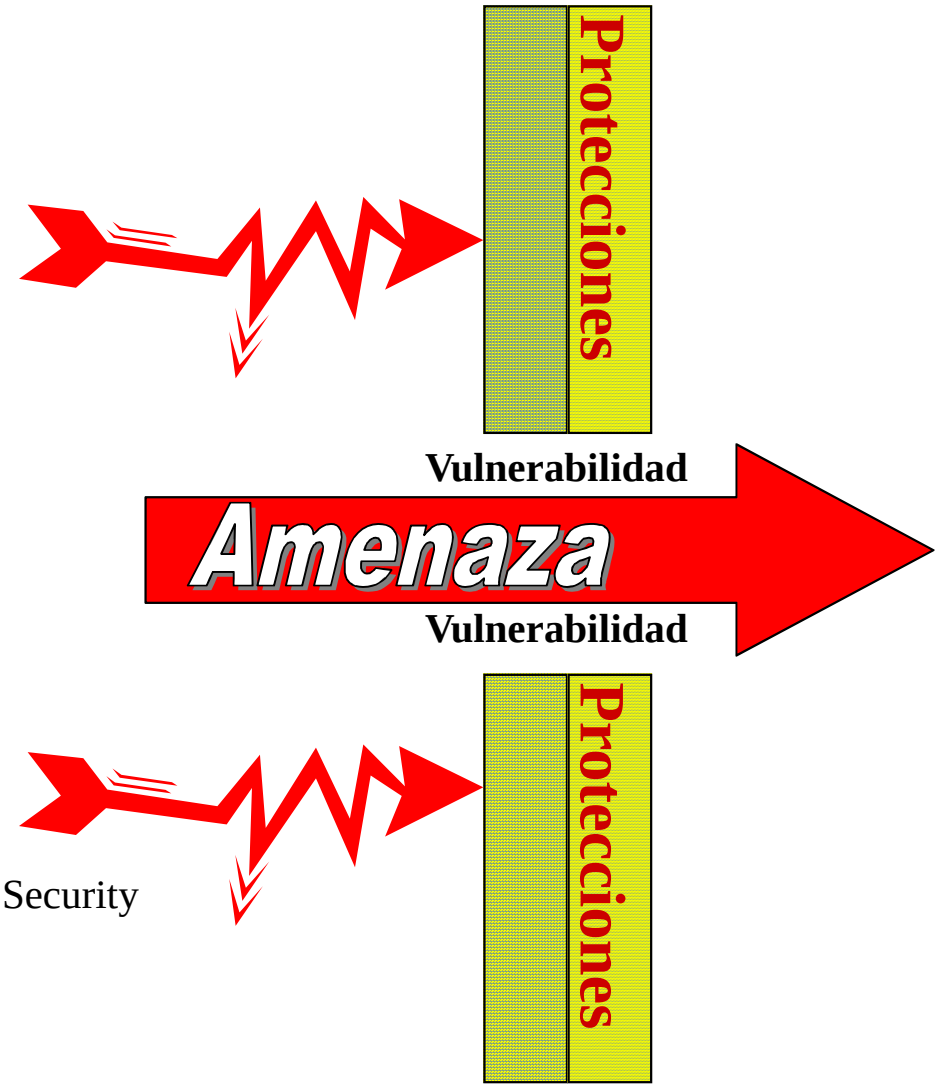
- Suplantación de identidad.
  - intruso se hace pasar por una entidad diferente, normalmente incluye alguna de las otras formas de ataque activo.
- Reactuación.
  - uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado,
- Modificación de mensajes.
  - una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados,
- Degradación del servicio.
  - impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones.

Tecnológico de Monterrey

Riesgo

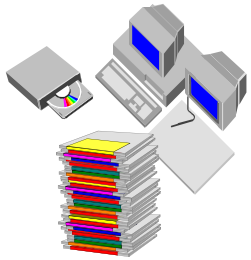
- Probabilidad / posibilidad de que un evento desfavorable ocurra.
- Tiene un impacto negativo si se materializa.
- A notar: que si no hay incertidumbre, no hay un riesgo per se.
- Ejemplos riesgos
  - Alto
  - Medio
  - Bajo
  - 327,782 USD

Vulnerabilidad vs amenaza



Activos

Datos
Instalaciones
Hardware/Software



Source:
An Introduction to Computer Security
The NIST Handbook
NIST- Serial
Publication 800-12

Tecnológico de Monterrey

Impacto

- Es la “materialización” de un riesgo.
- Una medida del grado de daño o cambio.
- Ejemplos
  - Retraso en la ejecución y conclusión de actividades de negocio.
  - Perdida de oportunidad y efectividad en la operación.
  - Falta de credibilidad frente a clientes.
  - Divulgación de información confidencial.

Tecnológico de Monterrey

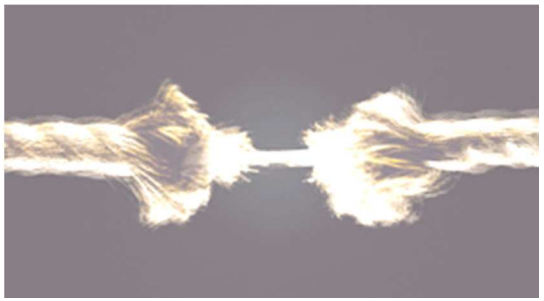
Control

- Es una medida o mecanismo para mitigar un riesgo.
- Es un mecanismo establecido para prevenir, detectar y reaccionar ante un evento de seguridad.
- Ejemplos
  - Desarrollo de políticas y procedimientos de uso de contraseñas.
  - Desarrollo e implantación de un programa de concientización.
  - Implementación de un plan de recuperación de desastres

En Resumen...

Debilidad
Control

Vulnerabilidad



Nivel de Vulnerabilidad

X

Amenaza

Riesgo

En Resumen...

Debilidad Control

No existe un procedimiento de control de cambios en Sistemas Operativos.

Vulnerabilidad

- **Falta de parches de seguridad.**
- **Huecos de seguridad por configuraciones erróneas.**

Nivel de Vulnerabilidad

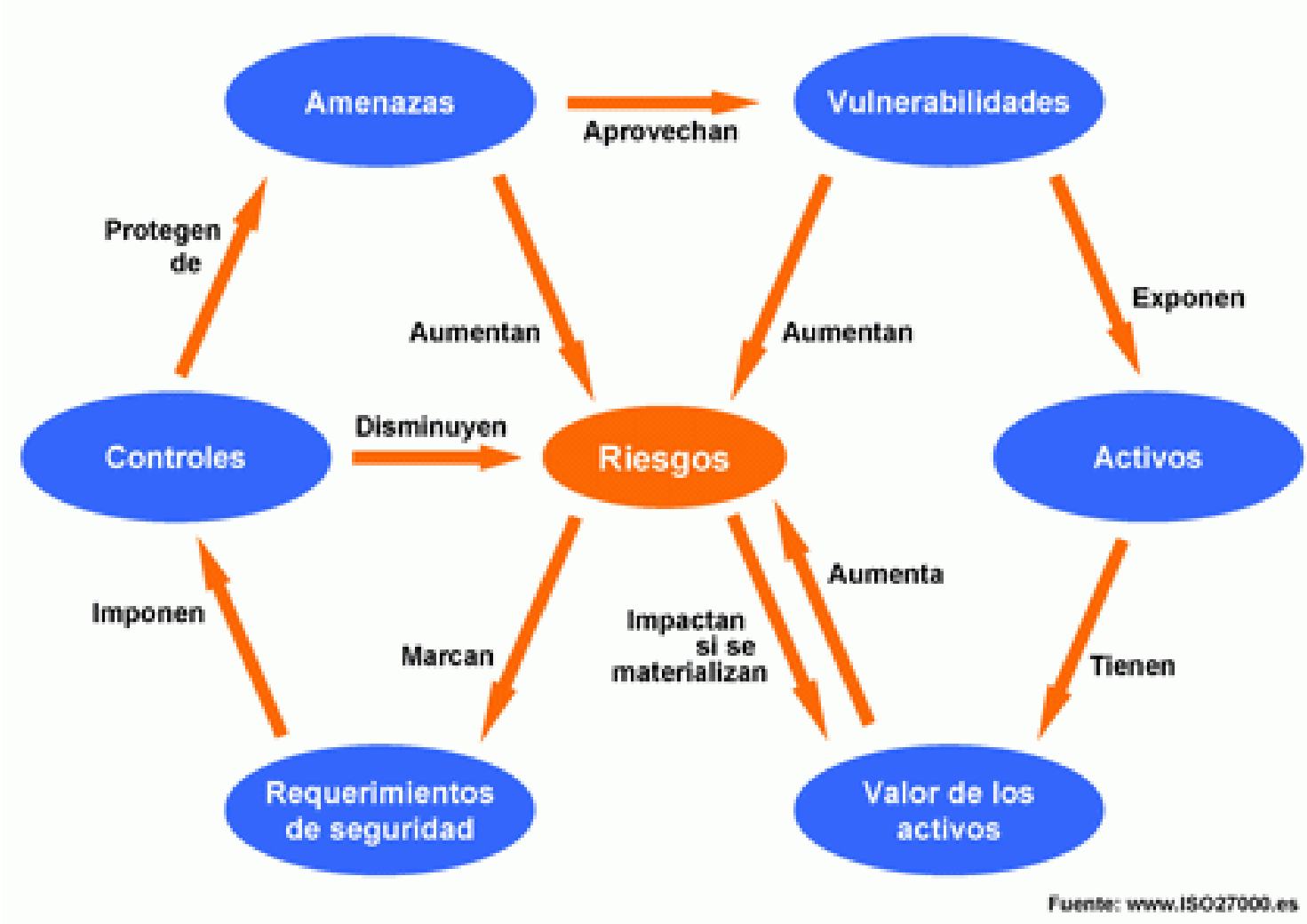
X

Amenaza

- **No ejecución del proceso de negocio.**
- **Pérdida de la confidencialidad de la información del negocio.**
- **Modificación no autorizada de la información del negocio.**

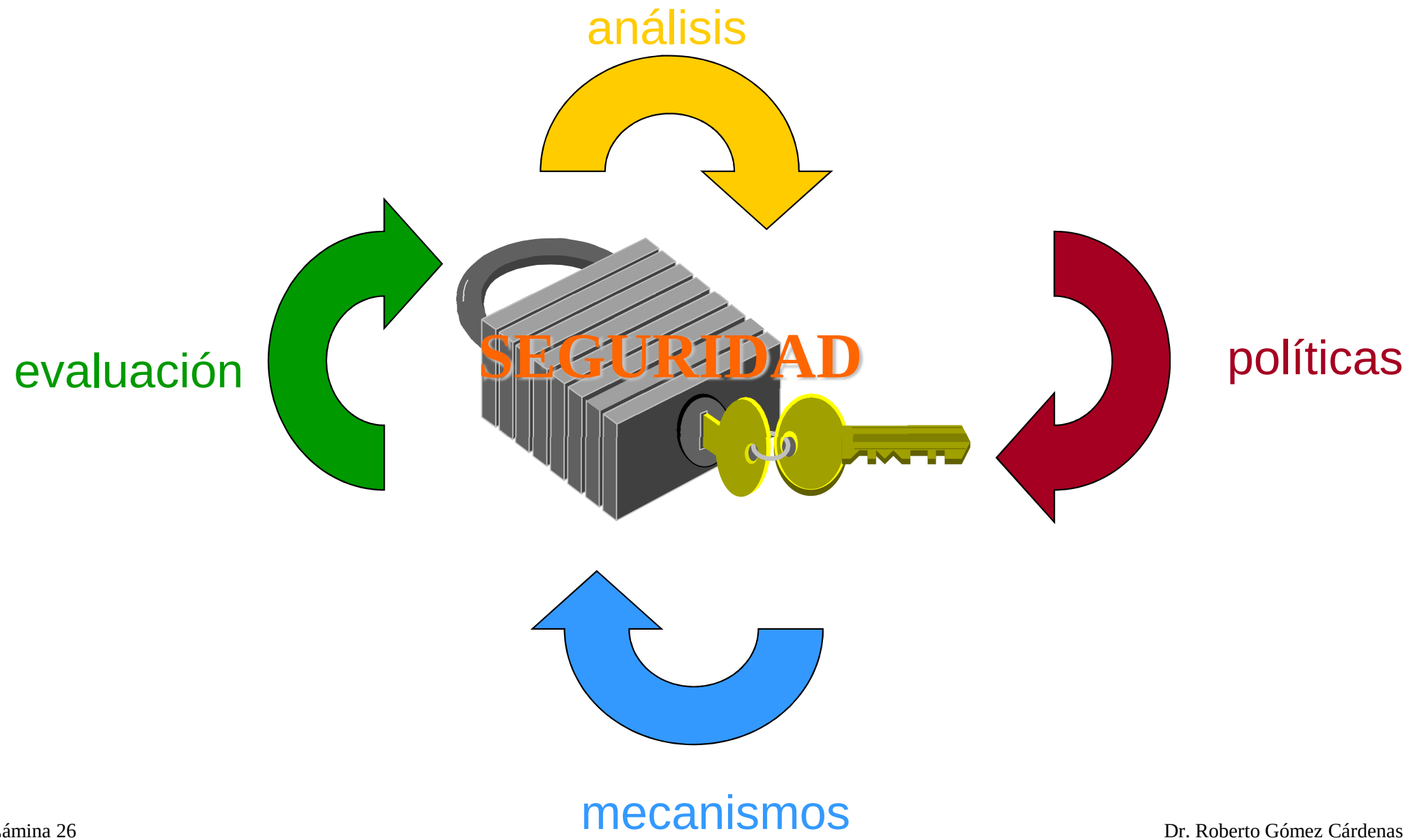
Riesgo

Interacción de todos los conceptos



Entonces, ¿de que se trata?

La estrategia es un ciclo



Tecnológico de Monterrey

Asegurando el sistema

- Objetivo
  - minimizar los riesgos potenciales de seguridad
- Análisis de riesgos
  - análisis amenazas potenciales que se pueden sufrir,
  - las pérdidas que se pueden generar
  - y la probabilidad de su ocurrencia
- Diseño política de seguridad
  - definir responsabilidades y reglas a seguir para evitar tales amenazas o
  - minimizar sus efectos en caso de que se produzcan
- Implementación
  - usar mecanismos de seguridad para implementar lo anterior

Tecnológico de Monterrey

Administración de riesgos

- Un proceso para identificar, dar prioridad y administrar los riesgos a un nivel aceptable dentro de la organización
- Responder preguntas
  - ¿Qué queremos proteger?
  - ¿Contra qué lo queremos proteger?
  - ¿Cómo lo queremos proteger?
- Dos enfoques
  - Cuantitativo
  - Cualitativo

Determinación del nivel de riesgo

- Identificar las amenazas
- Que tan probable es que ocurran
- Dos formas de evaluar probabilidad e impacto
  - Establecer la probabilidad sin considerar los controles existentes
  - Examinar el nivel de riesgo tomando en cuenta los controles existentes
  - Probabilidad: alta, media, baja

Tecnológico de Monterrey

¿Y que se hace con el riesgo?

- Etapa conocida como manejo o administración del riesgo
  - Risk Management
- Alternativas
  - Tolerar el riesgo: no se implementan controles
  - Transferir el riesgo: se transfiere el riesgo a un tercero
  - Mitigar el riesgo: se implementan controles
    - El costo de los controles debe ser analizado y evaluado detalladamente

Análisis costo/beneficio

1. Identificación costo posibles pérdidas (L)

Identificar amenazas

Se cierra el ciclo

3. Identificar posibles acciones (gasto) y sus implicaciones. (B) Seleccionar acciones a implementar.

¿ B ≤ P∗L ?

2. Determinar susceptibilidad. La probabilidad de pérdida (P)

Etapas Análisis y Evaluación de Riesgos

- Activos de información
- Identificación amenaza
- Elementos amenaza
  - Agente
  - Motivo
  - Resultado
- Determinar nivel de riesgo
  - Riesgo = Amenaza X Probabilidad Ocurrencia
- Selección del control: Análisis costo beneficio

Niveles de impacto

Nivel	Definición
Alto	La pérdida de confidencialidad, integridad o disponibilidad podría ser esperada o tener efectos severos en las operaciones organizacionales, activos o individuos. • Degradación severa o perdida de la capacidad de la misión en una extensión y duración que la organización no es capaz de realizar sus funciones primarias. • Resulta en un daño mayor para los activos de la organización. Resulta en pérdidas financieras mayores. • Resulta en daños severos o catastróficos para los individuos involucrando la perdida de la vida o serias amenazas a la vida • En corto plazo desmoviliza o desarticula a la organización
Medio	La pérdida de confidencialidad, integridad o disponibilidad podría ser esperada o tener efectos serios en las operaciones organizacionales, activos o individuos. • Degradación significativa en la capacidad de la misión en una extensión y duración que la organización es capaz de realizar sus funciones primarias, pero la efectividad es reducida. • Resulta en un daño significativo para los activos de la organización. • Resulta en pérdidas financieras significativas. • Resulta en daños significativos para los individuos pero no en la perdida de la vida o serias amenazas a esta. • Provoca la desarticulación de un componente de la organización. A largo plazo puede provocar desarticulación de la organización.
Bajo	La pérdida de confidencialidad, integridad o disponibilidad podría ser esperada o tener efectos limitados en las operaciones organizacionales, activos o individuos. • Degradación en la capacidad de la misión en una extensión y duración que la organización es capaz de realizar sus funciones primarias, pero la efectividad es reducida. • Resulta en un daño menor para los activos de la organización. • Resulta en pérdidas financieras menores. • Resulta en una exposición menor al daño. • Daño aislado, no perjudica ningún componente de la organización.

Tecnológico de Monterrey

Niveles Probabilidad

Nivel	Definición
Alto	La fuente de la amenaza está altamente motivada y tiene la capacidad suficiente, y los controles para impedir que la amenaza se ejerza son inadecuados. El ataque es inminente. No existen condiciones internas y externas que impidan el desarrollo del ataque
Medio	La fuente de la amenaza está motivada y cuenta con capacidad, pero los se cuenta con controles implementados para impedir que la amenaza se manifieste con éxito. Existen condiciones que hacen poco probable un ataque en corto plazo, pero no son suficientes para evitarlo en el largo plazo.
Bajo	La fuente de la amenaza carece de motivación o capacidad, o se cuenta con controles implementados para prevenir, o al menos significativamente impedir, que la amenaza se lleve a cabo. Existen condiciones que hacen muy lejana la posibilidad del ataque.

Matriz del nivel de riesgo

IMPACTO

PROBABILIDAD

	ALTO	MEDIO	BAJO
ALTO	Alto	Alto	Moderado Alto
MEDIO	Alto	Moderado Alto	Moderado Bajo
BAJO	Moderado Alto	Moderado Bajo	Bajo

Alto: una acción correctiva debe ser implementada
Moderado alto: una acción correctiva debería ser implementada
Moderado bajo: se requiere acciones de monitoreo
Bajo: no se requiere ninguna acción en este momento

Tecnológico de Monterrey

Ejemplos amenazas

Control	Descripción
Ice Storm	A severe weather condition characterized by falling freezing precipitation. Such a storm forms a glaze on objects, creating hazardous travel conditions and utility problems.
Earthquake	A sudden, transient motion or trembling of the earth's crust, resulting from the waves in the earth caused by faulting of the rocks or by volcanic activity.
Air pollution	The soiling of the atmosphere by contaminants to the point that injury may be caused to health, property, or plant or animal life, or the use and enjoyment of the outdoors may be prevented.
Electrical disturbance	A momentary fluctuation in the electrical power source, consisting of a voltage surge (peak), voltage dip, or interruptions of less than a half hour.
Emanation	A long-term disruption in the electrical power source, usually greater than a half hour.
Alteration of data	An accidental modification, insertion, or deletion of data or information stored on the system.
Alteration of software	The accidental modification, insertion, or deletion of operating system or application system programs or portions of code supporting the production systems.
Disclosure	The accidental release or proprietary, classified, company confidential, personal, or otherwise sensitive information.
Operator/user error	An accidental, improper, or otherwise illchosen act by an employee that results in processing delays, equipment damage, lost data, or modified data.
Theft	The unauthorized appropriation of hardware, software, media, computer supplies, or data of a classified nature, but included in the disclosure category.
Unauthorized use	An unauthorized use of computer equipment or programs. Examples of this include the running of personal programs such as games, inventories, and browsing other files.
Vandalism	The malicious and motiveless destruction or defacement of property..
Strike	An organized employee action (union or not, legal or not) designed to halt or disrupt normal business operations. Strikes can be categorized as unfair labor practice, economic, or unprotected strikes.

Tecnológico de Monterrey

Ejemplos controles

Amenaza	Definición
Backup	Backup requirements will be determined and communicated to operations, including a request that an electronic notification be sent to the application system administrator stating that backups were completed. Operations will be requested to test the backup procedures.
Recovery Plan	Develop, document, and test recovery procedures designed to ensure that the application and information can be recovered, using the backups created, in the event of loss.
Risk Analysis	Conduct a risk analysis to determine the level of exposure to identified threats and identify possible safeguards or controls.
Accounting of assets	Establish an inventory of major assets associated with each information system.
Information classification	Implement standards for security classification and the level of protection required for information assets.
Secure areas	Implement standards to ensure that physical security protections exist, based on defined perimeters through strategically located barriers throughout the organization.
Equipment security	Implement standards to ensure that equipment is located properly to reduce risks of environmental hazards and unauthorized access.
Network management	Implement appropriate standards to ensure the security of data in networks and the protection of connected services from unauthorized access.
Media handling and security	Implement procedures for the management of removable computer media such as tapes, disks, cassettes, and printed reports.
Cryptography	Implement policies and standards on the use of cryptographic controls, including management of encryption keys, and effective implementation.
Security of system files	Implement standards to exercise strict control over the implementation of software on operational systems.

Tecnológico de Monterrey

Política de Seguridad

- Especifica las características de seguridad que un sistema debe observar y proveer
  - conjunto de reglas que deben respetarse para mantener la seguridad de la información.
- Especifica las amenazas contra las que la organización debe protegerse y cómo debe protegerse
- Depende de los objetivos y metas de la organización.
- Generalmente es expresada en un lenguaje o idioma.
- Típicamente establecida en términos de *sujetos* y *objetos*.

Tecnológico de Monterrey

Objetos y Sujetos

- Un objeto es todo recurso “pasivo” del sistema. Por ejemplo, la información, un archivo, el código de un programa, un dispositivo de red, etc.

- Un sujeto es toda entidad “activa” en el sistema. Por ejemplo, un usuario, un programa en ejecución, un proceso, etc.

Tecnológico de Monterrey

Paradigmas

- *Paranoico*: Nada está permitido.
- *Prudente:* Lo que no está expresamente permitido, está prohibido.
- *Permisivo*: Lo que no está expresamente prohibido, está permitido.
- *Promiscuo:* Todo está permitido.

Tecnológico de Monterrey

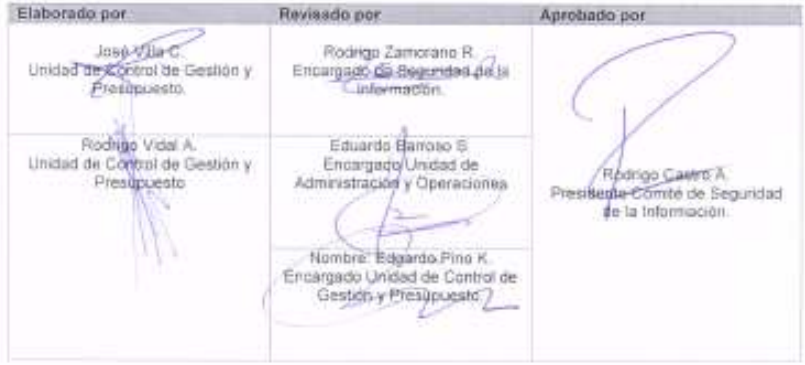
Tipos políticas de seguridad

- Políticas administrativas
  - Procedimientos administrativos.
- Políticas de control de acceso
  - Privilegios de acceso del usuario o programa.
  - Política de menor privilegio
- Políticas de flujo de información
  - Normas bajo la cuales se comunican los sujetos dentro del sistema.
  - La información a la que se accede, se envía y recibe por:
    - ¿Canales claros o canales ocultos? ¿Seguros o no?
  - ¿Qué es lo que hay que potenciar?
    - ¿La confidencialidad o la integridad?
    - ¿La disponibilidad?

Elementos Política Seguridad

- Portada
- Índice
- Sección de firmas
- Objetivo
- Antecedentes
- Alcance
- Marco Legal
- Definiciones
- Políticas
- Anexos

	MANUAL DE NORMAS Y PROCEDIMIENTOS DE SEGURIDAD	VERSION	1.0
		FECHA	09/06/2012
		Departamento de Soporte Técnico	



INVENTARIO DE FORMATOS

No.	Nombre y Clave	Responsable del resguardo	Tiempo mínimo de resguardo	Disposición final
1.				
2.				
3.				
4.				

VERSIONES DEL DOCUMENTO

El presente documento ha tenido las siguientes versiones con sus correspondientes cambios.

VERSIÓN	RAZÓN DE LOS CAMBIOS	FECHA DE ACTUALIZACIÓN	SUSTITUYE A:

Tecnológico de Monterrey

Ejemplo de Política (en lenguaje natural)

- Sólo se permitirá el intercambio de correo electrónico con redes de confianza.
- Toda adquisición de software a través de la red debe ser autorizada por el administrador de seguridad.
- Debe impedirse la inicialización de los equipos mediante disco.

Ejemplo politica (1)

5. Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, la Dirección de Telemática tiene la facultad de acceder a cualquier equipo de cómputo que no esten bajo su supervisión.

Del control de acceso local a la red.

1. El departamento de Cómputo de la Dirección de Telemática es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.
2. La Dirección de Telemática es la responsable de difundir el reglamento para el uso de la red y de procurar su cumplimiento.
3. Dado el carácter unipersonal del acceso a la Red-CICESE, el departamento de Cómputo verificará el uso responsable, de acuerdo al Reglamento para el uso de la red.
4. El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, bases de datos, equipo de supercómputo centralizado y distribuido, etc.) conectado a la red es administrado por el departamento de Cómputo.
5. Todo el equipo de cómputo que esté o sea conectado a la Red-CICESE, o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe de sujetarse a los procedimientos de acceso que emite el departamento de Cómputo.

De control de acceso remoto.

1. La Dirección de Telemática es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.
2. Para el caso especial de los recursos de supercómputo a terceros deberán ser autorizados por la Dirección General o por la Dirección de Vinculación.
3. El usuario de estos servicios deberá sujetarse al Reglamento de uso de la **Red-CICESE** y en concordancia con los lineamientos generales de uso de Internet.
4. El acceso remoto que realicen personas ajenas a la institución deberá cumplir las normas que emite la Dirección de Telemática.

De acceso a los sistemas administrativos.

1. Tendrá acceso a los sistemas administrativos solo el personal del CICESE que es titular de una cuenta de gastos o bien tenga la autorización del responsable si se trata de personal de apoyo administrativo o técnico.

Ejemplo política 2

Acceso a Internet

El internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias del negocio de ICETEX, por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

a) No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.
- El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN Messenger, Yahoo, Skype, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de ICETEX.
- El intercambio no autorizado de información de propiedad de ICETEX, de sus clientes y/o de sus funcionarios, con terceros.
- La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el Jefe respectivo y la Dirección de Tecnología, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

b) ICETEX debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación nacional vigente.

c) Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

d) Los funcionarios y terceros, al igual que los empleados o subcontratistas de estos, no pueden asumir en nombre de ICETEX, posiciones personales en encuestas de opinión, foros u otros medios similares.

Tecnológico de Monterrey

Procedimientos

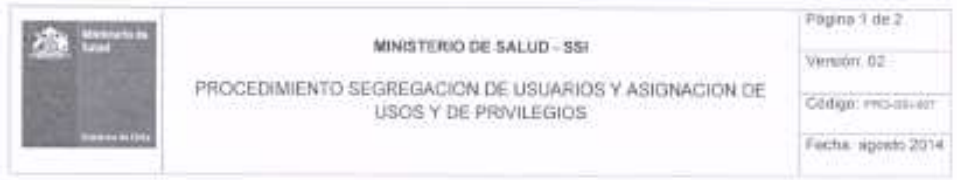
- Son la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas.

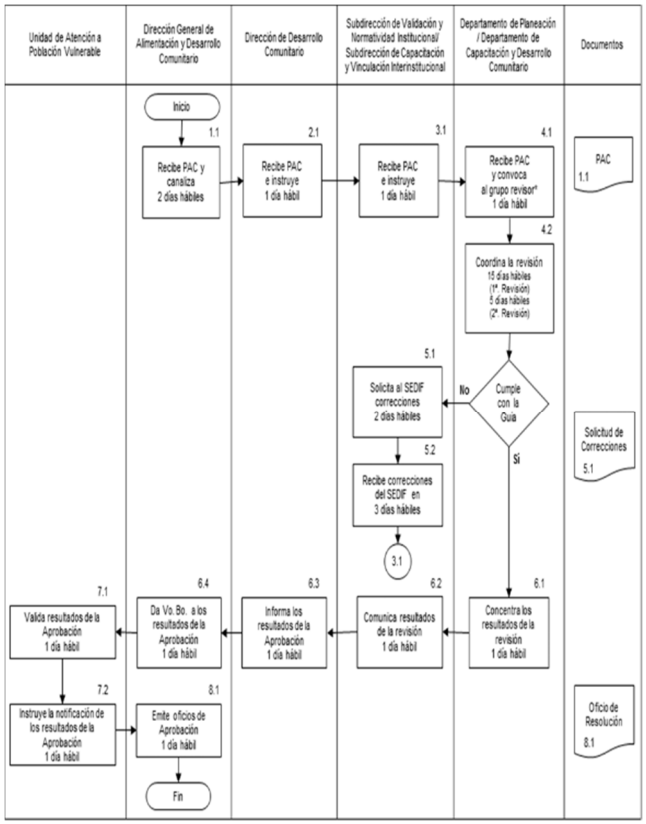
- Los Procedimientos de Seguridad permiten aplicar e implantar las Políticas de Seguridad que han sido aprobadas por la organización.

- Las Políticas definen "qué" se debe proteger en el sistema, mientras que los Procedimientos de Seguridad describen "cómo" se debe conseguir dicha protección

Elementos procedimiento

- Portada
- Índice
- Sección de firmas
- Objetivo
- Antecedentes
- Alcance
- Marco Legal
- Definiciones
- Procedimiento (nombre)
  - Diagramas De Flujo.
  - Procedimiento (el nombre del procedimiento y la descripción en palabras de este)
- Anexos



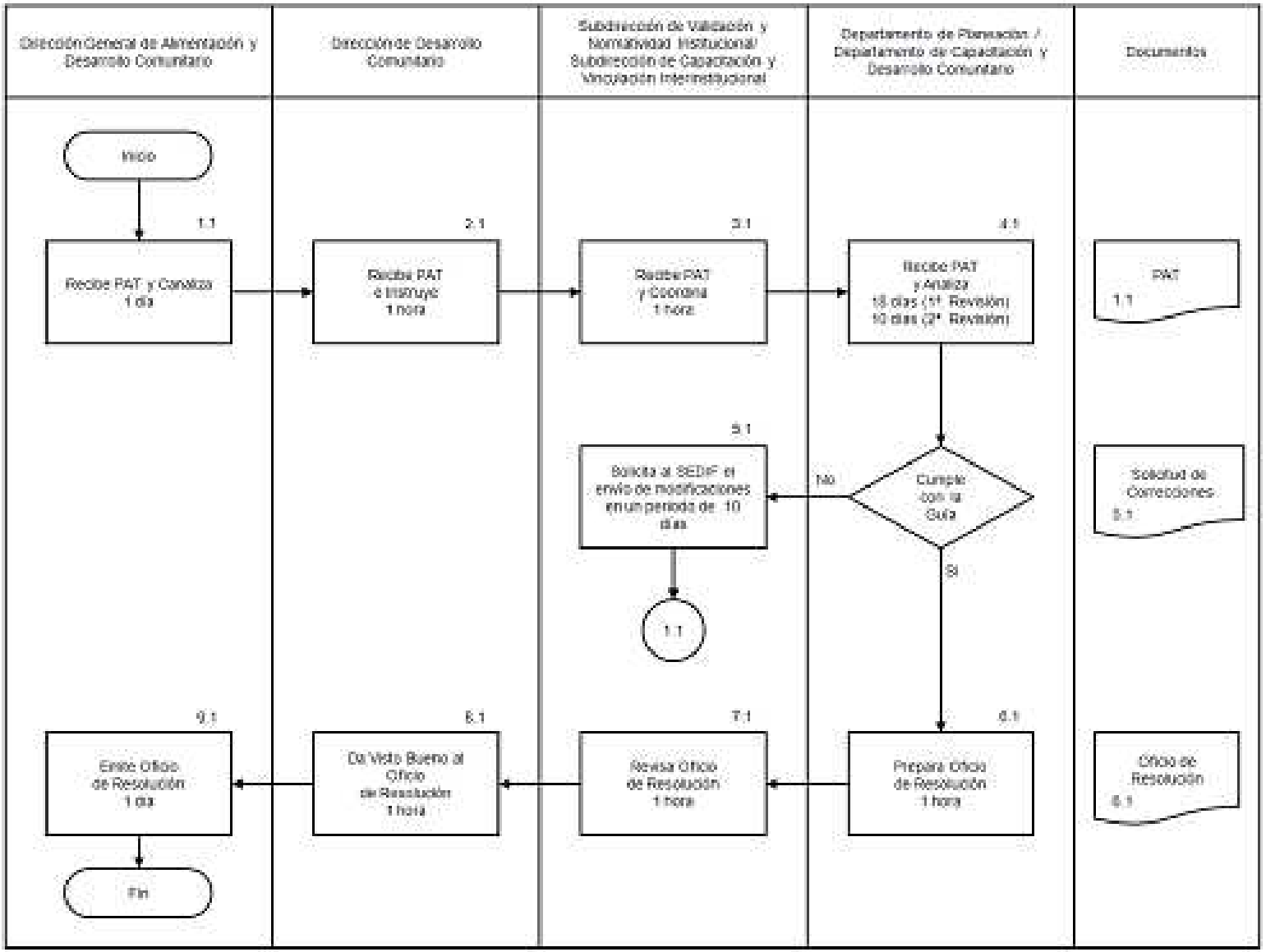


Procedimiento nº	Versión	Autor	Fecha Aprobación	Fecha última Actualización
2012/000 IGAE		ACS		marzo-2013

Ejemplo procedimiento

Usuario solicitante	1. Requisita solicitud de alta, baja o cambios de usuario SIAC y entrega a la Gerencia de Sistemas Integrales	Solicitud
Gerencia de Sistemas Integrales	2. Recibe solicitud, revisa y asigna el tipo de licencia a utilizar por el usuario SIAC, remite a la Subgerencia de Centro de Cómputo.	Solicitud
Subgerencia de Centro de Cómputo	3. Recibe solicitud, revisa códigos de transacciones y roles, determina: **¿Esta correcta la información?**	Solicitud
	No	
	4. Devuelve solicitud con las observaciones correspondientes. **(Regresa a la actividad 2)**	Solicitud
	Si	
	5. Verifica el movimiento solicitado y procede según el tipo de solicitud:	
	Alta **(Continúa en la actividad 8)**	
	Cambio **(Continúa en la actividad 10)**	
	Baja	
	6. Verifica en sistema si el servidor público que exista cuenta con el perfil de usuario de SIAC.	
	7. Realiza el movimiento de baja de usuario del sistema SIAC **Fin**	

Diagrama flujo procedimiento



Acuerdos de Nivel de Servicio

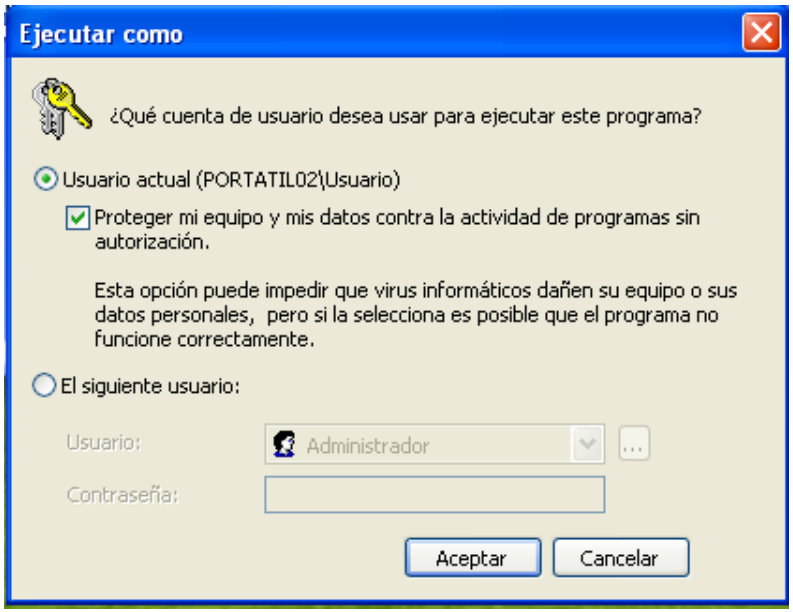
- Documento en el que se estipulan los niveles de un servicio en función de una serie de parámetros objetivos, establecidos de mutuo acuerdo entre ambas partes, así, refleja contractualmente el nivel operativo de funcionamiento, penalizaciones por caída de servicio, limitación de responsabilidad por no servicio, etc....
- No ha de estar relacionado necesariamente con la contratación de servicios a terceras partes, sino que puede implantarse a nivel interno, transformando una determinada unidad de negocio en centro de servicios que provea a la propia compañía
- Ejemplo:
  - http://edu.jccm.es/joomla15/index.php/sobre-joomla/informacion-general/81-acuerdo-de-nivel-de-servicio-sla.html

Propietarios, custodio y usuario

- Propietario
  - Responsable por definir los niveles y estrategias de protección de la información.
- Custodio
  - Responsable por el cumplimiento de las directrices de uso y acceso a la información. Así como conocer y participar en las estrategias de contingencia y recuperación de la misma
- Usuario
  - Responsable por hacer un uso adecuado y tener acceso autorizado a la información.

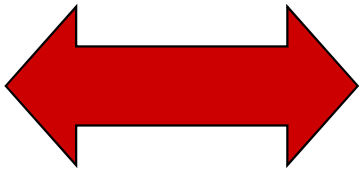
El concepto de mínimo privilegio

- Se deben otorgar los permisos estrictamente necesarios para efectuar las acciones que se requieran, ni más ni menos de lo solicitado.
- Ventajas:
  - Evita que un usuario con los mínimos privilegios intente sabotear el sistema de forma intencionada o bien al no estar bien informado de manera inintencionada



Mecanismos de seguridad

- Son la parte más visible de un sistema de seguridad.
- Se convierten en la herramienta básica para garantizar la protección de los sistemas o de la propia red.
- Se dividen en:
  - prevención
  - detección
  - recuperación



Estrategias de protección
- Evitación
- Prevención
- Detección
- Recuperación

Evitación

- No exponer activos a amenazas.
- Organizar las tareas de modo de evitar amenazas.
- Definición y uso de áreas y/o equipos restringidos o aislados.

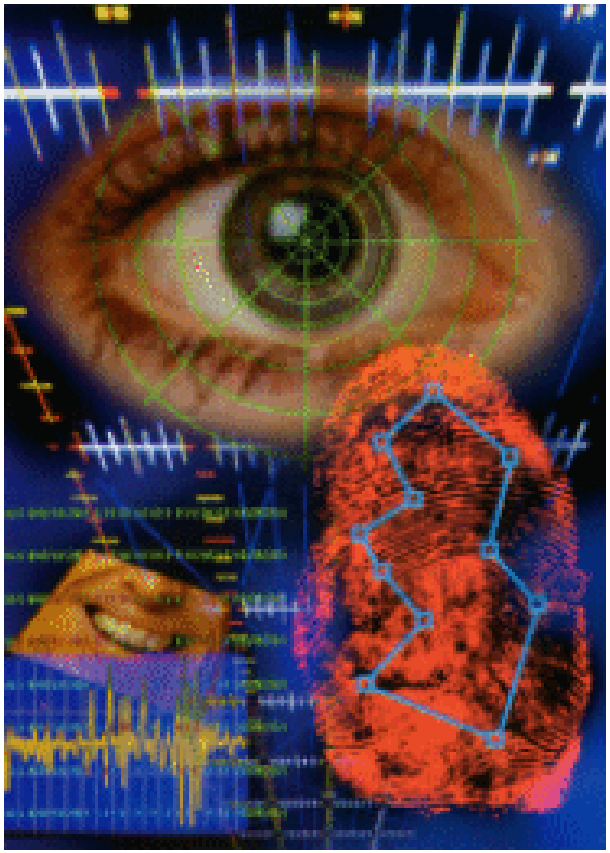
Prevención

- Incluye funciones de seguridad en hardware y software.
- Debe incluir la definición y observancia de políticas de seguridad.
- Incluye controles administrativos.
- Es la estrategia más ampliamente usada.

Tecnológico de Monterrey

Mecanismos prevención

- Aumentan la seguridad de un sistema durante el funcionamiento normal de éste.
- Previenen la ocurrencia de violaciones a la seguridad
- Ejemplos mecanismos:
  - encripción durante la transmisión de datos
  - passwords difíciles
  - firewalls
  - biométricos



Mecanismos prevención más habituales

- Mecanismos de autenticación
- Mecanismos de control de acceso
- Mecanismos de separación
- Mecanismos de seguridad en las comunicaciones

Tecnológico de Monterrey

Mecanismos autenticación

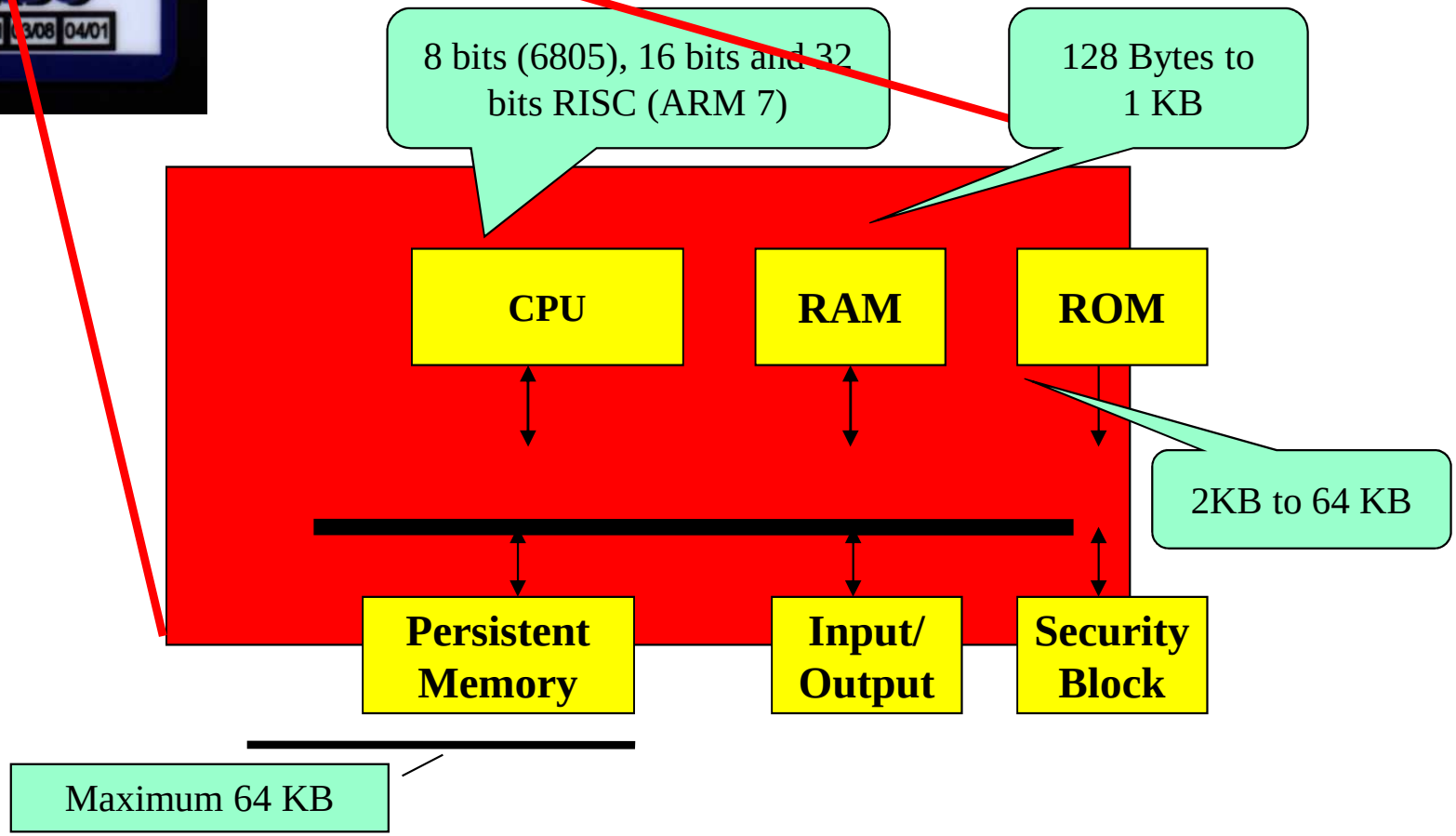
- Clasificación
  - Basados en algo que se sabe
  - Basados en algo que se es
  - Basadas en algo que se tiene
- Posible combinar los métodos
  - autenticación de dos factores
    - basado en algo que se sabe y algo que se es
    - basado en algo que se sabe y algo que se tiene
    - basado en algo que se es y algo que se tiene
    - basado en algo que se es y algo que se sabe
    - otras combinaciones
  - autenticación de tres factores
    - basado en algo que se es, algo se sabe y algo que se tiene

Tecnológico de Monterrey

Basados en algo que se tiene

- Usar un objeto físico que llevan consigo y que de alguna forma comprueba la identidad del portador.
- Las tarjetas de acceso son las prendas típicas
- Cada tarjeta tiene un número único.
- El sistema tiene una lista de las tarjetas autorizadas.

Arquitectura Tarjeta Inteligente



Tecnológico de Monterrey

Problemas de este mecanismo

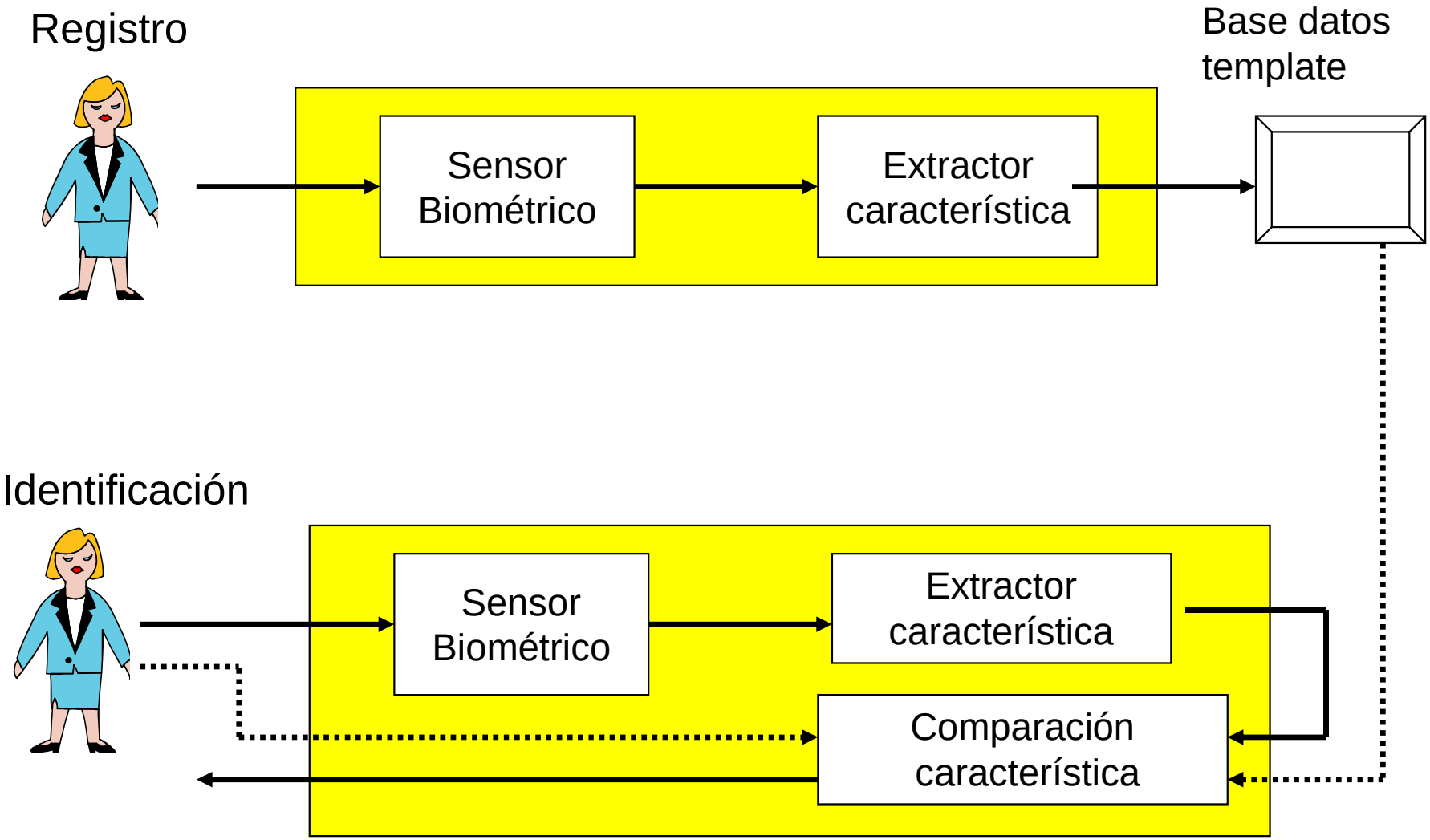
- El objeto no prueba quien es la persona.
  - Cualquiera que tenga la tarjeta puede entrar al área restringida.
- Si una persona pierde su objeto no podra entrar al área restringida aunque no haya cambiado su identidad.
- Algunas prendas pueden ser copiadas o falsificadas con facilidad.

Tecnológico de Monterrey

Basados en algo que se es

- Se realiza una medición física y se compara con un perfil almacenado con anterioridad,
  - técnica conocida como biométrica,
  - se basa en la medición de algún rasgo de una persona viva.
- Existen dos formas para usar biometricos:
  - comparar las medidas de un individuo con un perfil específico almacenado.
  - buscar un perfil en particular en una gran base de datos.

El proceso biométrico



Tecnológico de Monterrey

Características biométrico ideal

- Universal
  - toda persona posee la característica
- Único
  - dos personas no comparten la característica
- Permanente
  - la característica no debe cambiar o alterarse
- Colectable (collectable)
  - característica es realmente presentable a un sensor y es fácilmente cuantificable.

Tecnológico de Monterrey

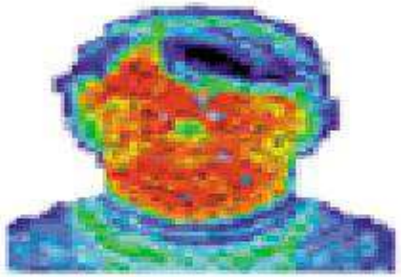
Sistemas biométricos prácticos

- Desempeño
  - robustez, requerimientos de recursos, y factores operacionales o de ambiente que afectan su confiabilidad y velocidad
- Aceptación
  - personas dispuestas a aceptar un identificador biométrico en su vida diaria.
- Confiablidad
  - que tan fácil es engañar al sistema, a través de métodos fraudulentos

Tecnologías Biométricas

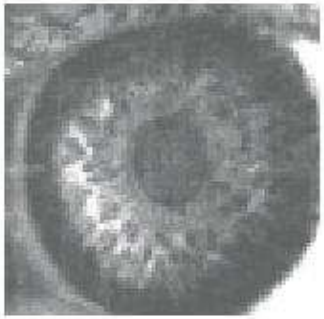
- Imágenes faciales
- Geometría mano
- Métodos basados en el ojo
- Firmas
- Voz
- Geometría de la vena
- Imágenes palma y dedos


face


facial thermogram

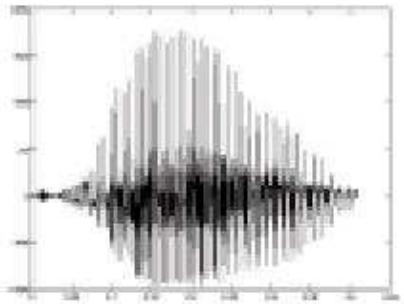

fingerprint


hand geometry

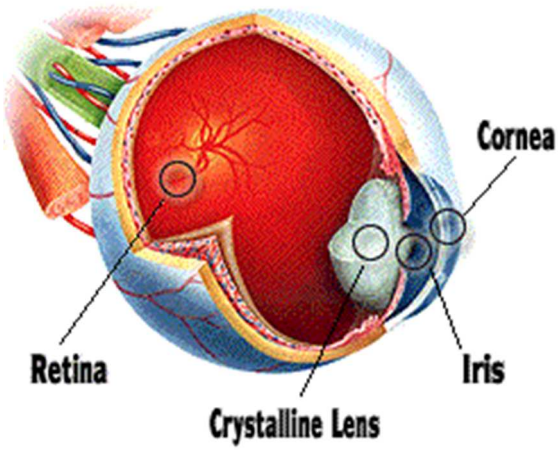

iris

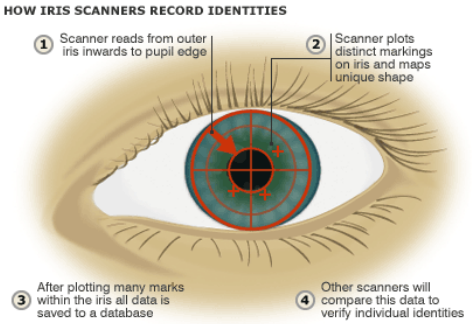

retinal scan

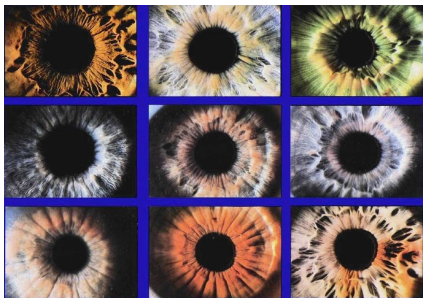

signature

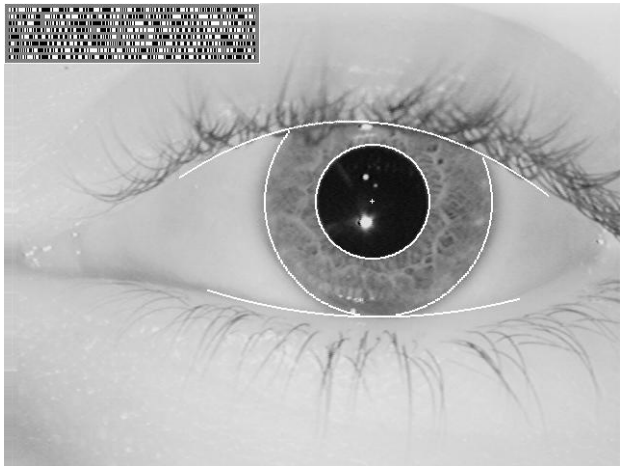

voice print

Retina y huella

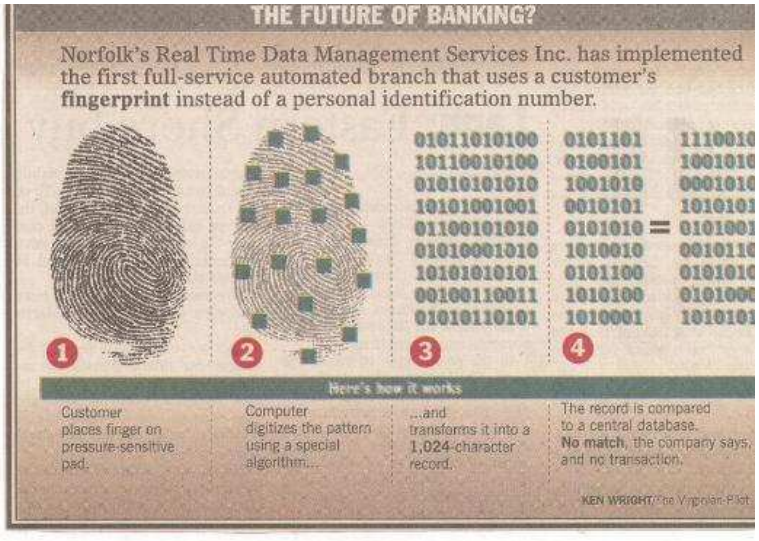


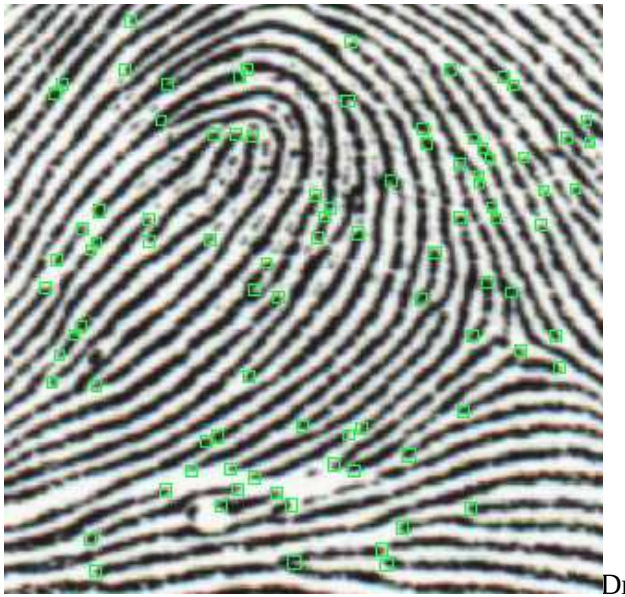






http://news.bbc.co.uk/nol/shared/spl/hi/guides/45690





Tecnológico de Monterrey

Ejemplo 1

Tecnológico de Monterrey

Ejemplo 2

Tecnológico de Monterrey

Comparación

Biometrico	Universal	Unico	Permanente	Colectable	Desempeño	Aceptación	Confiabilidad
Cara	alta	baja	media	alta	baja	baja	bajo
Huella digital	media	alta	alta	media	alta	media	alto
Gometria Mano	media	media	media	alta	media	media	media
Iris	alta	alta	alta	media	alta	baja	alta
Scan retina	alta	alta	media	baja	alta	baja	alta
Firma	baja	baja	baja	alta	baja	alta	baja
Impresión voz	media	baja	baja	media	baja	alta	baja
F. Termográfico	alta	alta	baja	alta	media	alta	alta

Tecnológico de Monterrey

Basados en algo que se sabe

- Primeros sistemas de autenticación se basaron en claves de acceso: nombre usuario y una clave de acceso.
- Son fáciles de usar y no requieren de un hardware especial.
- Siguen siendo el sistema de autenticación más usado hoy en día.
- Passwords, frases y números de identificación personal, NIP.

Tecnológico de Monterrey

El password

- Primera barrera contra ataques.
- El password es la parte más sensible de la seguridad en Unix.
- Es posible tener un sistema donde se ha tenido mucho cuidado del aspecto de seguridad y, sin embargo, que es vulnerable debido a passwords mal elegidos por los usuarios.

Probabilidad de descifrar un password

EL NCSC en 1985 definió la probabilidad de descifrar un password como:

$$P = (LxR) / S$$

L = tiempo de vida del password

R = es el número de intentos por unidad de tiempo que es posible realizar para descifrar un password.

S= es el espacio de passwords; el número total de passwords únicos disponibles, donde:

Espacio de passwords

$$S = A^{M}$$

A = el número total de caracteres en el alfabeto

M= longitud el password

Tecnológico de Monterrey

Aspectos a cuidar en la selección de un password

- No use el nombre del login en ninguna forma
- No use nombres propios, apellidos o sobrenombres.
- No use el nombre de familiares o amigos.
- No use palabras contenidas en diccionarios
- No use información relacionada con usted
- No use únicamente dígitos o la misma letra
- No use menos de siete caracteres

Tecnológico de Monterrey

Consejos para la selección de passwords

- Use mayúsculas y minúsculas
- Use dígitos y signos de puntuación.
- Use un password fácil de recordar para evitar escribirlo
- Use un password que pueda teclear rápido y sin mirar al teclado.
- Use passwords derivados de frases célebres:

  p.e: El respeto al derecho ajeno es la paz, deriva en ERADAELP

Tipos de contraseñas con respecto a la aplicación

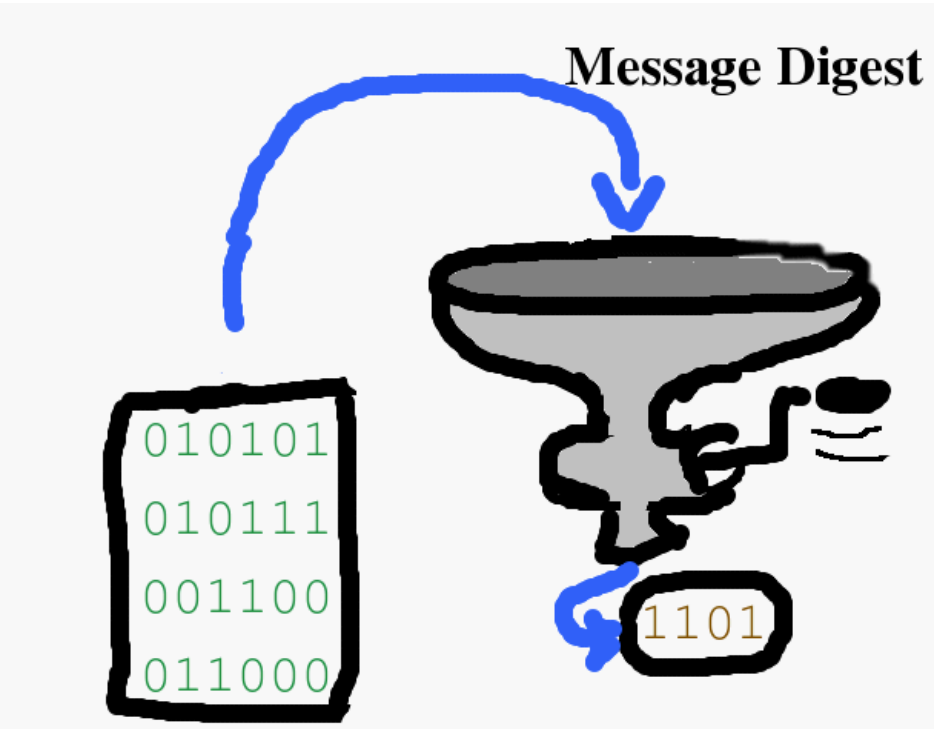
- Passwords de aplicaciones
  - ARJ, ZIP, RAR, etc
  - Micosoft Office passwords
  - Documentos PDF
- Sistemas Operativos
  - Windows
  - Unix

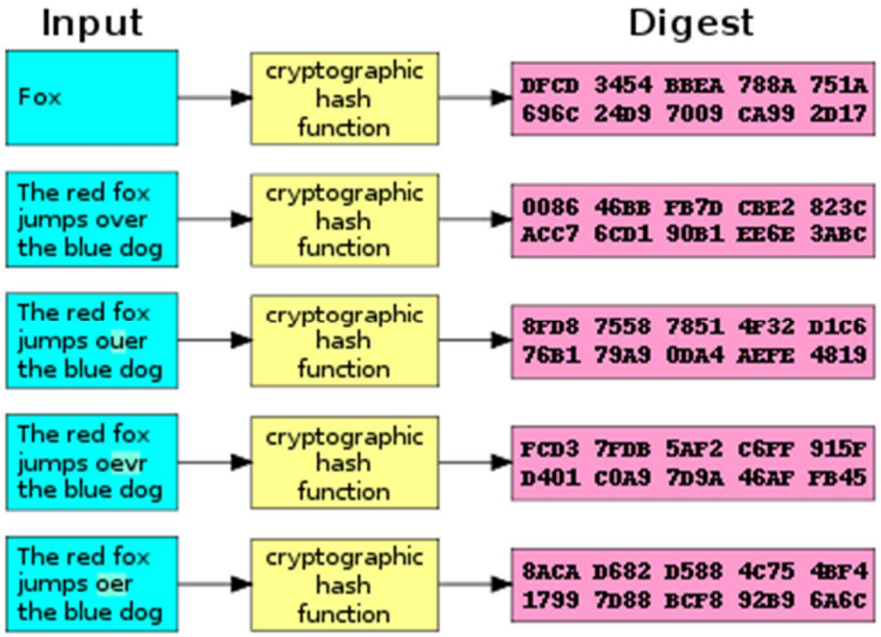
Tecnológico de Monterrey

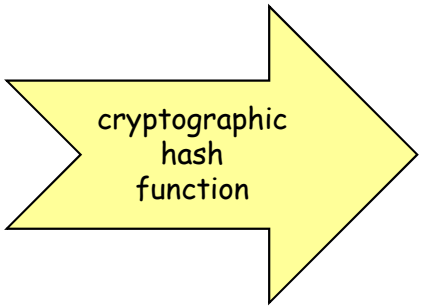
Almacenamiento contraseñas

- ¿Cómo se almacenan las contraseñas?
  - ¿Donde se almacenan las contraseñas?
    - Windows: C:\WINDOWS\system32\config\SAM
    - Linux: /etc/passwd
    - MacOS: /var/db/shadow/hash/
    - Shadow passwords
  - /etc/shadow sólo puede leerse por root
  - /etc/passwd muestra caracteres especiales '*', o x' en lugar del hash de la contraseña

Hash: huella digital, message digest o función de un solo sentido







9aa6abe505e5c526
d2238f641b903af4

Tecnológico de Monterrey

Salted hashes

- Salted hashes: Para cada contraseña se genera un número aleatorio (un nonce). Se hace el hash del password con el nonce, y se almacenan el hash y el nonce
  - Usual
  - hash = md5(“deliciously salty” + password)
    - MD5 is broken
    - Sus competidores actuales como SHA1 y SHA256 son rápidos, lo cal es un problema
  - Con hashes de 16b, hay 2^16 = 65,536 variaciones para la misma contraseña

Tecnológico de Monterrey

Saltos

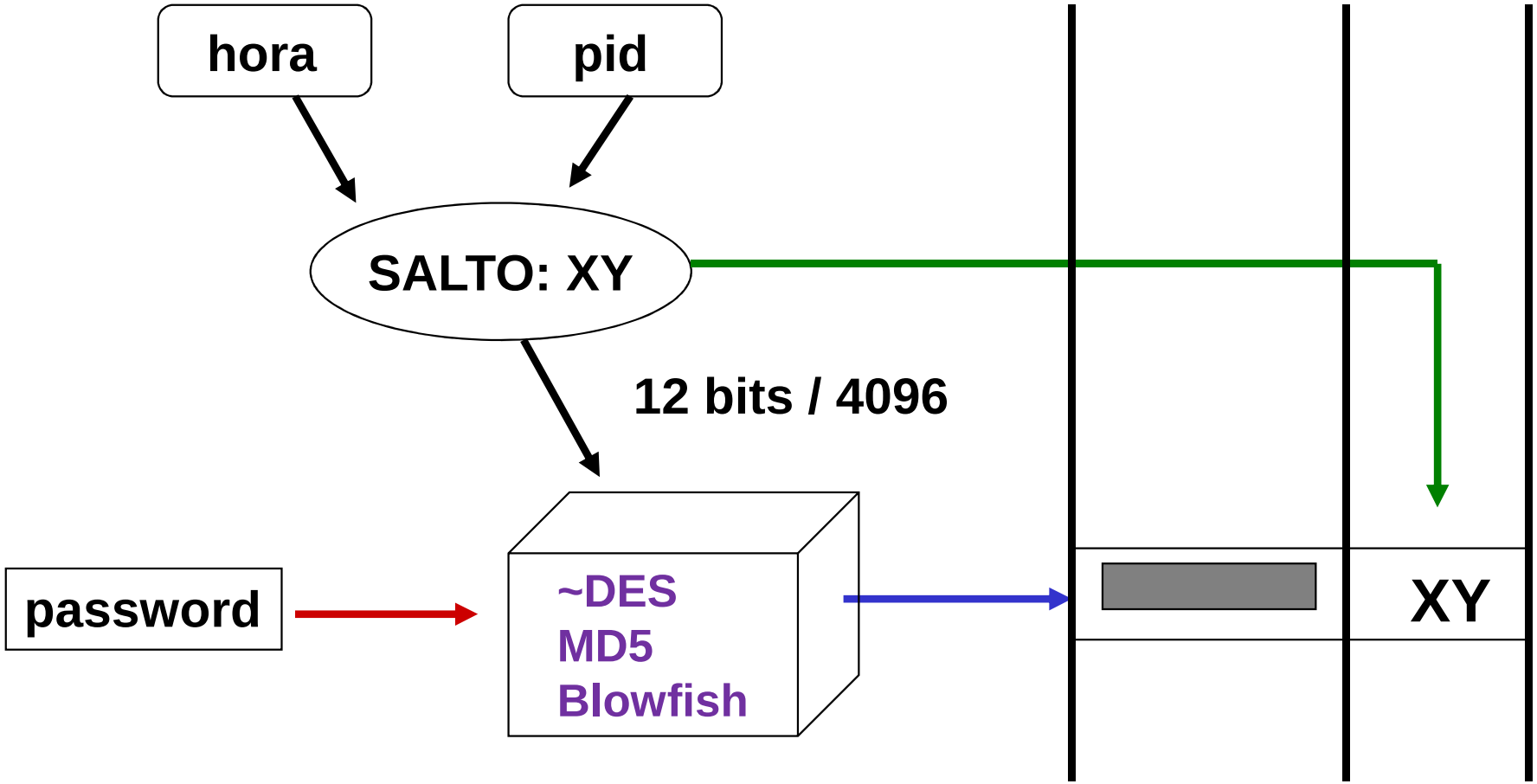
- Para hacer más robusto el algoritmo, se le añade un número de 12 bits (entre 0 y 4,095), obtenido del tiempo del sistema.
- Este número se le conoce como salto.
- El salto es convertido en un string de dos caracteres y es almacenado junto con el password en el archivo /etc/passwd ocupando los dos primeros lugares.
- Cuando se teclea el password este es encriptado con el salto, ya que si usa otro, el resultado obtenido no coincidiría con el password almacenado.

Tecnológico de Monterrey

Ejemplo passwords y saltos

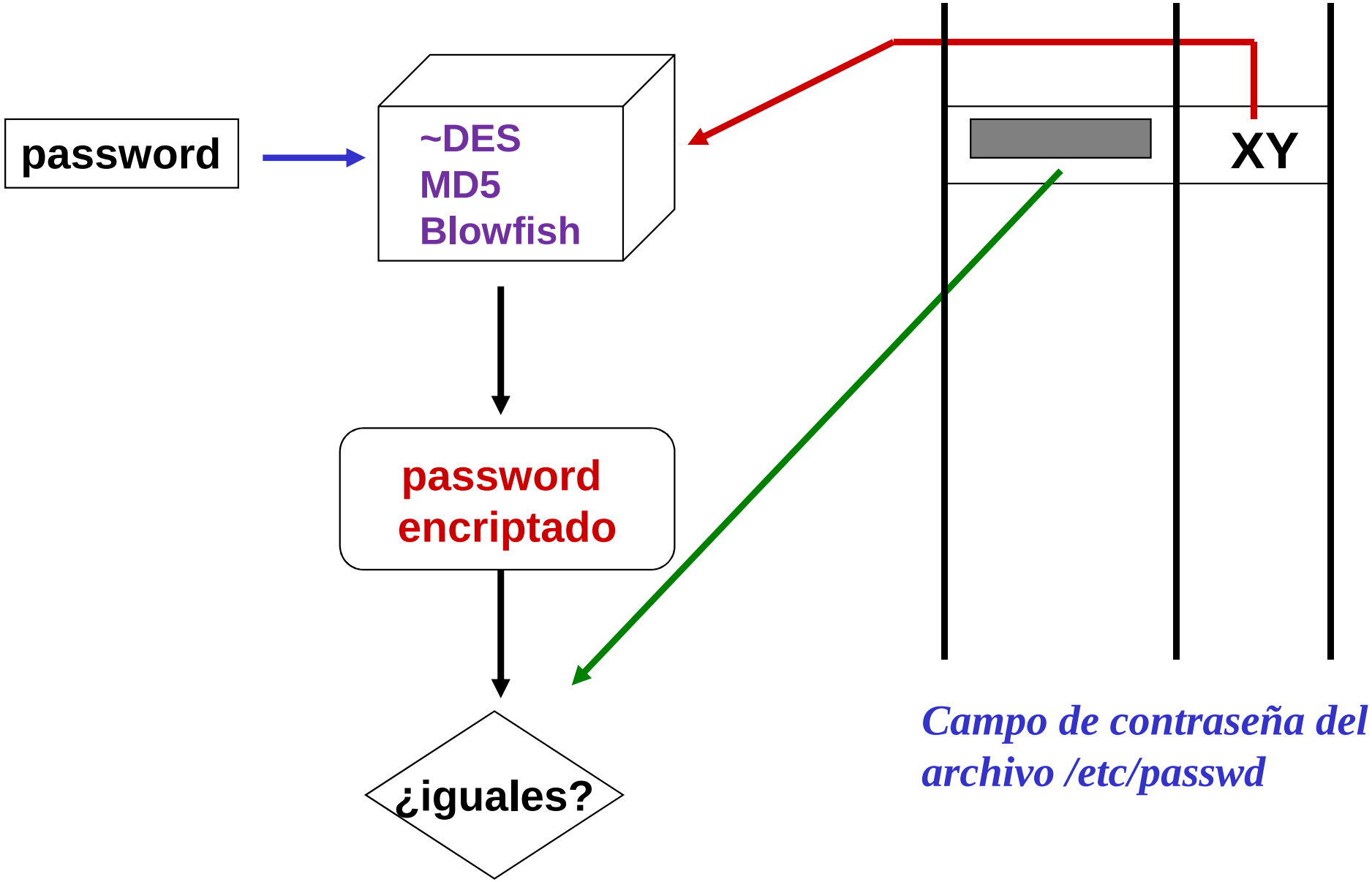
Password	Salto	Password Encriptado
My+Self	oZ	oZsV5zgRK6sjw
vaLgLo	Na	NaWyhsolA2gTM
ATSw.IM!	Hc	HcLrEM.BYtLwk
Global	Gi	GiRzWzP5IEPM
Global	DY	DYmeXoTgacmWY
Global	pd	pdOTBzon3G2KU

Encripción de un password



Campo de contraseña del archivo /etc/passwd

Verificación de un password



Tecnológico de Monterrey

Crackeo

- El termino se refiere al hecho de encontrar la contraseña de una determinada cuenta o de un conjunto de cuentas.
- Puede ser considerado ilegal o parte de una auditoria.

Algunas técnicas ataques contraseñas

1. Ataque diccionario
2. Ataque fuerza bruta
3. Ataque tablas arcoiris
4. Phishing
5. Ingeniería social
6. Malware
7. Offline cracking
8. Shoulder surfing
9. Spidering
10. Adivinar

Algunas anecdotas

- Prince William photos accidentally reveal RAF password (21.nov.2012)

- Very generous of FOX to show the Redskins Wi-Fi password on national tv (18.sep.2011)

La lección de Adobe

Important Customer Security Announcement

POSTED BY BRAD ARKIN, CHIEF SECURITY OFFICER ON OCTOBER 3, 2013 1:15 PM IN EXECUTIVE PERSPECTIVES

Cyber attacks are one of the unfortunate realities of doing business today. Given the profile and widespread use of many of our products, Adobe has attracted increasing attention from cyber attackers. Very recently, Adobe's security team discovered sophisticated attacks on our network, involving the illegal access of customer information as well as source code for numerous Adobe products. We believe these attacks may be related.

Our investigation currently indicates that the attackers accessed Adobe customer IDs and encrypted passwords on our systems. We also believe the attackers removed from our systems certain information relating to 2.9 million Adobe customers, including customer names, encrypted credit or debit card numbers, expiration dates, and other information relating to customer orders. At this time, we do not believe the attackers removed decrypted credit or debit card numbers from our systems. We deeply regret that this incident occurred. We're working diligently internally, as well as with external partners and law enforcement, to address the incident. We're taking the following steps:

- As a precaution, we are resetting relevant customer passwords to help prevent unauthorized access to Adobe ID accounts. If your user ID and password were involved, you will receive an email notification from us with information on how to change your password. We also recommend that you change your passwords on any website where you may have used the same user ID and password.

- We are in the process of notifying customers whose credit or debit card information we believe to be involved in the incident. If your information was involved, you will receive a notification letter from us with additional information on steps you can take to help protect yourself against potential misuse of personal

Tecnológico de Monterrey

Cuentas afectadas

- 3 millones de afectados
- 38 millones de afectados
- Más de 150 millones de usuarios afectados
- Top 100 de las contraseñas usadas

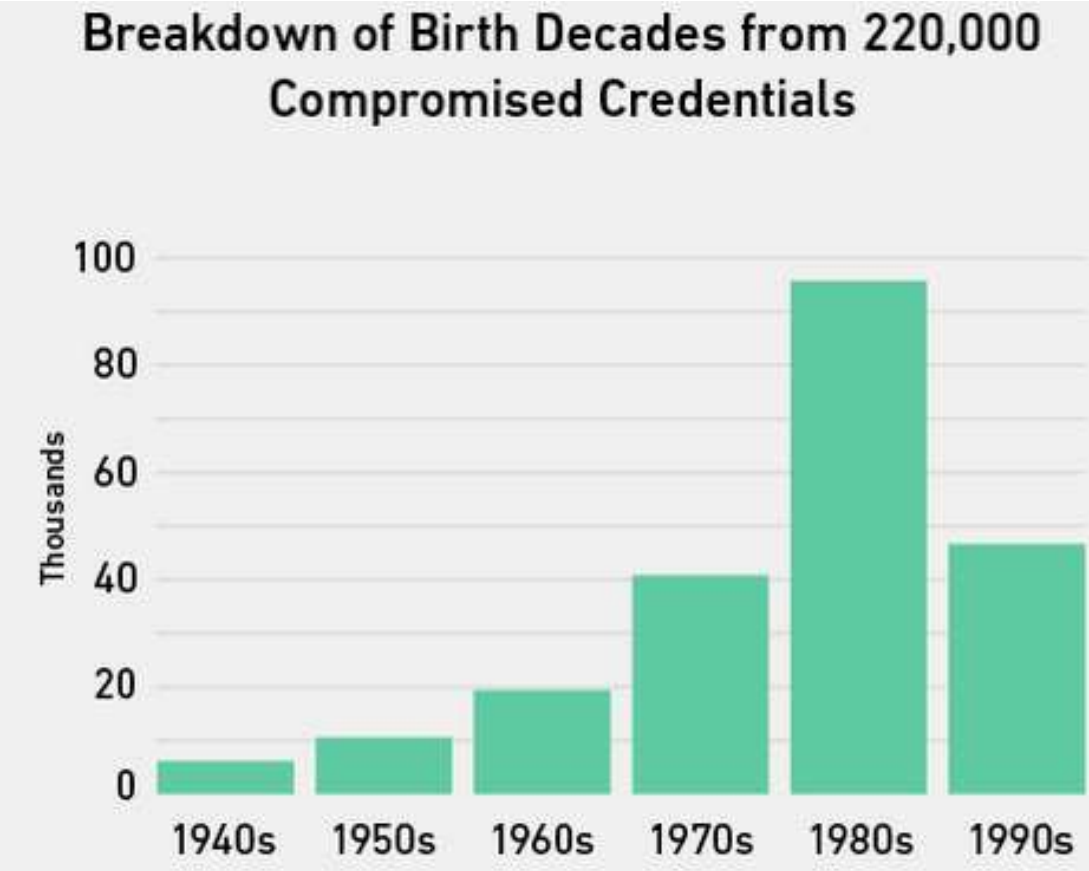
#	Count	Ciphertext	Plaintext
1.	1911938	EQ7fIpT7i/Q=	123456
2.	446162	j9p+HwtWWT86aMjgZFLzYg==	123456789
3.	345834	L8qbAD3jl3jioxG6CatHBw==	password
4.	211659	BB4e6X+b2xLioxG6CatHBw==	adobe123
5.	201580	j9p+HwtWWT/ioxG6CatHBw==	12345678
6.	130832	5djv7ZCI2ws=	qwerty
7.	124253	dQiOasWPYvQ=	1234567
8.	113884	7LqYzKVeq8I=	111111
9.	83411	PMDTbPOLZxuO3SwrFUvYGA==	photoshop
10.	82694	e6MPXQ5G6a8=	123123
11.	76910	j9p+HwtWWT8/HeZN+3oiCQ==	1234567890
12.	76186	diQ+ie23vAA=	000000
13.	70791	kCcUSCmonEA=	abc123
14.	61453	ukxzEcXU6Pw=	1234
15.	56744	5wEAInH22i4=	adobe1
16.	54651	WqflwJFYW3+PszVFZo1Ggg==	macromedia
17.	48850	hjAYsdUA4+k=	azerty
18.	47142	rpkvF+oZzQvioxG6CatHBw==	iloveyou
19.	44281	xz6PIeGzr6g=	aaaaaa
20.	43670	Ypsmk6AXQTk=	654321

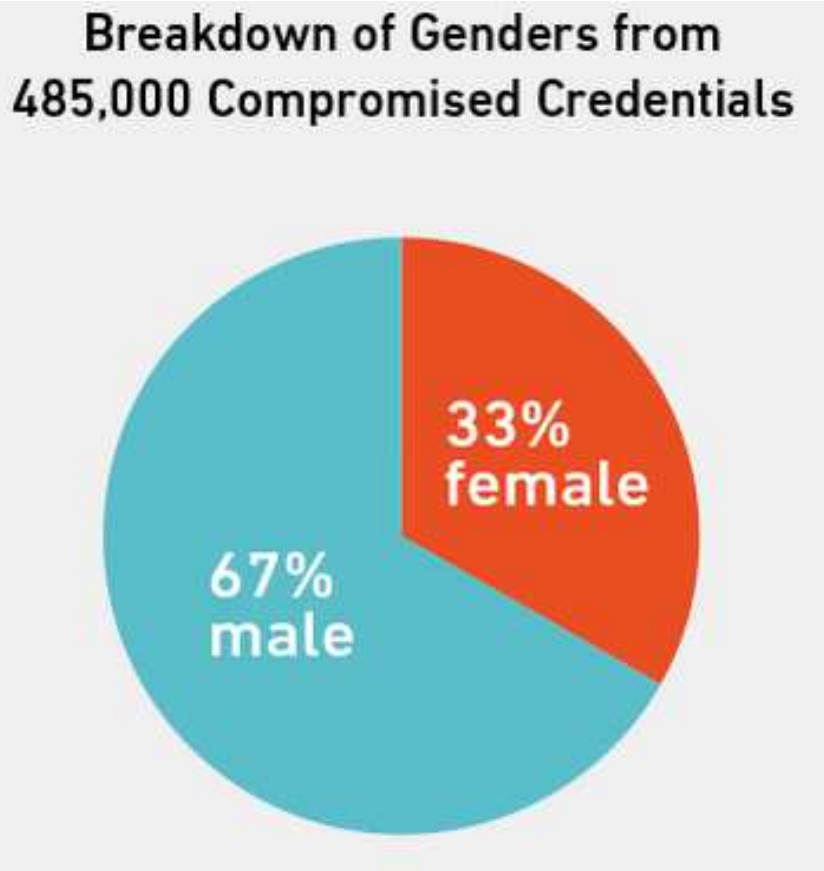
¿Cómo se almacenaban las contraseñas?

- Se seleccionó un cifrado simétrico (3DES) en modo ECB en lugar de hash.
- Se uso la misma llave para cada contraseña.
- Al usuario se le permitía ingresar “pistas” para recuperar su contraseña en caso de olvidarla.

```
111286969-|--|-th[redacted]bog.com-|-EQ7fIpT7i/Q=-|-it is 123456|--
111410317-|--|-gi[redacted]ail.com-|-EQ7fIpT7i/Q=-|-La mia pass e 123456|--
111500020-|--|-na[redacted]mail.com-|-EQ7fIpT7i/Q=-|-my number 123456|--
115288066-|--|-st[redacted]oek@yahoo.com-|-EQ7fIpT7i/Q=-|-123456 is die password|--
116948087-|--|-ma[redacted]ail.com-|-EQ7fIpT7i/Q=-|-123456 es la contrase?a|--
102473448-|--|-lu[redacted]e@yahoo.com-|-EQ7fIpT7i/Q=-|-123456 is the password|--
102573487-|--|-ki[redacted]000@yahoo.com-|-EQ7fIpT7i/Q=-|-the password is 123456|--
```

Unmasked: What 10 million passwords reveal about the people who choose them





Los 50 passwords más usados

1. 123456	11. 123123	21. mustang	31. 7777777	41. harley
2. password	12. baseball	22. 666666	32. f*cky*u	42. zxcvbnm
3. 12345678	13. abc123	23. qwertyuiop	33. qazwsx	43. asdfgh
4. qwerty	14. football	24. 123321	34. jordan	44. buster
5. 123456789	15. monkey	25. 1234...890	35. jennifer	45. andrew
6. 12345	16. letmein	26. p*s*y	36. 123qwe	46. batman
7. 1234	17. shadow	27. superman	37. 121212	47. soccer
8. 111111	18. master	28. 270	38. killer	48. tigger
9. 1234567	19. 696969	29. 654321	39. trustno1	49. charlie
10. dragon	20. michael	30. 1qaz2wsx	40. hunter	50. robert

Añadiendo un número

Most Used Numbers (0-99) at the End of Passwords			Least Used Numbers (0-99) at the End of Passwords		
1.	examplepassword**1**	23.84%	100.	examplepassword**39**	0.15%
2.	examplepassword**2**	6.72%	99.	examplepassword**49**	0.16%
3.	examplepassword**3**	3.86%	98.	examplepassword**60**	0.17%
4.	examplepassword**12**	3.55%	97.	examplepassword**38**	0.18%
5.	examplepassword**7**	3.54%	96.	examplepassword**37**	0.18%
6.	examplepassword**5**	3.35%	95.	examplepassword**41**	0.18%
7.	examplepassword**4**	3.19%	94.	examplepassword**61**	0.18%
8.	examplepassword**6**	3.06%	93.	examplepassword**46**	0.19%
9.	examplepassword**9**	2.91%	92.	examplepassword**53**	0.19%
10.	examplepassword**8**	2.89%	91.	examplepassword**48**	0.19%

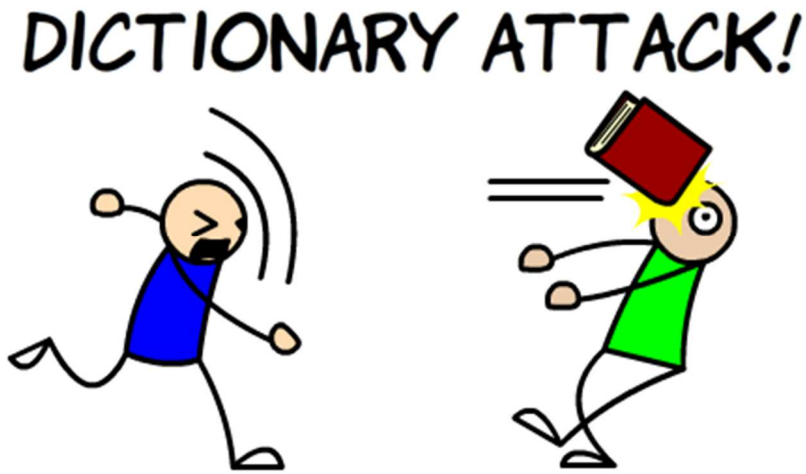
Tecnológico de Monterrey

Los 20 patrones más comunes de secuencias en 10 millones de passwords

Fuerza bruta vs diccionario

- Fuerza bruta: probar todas las combinaciones de un conjunto de símbolos. Dado el tiempo y CPU suficiente las contraseñas eventualmente serán crackeadas.

- Diccionario: Lista de palabras, encriptadas una vez en un tiempo dado y verifica si los hashes son iguales.



Tecnológico de Monterrey

Tiempo de crackeo

Conjunto caracteres	Número de símbolos en el conjunto	Passwords de 3 símbolos		Passwords de 6 símbolos	
		Cantidad	Tiempo	Cantidad	Tiempo
Letras latinas minúsculas	26	17,576	0.02 segs	308.915.776	5 min
Letras latinas minúsculas y dígitos.	36	46,656	0.04 segs	2.176.782.336	36 min
Letras latinas minúsculas, mayúsculas y dígitos.	62	238,238	0.2 segs	56.800.235.584	15 hrs
Letras latinas minúsculas, mayúsculas, dígitos y caracteres especiales	94	830,584	1 seg	689.869.781.056	8 dias

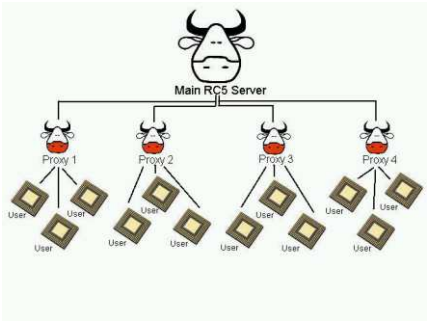
Tecnológico de Monterrey

Tiempo de crackeo

Conjunto caracteres	Número símbolos	Passwords de 8 símbolos		Passwords de 12 símbolos	
		Cantidad	Tiempo	Cantidad	Tiempo
Letras latinas minúsculas	26	208.827.064.576	58 hrs	95.428.956.661.682.176	3,000 años
Letras latinas minúsculas y dígitos.	36	2.821.109.907.456	32 días	4.738.381.338.321.616.896	150,000 años
Letras latinas minúsculas, mayúsculas y dígitos.	62	2.183.40.105.584.896	7 años	3.226.266.762.397.899.821 .056	100 millones años
Letras latinas minúsculas, mayúsculas, dígitos y caracteres especiales	94	6.095.689.385.410.816	193 años	475.920.314.814.253.376.4 75.1366	Más de lo que ha existido la tierra

Procesamiento

- CPUs
- Procesadores gráficos
  - GPGPU, (General-purpose computing on graphics processing units) en Georgia Tech Research Institute



- Botnets
- Distributed.net
- FPGAs: DeepCrack de la EFF
- La nube

Password Cracking en la nube

Password cracking in the cloud

Cloud computing gives bad guys a new tool

Security: Risk and Reward *By Andreas M. Antonopoulos, Network World*
November 17, 2010 05:23 PM ET

Comment Print Recommend Be the first of your friends to recommend this.

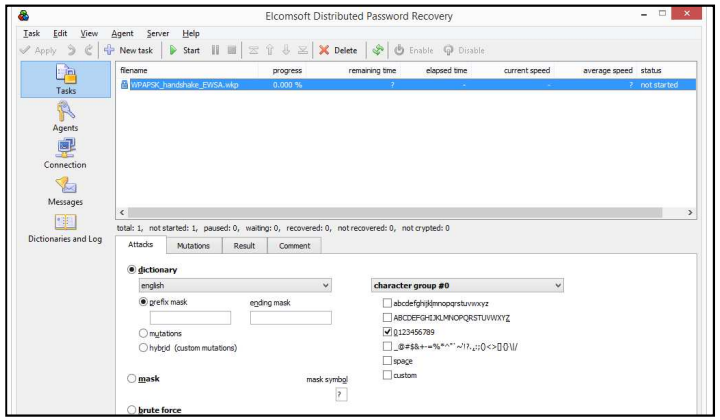
On-demand cloud computing is a wonderful tool for companies that need some computing capacity for a short time, but don't want to invest in fixed capital for long term. For the same reasons, cloud computing can be very useful to hackers -- a lot of hacking activities involve cracking passwords, keys or other forms of brute force that are computationally expensive but highly parallelizable.

For a hacker, there are two great sources for on-demand computing: botnets made of consumer PCs and infrastructure-as-a-service (IaaS) from a service provider. Either one can deliver computing-on-demand for the purpose of brute-force computation. Botnets are unreliable, heterogeneous and will take longer to "provision." But they cost nothing to use and can scale to enormous size; researchers have found botnets composed of hundreds of thousands of PCs. A commercial cloud-computing offering will be faster to provision, have predictable performance and can be billed to a stolen credit card.

Ejemplo “password recovery software”

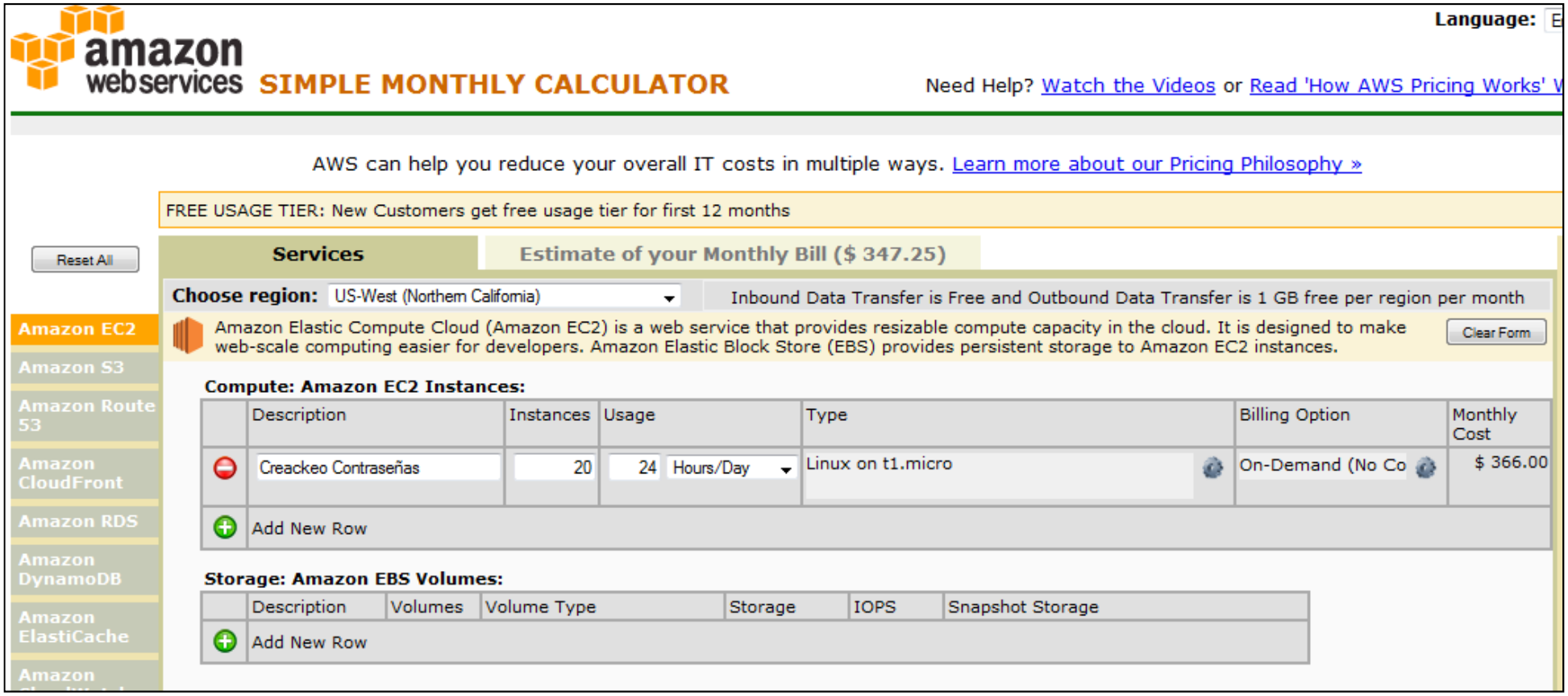
Application family	Applications	Extensions	Type of recovery	Password types	Hardware Acceleration
ZIP archives	PKZip, WinZip	.ZIP, .EXE	password	file opening password	NVIDIA
ZIP archives	WinZip (AES)	.ZIPX. .EXE	password	file opening password	NVIDIA
RAR archives	RAR/WinRAR 3/4/5	.RAR	password	file opening password	NVIDIA
Microsoft Office 2007	Word, Excel, PowerPoint, Project	.DOCX, .XLSX, .PPTX, .MSPX	password	file opening password	NVIDIA AMD Tableau
Microsoft Office 2007	Access	.ACCDB	password	file opening password	–
Microsoft Office 2010	Word, Excel, Access, PowerPoint, OneNote	.DOCX, .XLSX, .ACCDB, .PPTX, .ONE	password	file opening password	NVIDIA AMD Tableau
PGP and Open-Key Passwords	Personal Information Exchange certificates - PKCS #12	.PFX, .P12	password		NVIDIA
IKE	Internet Key Exchange (IKE) passwords		password		NVIDIA
TrueCrypt	TrueCrypt disk encryption		password		NVIDIA
TrueCrypt	TrueCrypt encrypted containers		password		NVIDIA
BitLocker	BitLocker and BitLocker To Go disk encryption		password		NVIDIA AMD
	MD5 hashes		password	plaintext passwords	NVIDIA^2
	Salted MD5 hashes		password	plaintext passwords	NVIDIA^2
Adobe Acrobat PDF	PDF with 256-bit encryption	.PDF	password	"user" and "owner" password	NVIDIA^4
Adobe Acrobat PDF	PDF with 128-bit encryption	.PDF	password	"user" and "owner" password	–

Up to 5 clients - **$ 599**
Up to 20 clients - **$ 1999**
Up to 100 clients - **$ 4999**
100+ clients - **contact us**



https://www.elcomsoft.com/edpr.html

Ejemplo costo computo nube



http://calculator.s3.amazonaws.com/index.html

Up to 5 clients	- **$ 599**
Up to 20 clients	- **$ 1999**
Up to 100 clients	- **$ 4999**
100+ clients	- **contact us**

https://www.elcomsoft.com/edpr.html

Las contraseñas son como la ropa interior…

- Debes cambiarla regularmente.
- No puedes dejar que nadie la vea
- No la compartas ni con tus amigos.
- Mientras más largas, mejor.
- No las dejes tiradas por ahí.
- Sé misterioso.

Concluyendo…

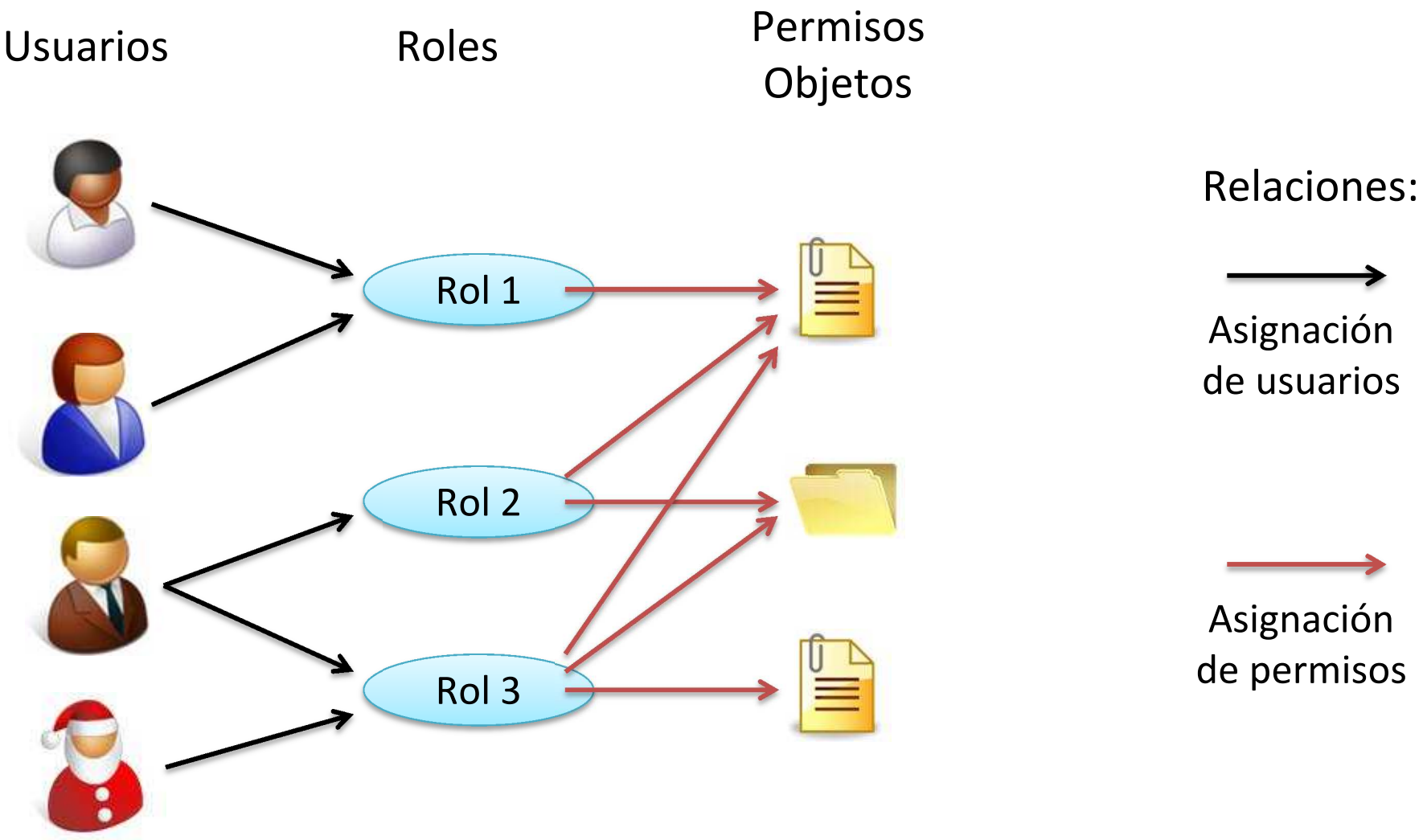
Mecanismos de control de acceso

- La autenticación pretende establecer quién eres.
- La autorización (o control de accesos) establece qué puedes hacer con el sistema.
- Dos modelos: DAC y MAC
- Control de acceso discrecional (DAC),
  - un usuario bien identificado (típicamente, el creador o 'propietario' del recurso) decide cómo protegerlo estableciendo cómo compartirlo, mediante controles de acceso impuestos por el sistema.
- Control acceso mandatorio (MAC)
  - es el sistema quién protege los recursos.
  - todo recurso del sistema, y todo usuario tiene una etiqueta de seguridad.

Control de acceso basado en Roles

- También conocido como RBAC
  - Role Based Access Control
- Surge a finales de los 80s y toma un fuerte impulso en los 90s.
- Combina aspectos de DAC y MAC , pero con una visión más orientada a la estructura organizacional.
- Básicamente consiste en la creación de roles para los trabajos o funciones que se realizan en la organización.
- Los miembros del staff se asignan a roles y a través de estos roles adquieren permisos para ejecutar funciones del sistema.

RBAC básico ilustrado

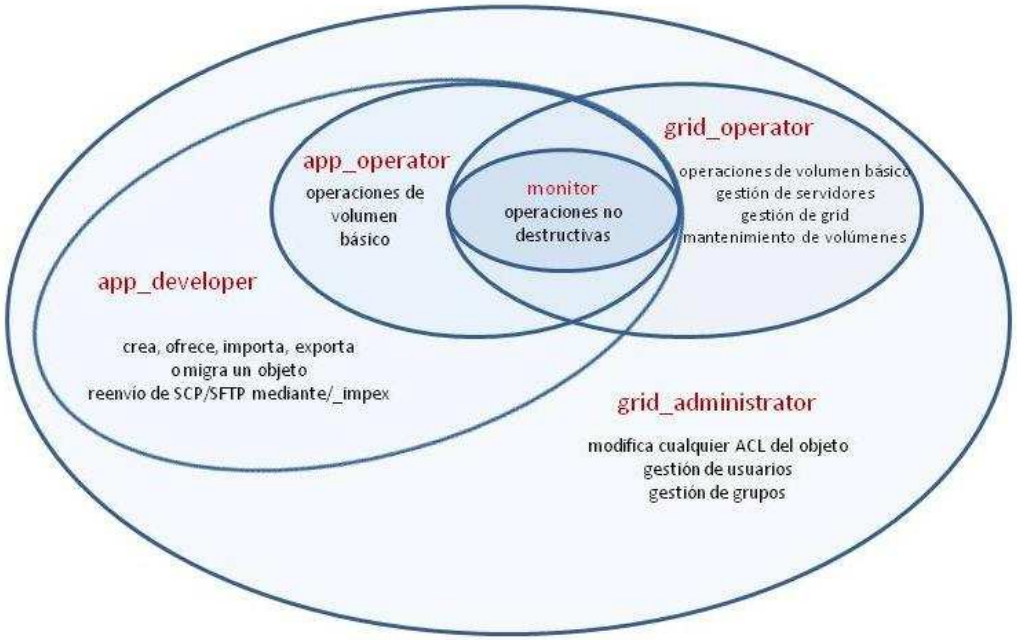


Tecnológico de Monterrey

RBAC

- Los sujetos acceden a los objetos en base a las actividades que (los sujetos) llevan a cabo en el sistema.
- Es decir, considerando los roles que ocupan en el sistema.
- Rol
  - Es el conjunto de acciones y responsabilidades asociadas con una actividad en particular.
  - También conocido como *Perfil*.

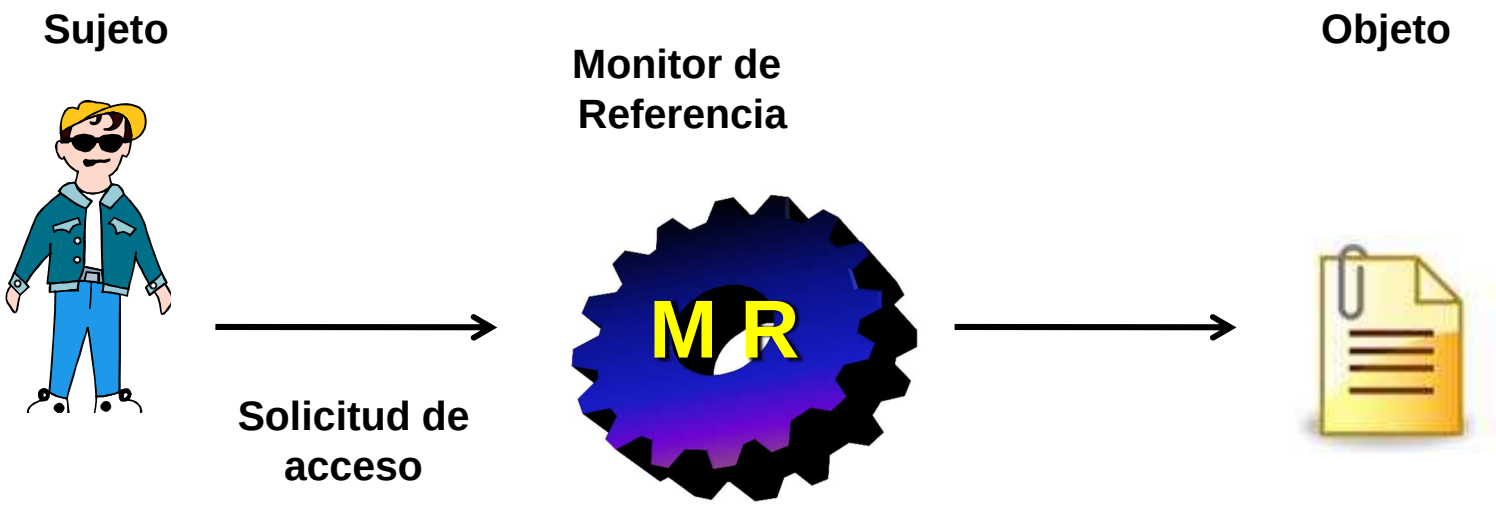
Ejemplo RBAC: Sistema GRid



	Listar Aplics	Migrar Aplic o clase	Aprovisio-nar una aplicación	Crear o importar aplicación	Enumerar catálogos	Mostrar info servidores	Listar ACL Grid	Reiniciar la Grid	Crear o borrar usuarios	Desbloqueo de usuarios	Importar exportar volums	Limipia o reparar volums
Monitor	X				X	X						
Operador	X				X	X						
Desarrollador	X	X	X	X	X	X					X	
Operador Grid	X				X	X	X	X				X
Admon Grid	X	X	X	X	X	X	X	X	X	X	X	X

Control acceso y monitor referencia

- Monitor referencia: mecanismo responsable de “mediar” cuando los sujetos intentan realizar operaciones sobre los objetos en función de una política de acceso.



Matrices

	R_1	R_2	...	R_n
U_1	✖			
U_2	✖			
U_3		✖		✖
U_4				✖
U_5				✖
U_6				✖
...				
U_m	✖			

(Usuarios, Roles)

OBJECTS

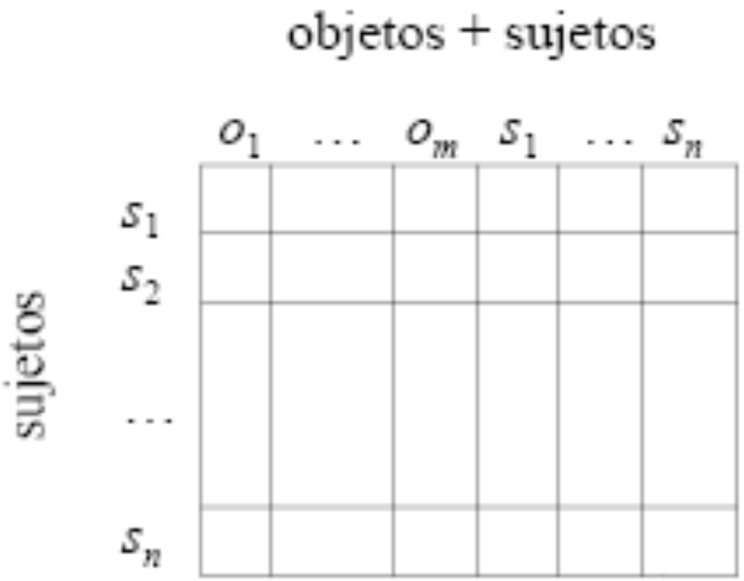
ROLES	R_1	R_2	R_n	F_1	F_1	P_1	P_2	D_1	D_2
R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R_2		control		write *	execute			owner	seek *
...									
R_n			control		write	stop			

(Roles, Objetos)

- Similar a DAC
- Roles pueden ser objetos

Matriz de control de acceso

- Modelo conceptual que describe el estado de protección de manera precisa.
- Matriz que describe los permisos de los sujetos (usuarios o procesos) sobre los objetos.



- Sujetos $S = \{ s_1,\ldots,s_n \}$
- Objetos $O = \{ o_1,\ldots,o_m \}$
- Permisos $R = \{ r_1,\ldots,r_k \}$
- Entradas $A[s_i, o_j] \subseteq R$

$A[s_i, o_j] = \{ r_x, \ldots, r_y \}$
Es decir el sujeto s_i tiene permisos $r_x, \ldots, r_y$ sobre el objeto o_j

Un primer ejemplo

- Dos usuarios: toto, cachafas
- Tres archivos: info.pdf, script.sh, foto.jpg
- Tres permisos:
  - r=lectura, w=escritura, x=ejecución

	info.pdf	script.sh	foto.jpg
toto	---	*rwx*	*rw*
cachafas	*rw*	*rx*	*r*

Tecnológico de Monterrey

Un segundo ejemplo

	A1	A2	A3	A4	Imp1	Imp2	DD1	DD2
U1	eje lec							
U2	lec esc borr							lec esc format
U3		esc lec eje		esc lec eje	imp			lec format
U4			esc		imp		lec esc	
U5		lec ejec	lec eje			imp		

Tecnológico de Monterrey

Implementación

- Dos formas de implementar la matriz de control de accesos:
  - Lista de control de accesos (ACL):
    - Hay una lista por objeto.
    - Indica los permisos que posee cada sujeto sobre el objeto.
  - Lista de capacidades:
    - Hay una lista por sujeto.
    - Indica los permisos que posee el sujeto sobre cada objeto.

Tecnológico de Monterrey

Listas de control de accesos

- Consiste en almacenar la matriz de control de accesos por columnas.
- Dado un objeto, tenemos las siguientes ventajas :
  - Es fácil ver los permisos del mismo para todos los sujetos.
  - Es fácil revocar todos sus accesos, reemplazando su ACL por una vacía.
  - Es fácil darlo de baja, borrando su ACL.
- Problemas:
  - ¿Cómo verificar a que puede acceder un sujeto?

Tecnológico de Monterrey

Lista control de acceso

Objeto	Usuario	Permisos
A1	U1	eje, lec
	U2	lec, esc, borr
A2	U3	esc, lec, eje
	U5	lec, eje
A3	U4	esc
	U5	lec, eje
A4	U3	esc, lec, eje
Imp1	U3	imp
	U4	imp
Imp2	U5	imp
DD1	U4	lec, esc
DD2	U2	lec, esc, format
	U3	lec, format

Tecnológico de Monterrey

Lista de capacidades

- Consiste en almacenar la matriz de control de accesos por filas.
- Dado un sujeto, tenemos las siguientes ventajas:
  - Es fácil de chequear todos los permisos que posee.
  - Es fácil de revocar sus permisos, reemplazando su lista de capacidades por una vacía.
  - Es fácil darlo de baja, eliminando su lista de capacidades.
- Problemas:
  - ¿Cómo verificar quien puede acceder a un objeto?

Tecnológico de Monterrey

Ejemplo lista capacidades

Usuario	Objeto(s)	Permisos
U1	A1	lec, eje
U2	A1	lec, esc, borr
	DD2	lec, esc, format
	A2	lec, esc, eje
U3	A4	esc, lec, eje
	Imp1	imp
	DD2	lec, forma
	A3	esc
U4	Imp1	imp
	DD1	lec, esc
	A2	lec, eje
U5	A3	lec, eje
	Imp2	imp

Lista capacidades vs ACL

LISTA CONTROL ACCESO ACL

MATRIZ DE ACCESO

	$Objeto_1$	$Objeto_2$	$Objeto_3$	...	$Objeto_M$
$Usuario_1$	rwx	rw	rwx	...	rw
$Usuario_2$	x	r	x	...	rw
$Usuario_3$	x	rw	rwx	...	r
...	...	...	...	...	...
$Usuario_N$	x	rw	x	...	w

ACL

ACL $Objeto_2$	$Usuario_1$	$Usuario_2$	$Usuario_3$	...	$Usuario_N$
	rw	r	rw	...	rw

CAPACIDADES

MATRIZ DE ACCESO

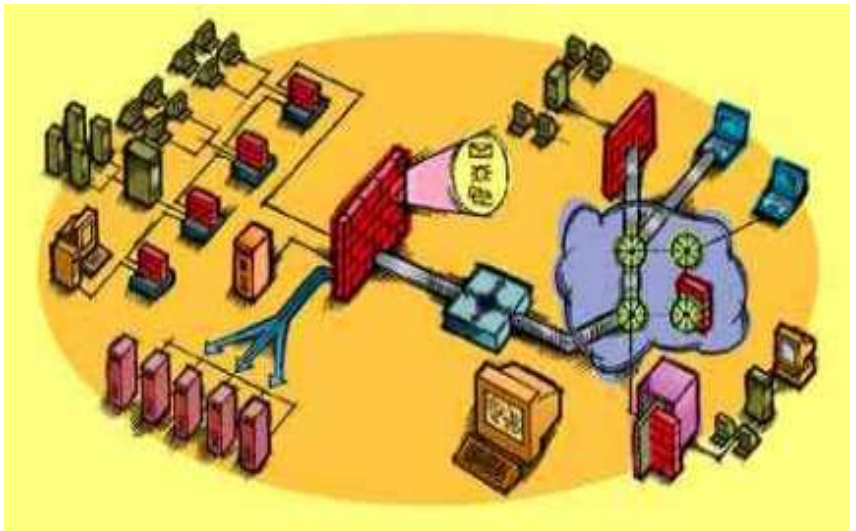
	$Objeto_1$	$Objeto_2$	$Objeto_3$	...	$Objeto_M$
$Usuario_1$	rwx	rw	rwx	...	rw
$Usuario_2$	x	r	x	...	rw
$Usuario_3$	x	rw	rwx	...	r
...	...	...	...	...	...
$Usuario_N$	x	rw	x	...	w

Capacidades

Capab $Usuario_3$	$Objeto_1$	$Objeto_2$	$Objeto_3$	...	$Objeto_N$
	x	rw	rwx	...	r

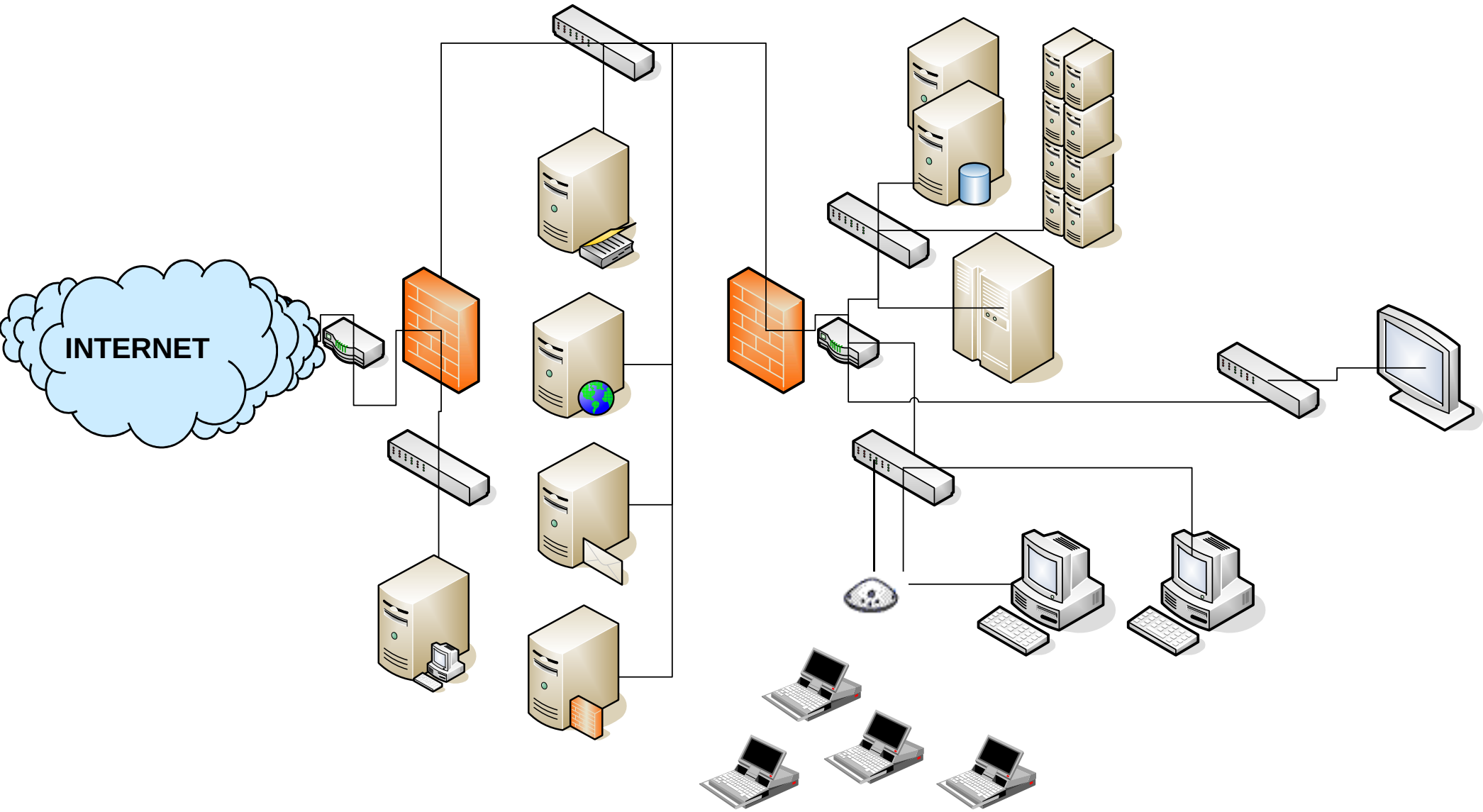
Mecanismos de separación

- Definición de un perímetro de seguridad
- Definir las zonas “abiertas” y las zonas cerradas.
  - DMZ: Zona desmilitarizada
  - *Segmentar* la red interna
- Mecanismos que sirven para delimitar una frontera
  - Filtros de paquetes
  - Firewalls
  - Wrappers
  - Proxies



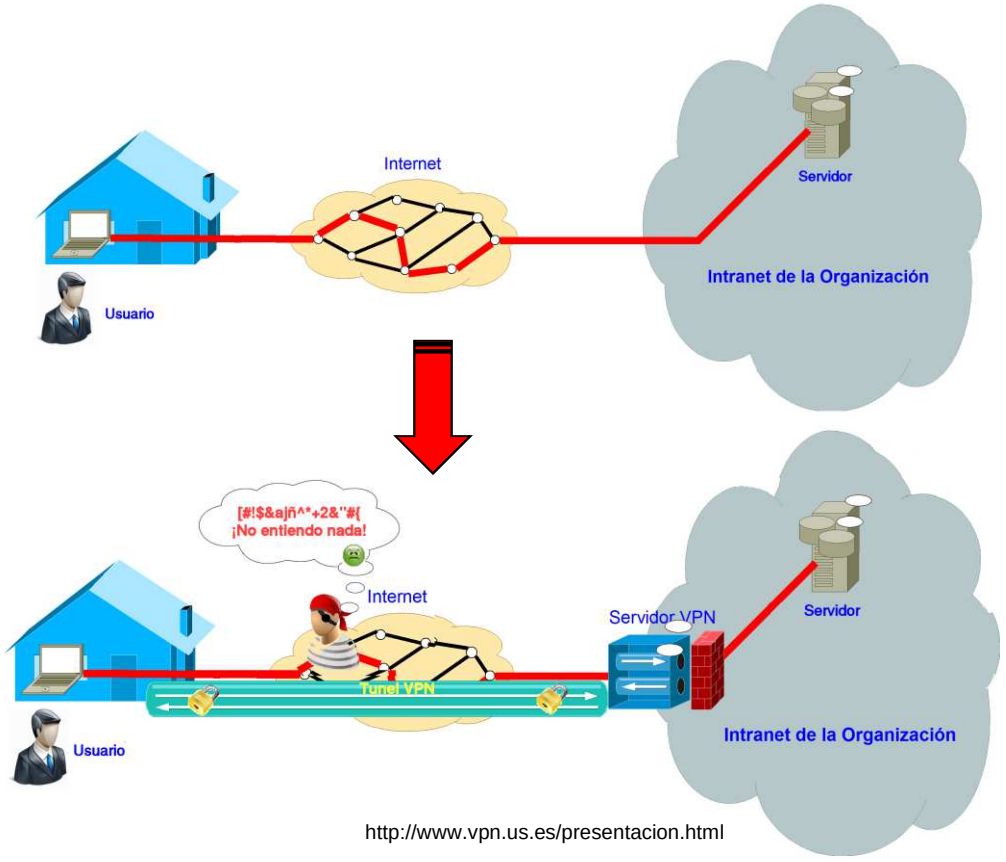
Tecnológico de Monterrey

Ejemplo separación

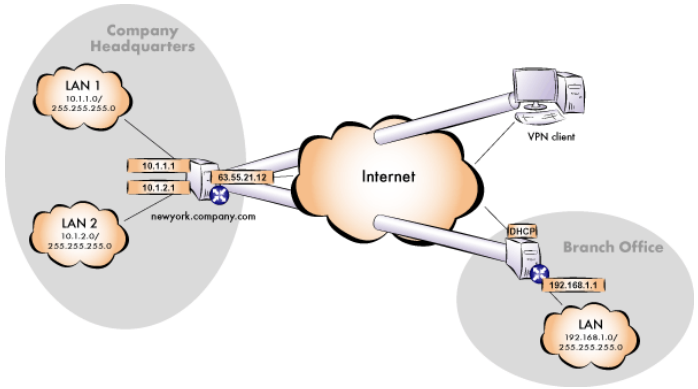


Mecanismos seguridad en las comunicaciones

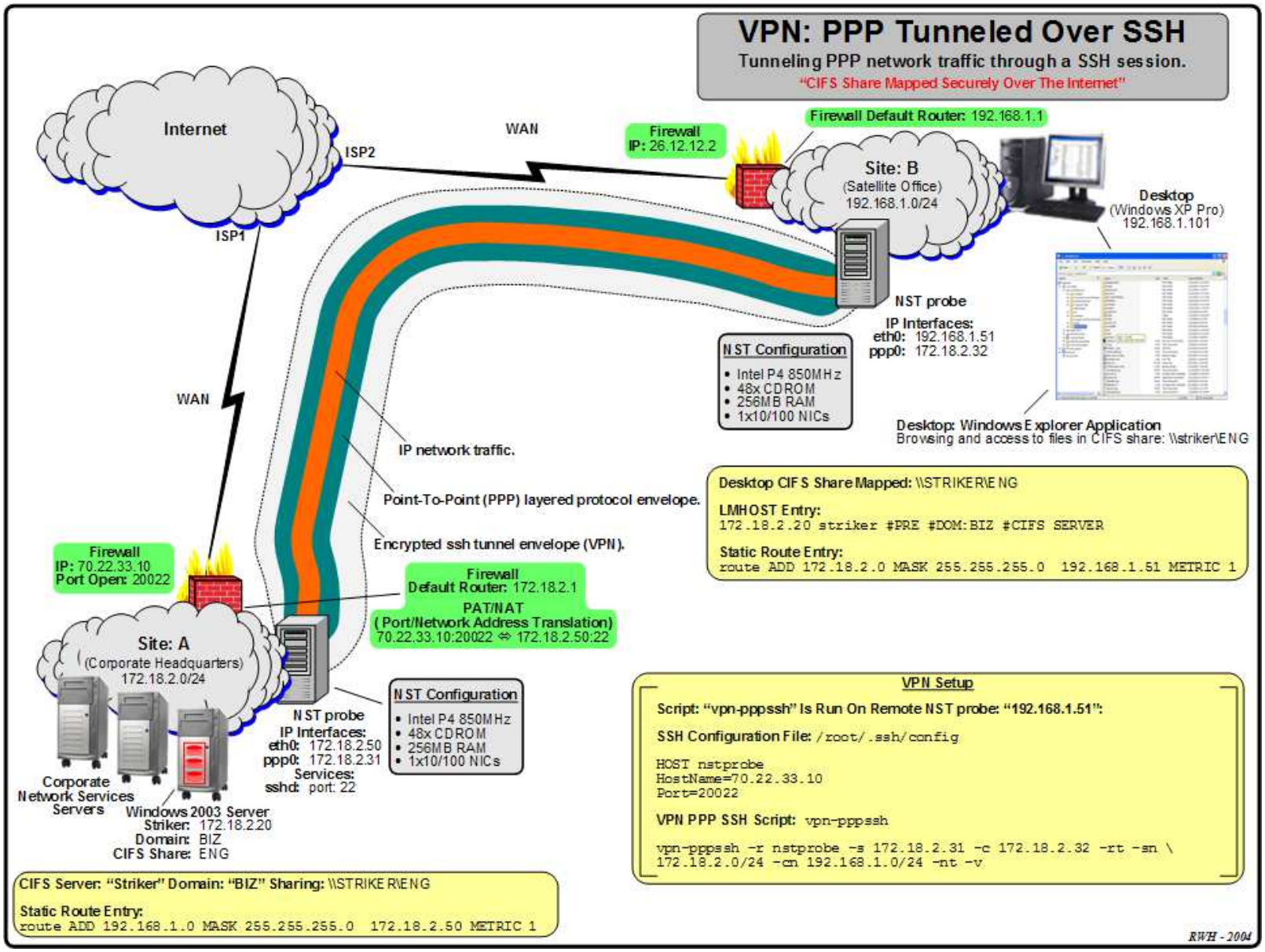
- Seguridad transmisión información entre diferentes entidades.
- Objetivos
  - ***Confidencialidad*** de la información transmitida
  - ***Integridad*** de los datos entre las diferentes entidades
  - ***Autenticidad*** de las partes comunicantes y de la información transmitida
  - ***Control acceso:*** usuario solo tiene acceso a lo que requiere para su función.
- Herramientas
  - Criptografía: VPNs



http://www.vpn.us.es/presentacion.html



Ejemplo VPN



Fuente: http://nst.sourceforge.net/nst/docs/user/ch06s03.html

Tecnológico de Monterrey

DESDE AQUÍ ABARCA EL SEGUNDO PARCIAL

SEMESTRE 201513

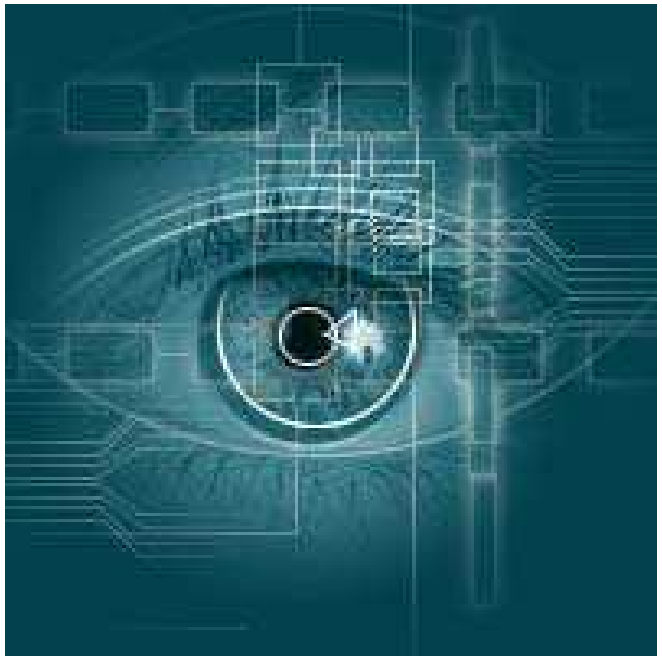
Tecnológico de Monterrey

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.

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

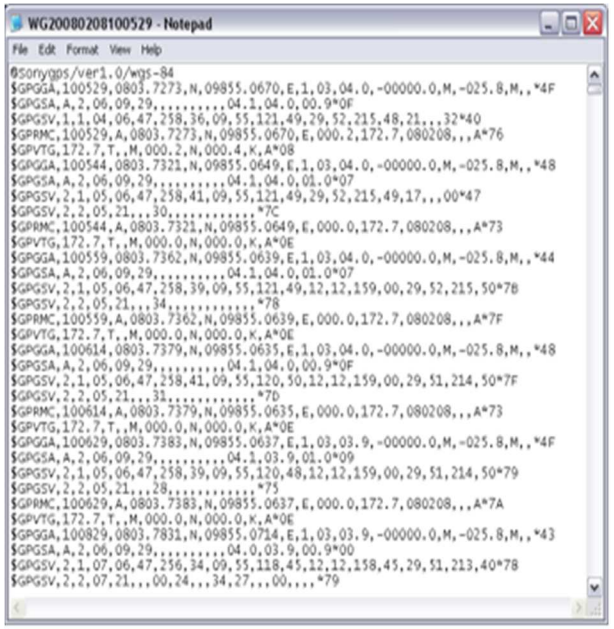


Mecanismos de recuperación

- 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

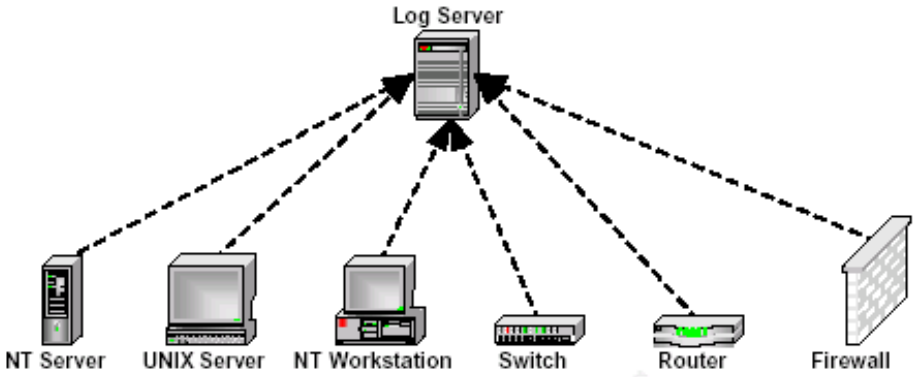
- Se refiere al procedimiento a través del cual un sistema operativo registra eventos conforme van ocurriendo y los preserva para un uso posterior.
- Bitácora:
  - Registro de datos sobre quien, que, cuando, donde y por que (W5: who, what, when, where y why, W5) un evento relacionado con un dispositivo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

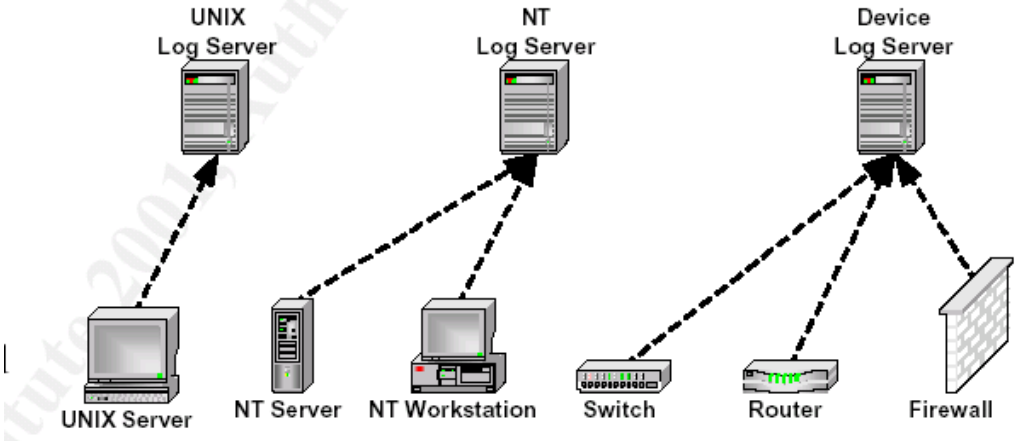



```
[2011.09.27 10.12.15 ]  product_version: DMO
[2011.09.27 10.12.15 ] [AutoOsDetection()] - Entered
[2011.09.27 10.12.15 ]  [Param] ProductInfo:DMO
[2011.09.27 10.12.15 ]  [Param] OSInfo:Red Hat Enterprise Linux Server release 5.5 {32-bit}
[2011.09.27 10.12.15 ]  [Param] CPU Arch:Kernel=i686
[2011.09.27 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
```

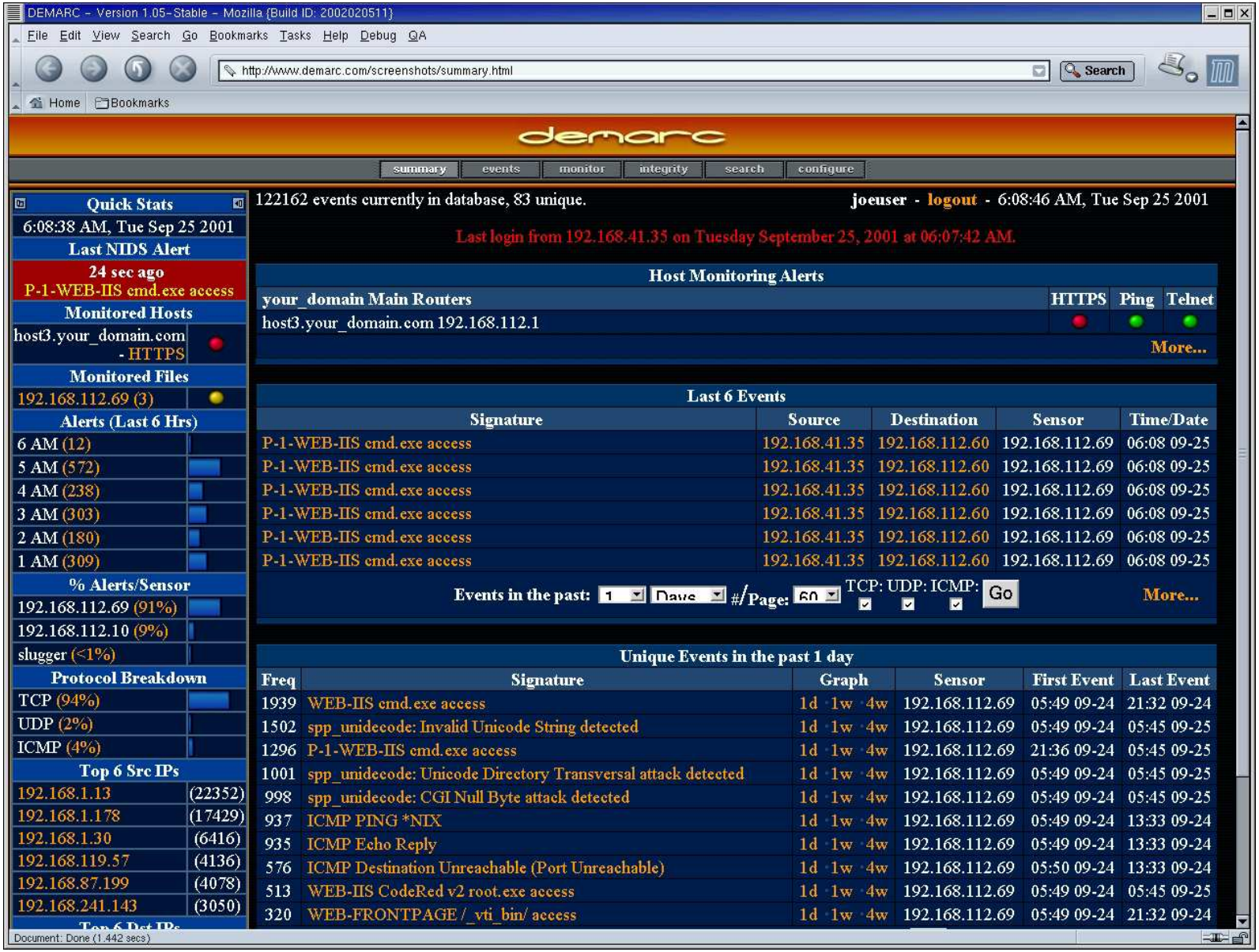
Consolidación de bitácoras

- 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.

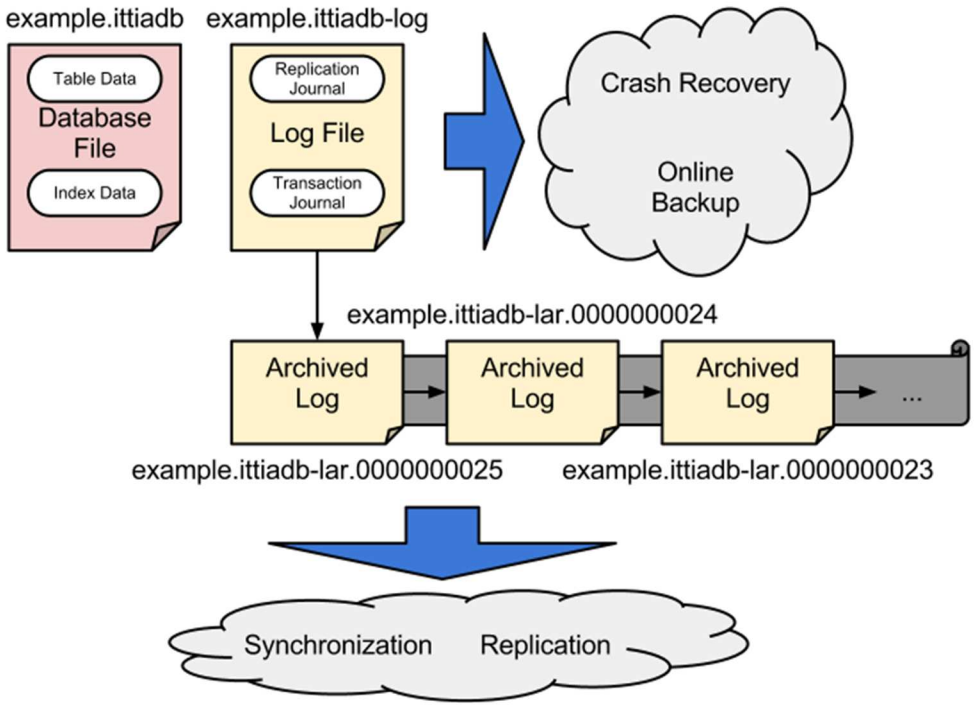


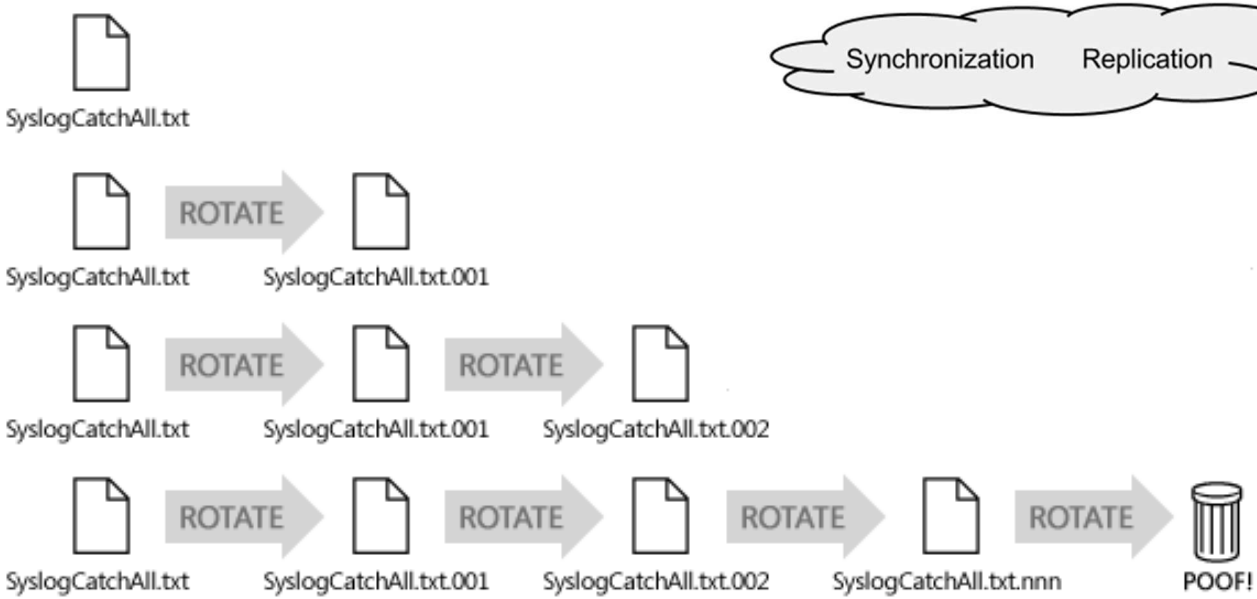


Ejemplo consolidación

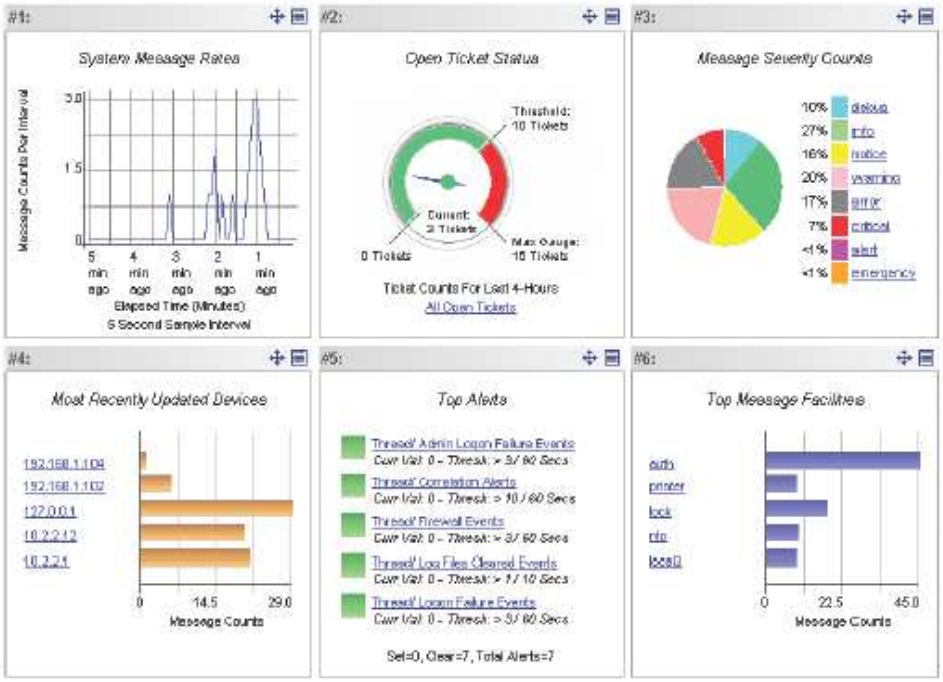


Rotación de bitácoras





Correlación de bitácoras



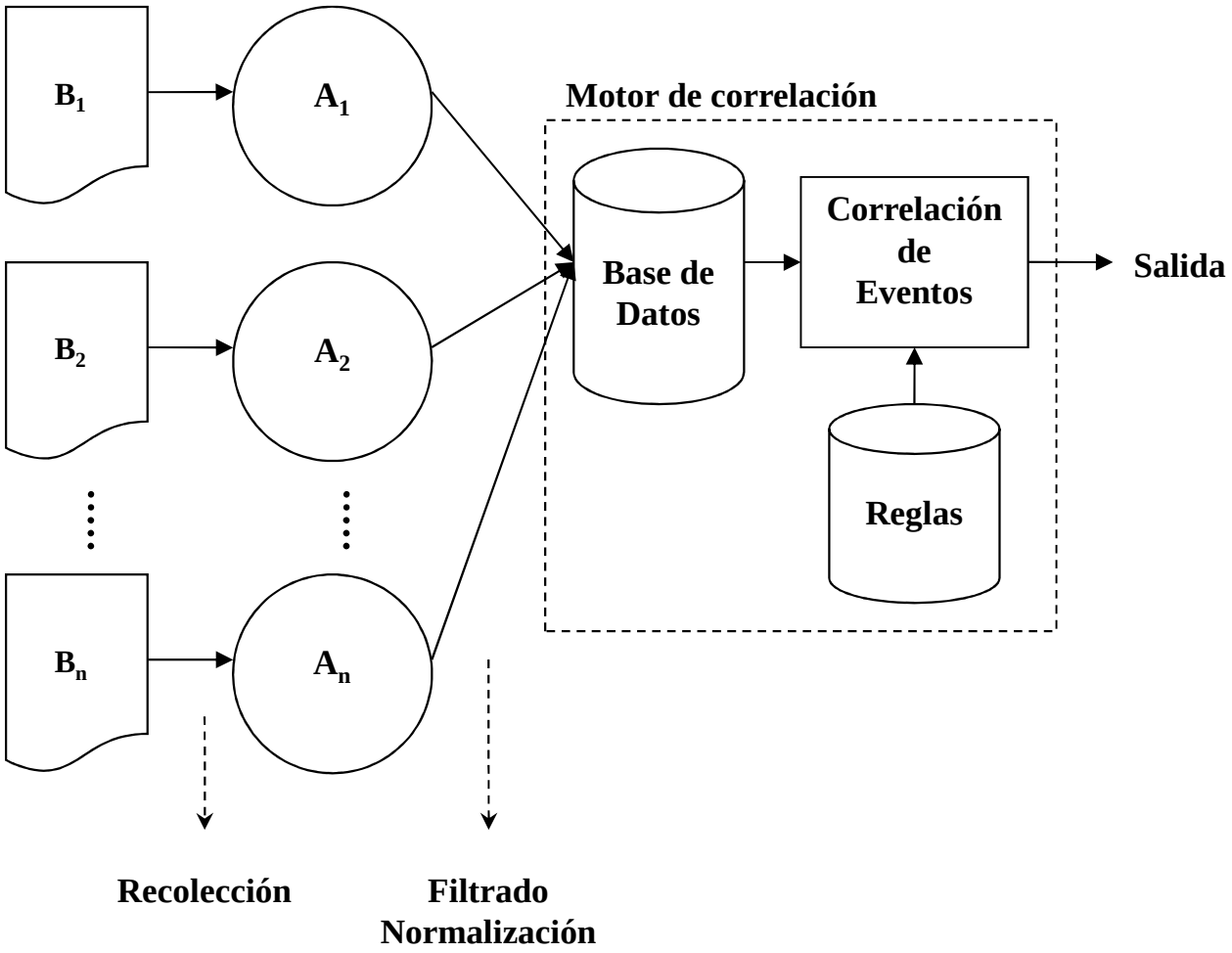
Tecnológico de Monterrey

Algunos aspectos a considerar

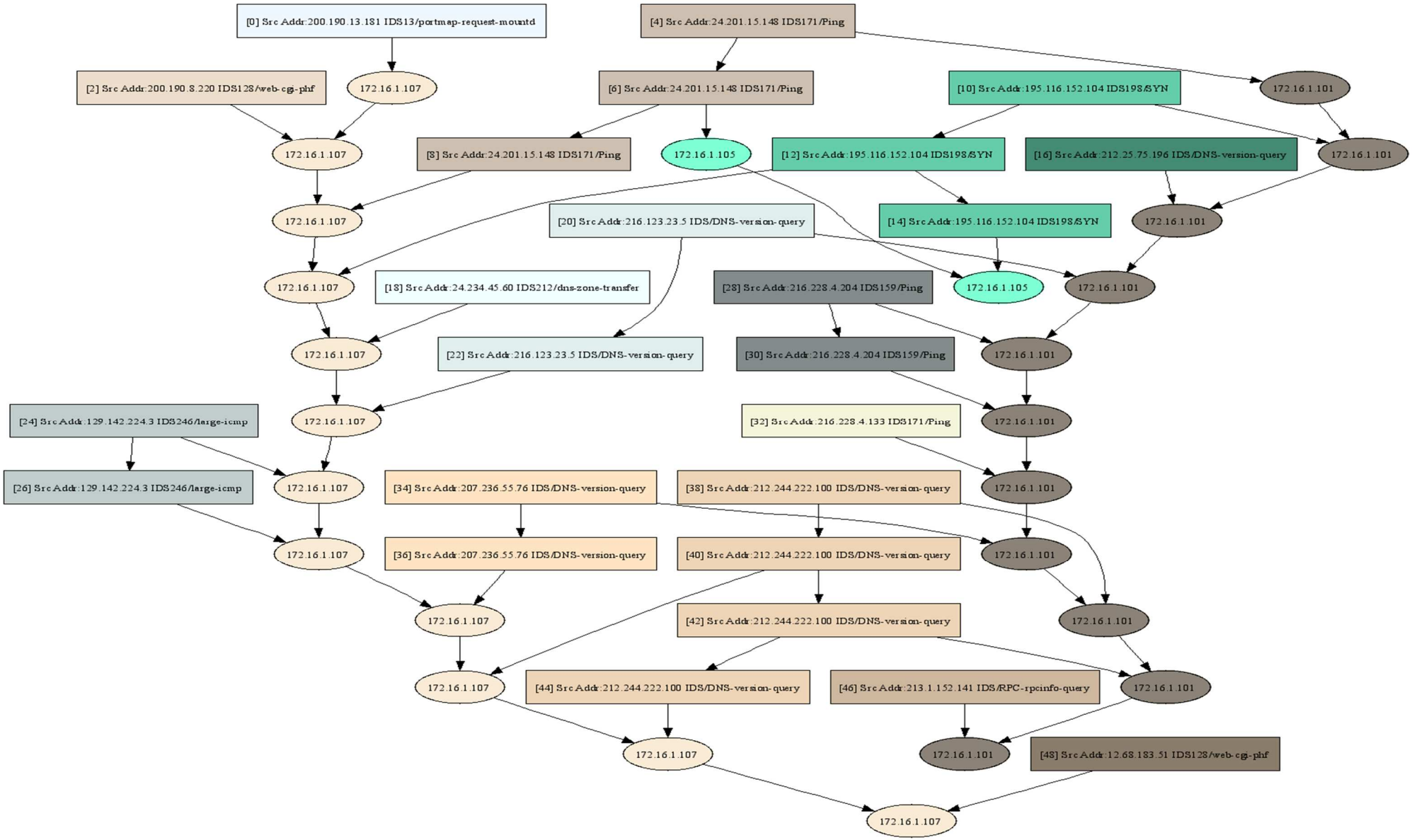
- Es posible configurar los sistemas de tal forma que los eventos:
  - Se escriban en uno o en distintos archivos,
  - Se envíen a través de la red a otra computadora,
  - Se transmitan a algún dispositivo.
- Principales desventajas
  - Espacio disco
  - Desempeño del sistema
- Confidencialidad e integridad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

http://www.bipm.org/

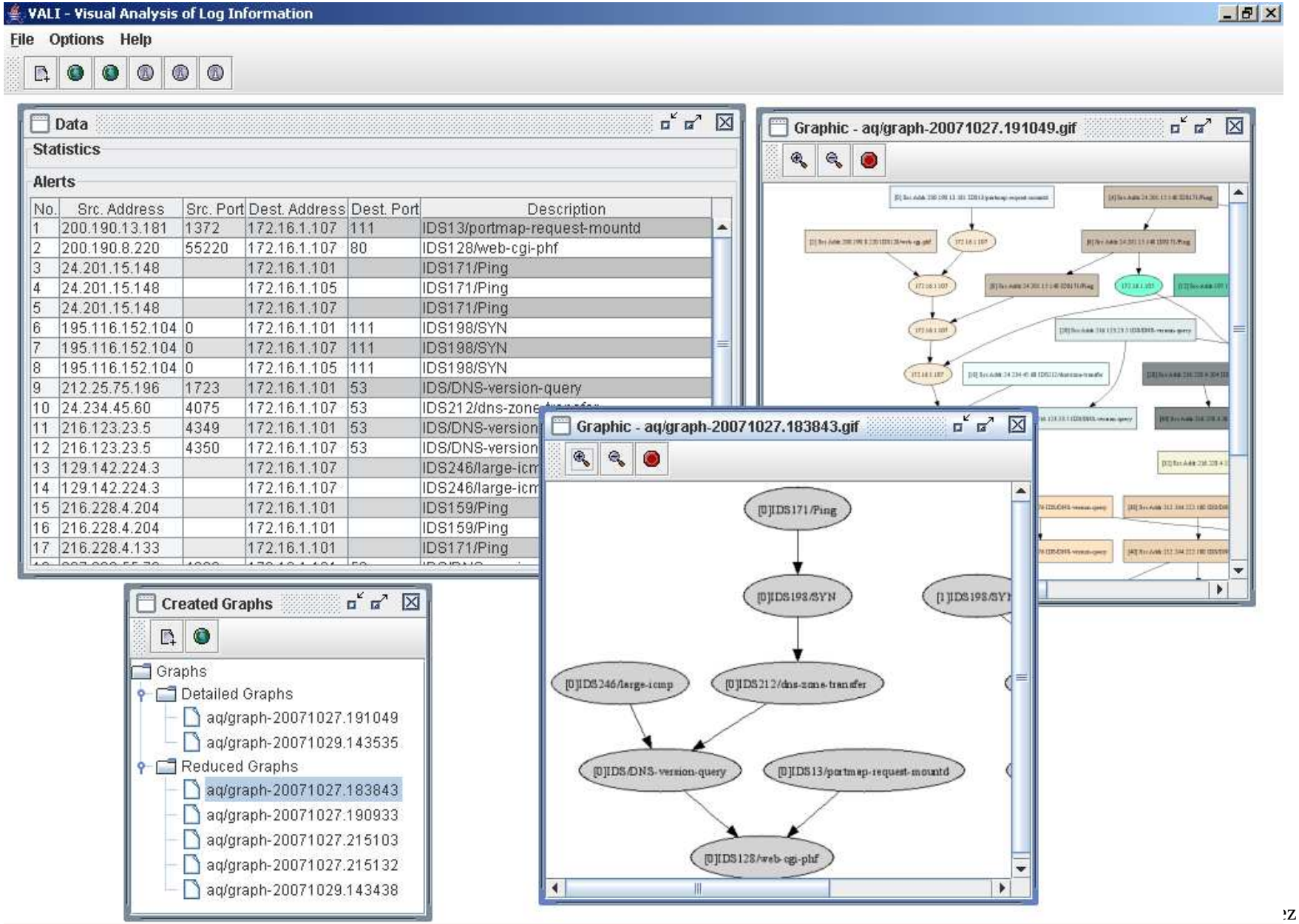
Uniendo todo



Visión gráfica de las bitácoras



El sistema VALI (Visual Analysis of Log Information)



Tecnológico de Monterrey

Los respaldos

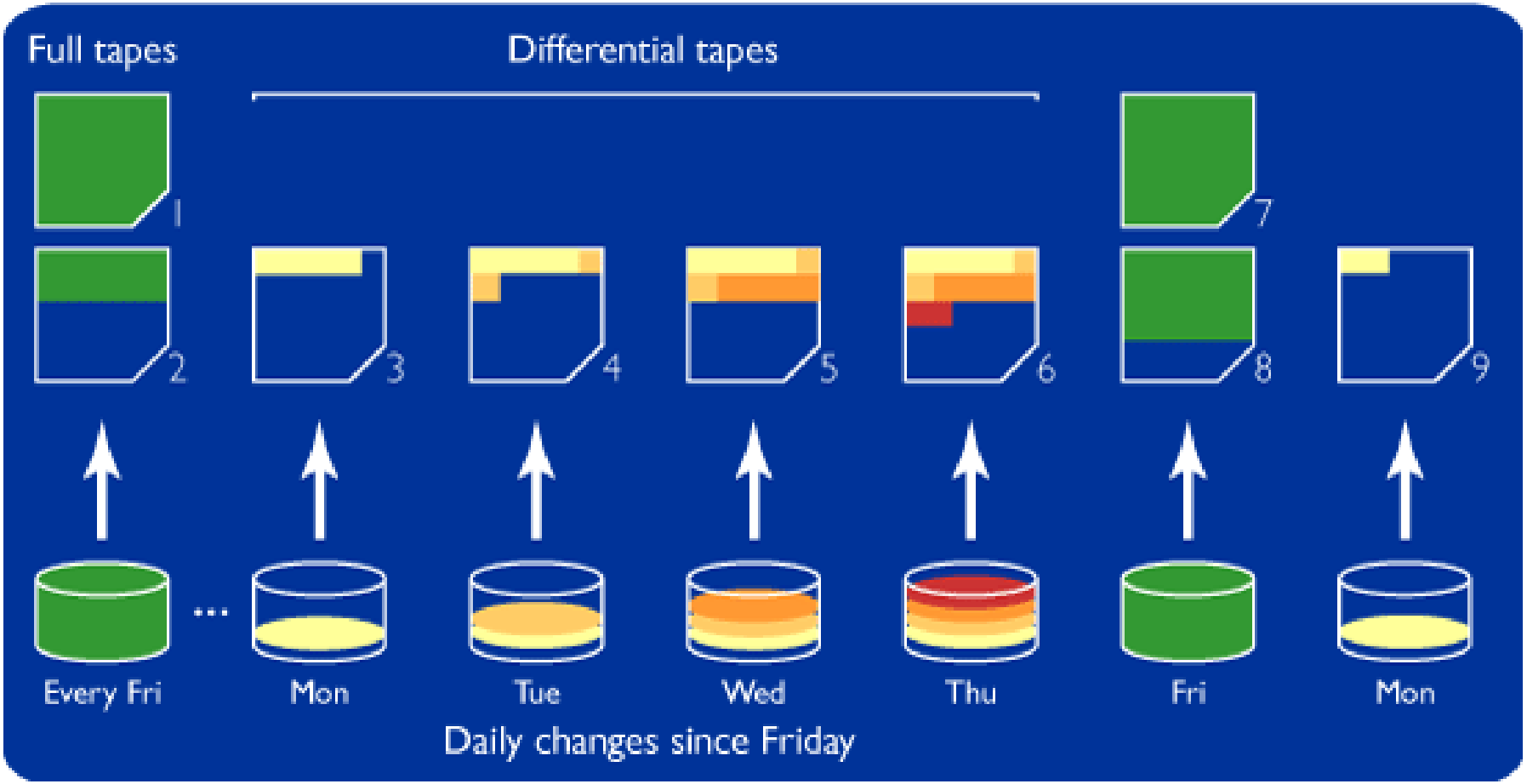
- Es una copia de los datos escrita en cinta u otro medio de almacenamiento duradero.
- De manera rutinaria se recuerda a los usuarios de computadoras que respalden su trabajo con frecuencia.
- Los administradores de sitios pueden tener la responsabilidad de respaldar docenas o incluso cientos de máquinas

Tecnológico de Monterrey

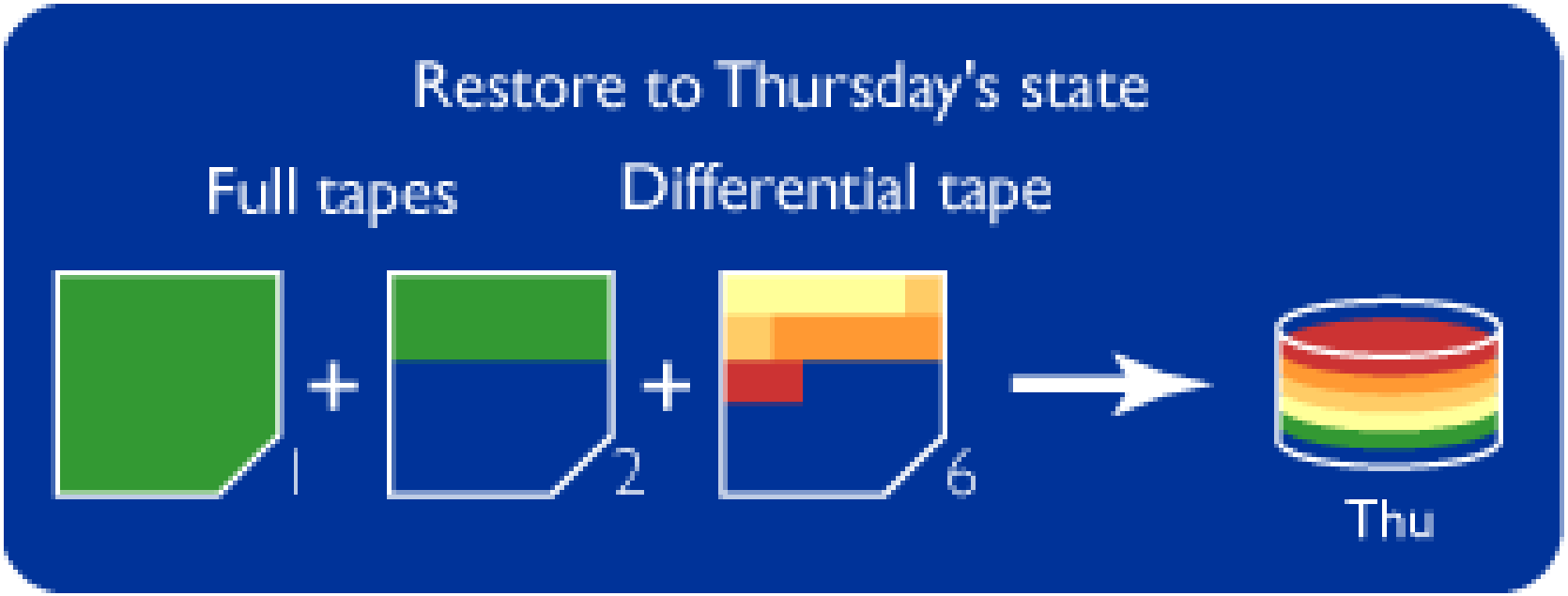
Tipos de respaldos

- 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.

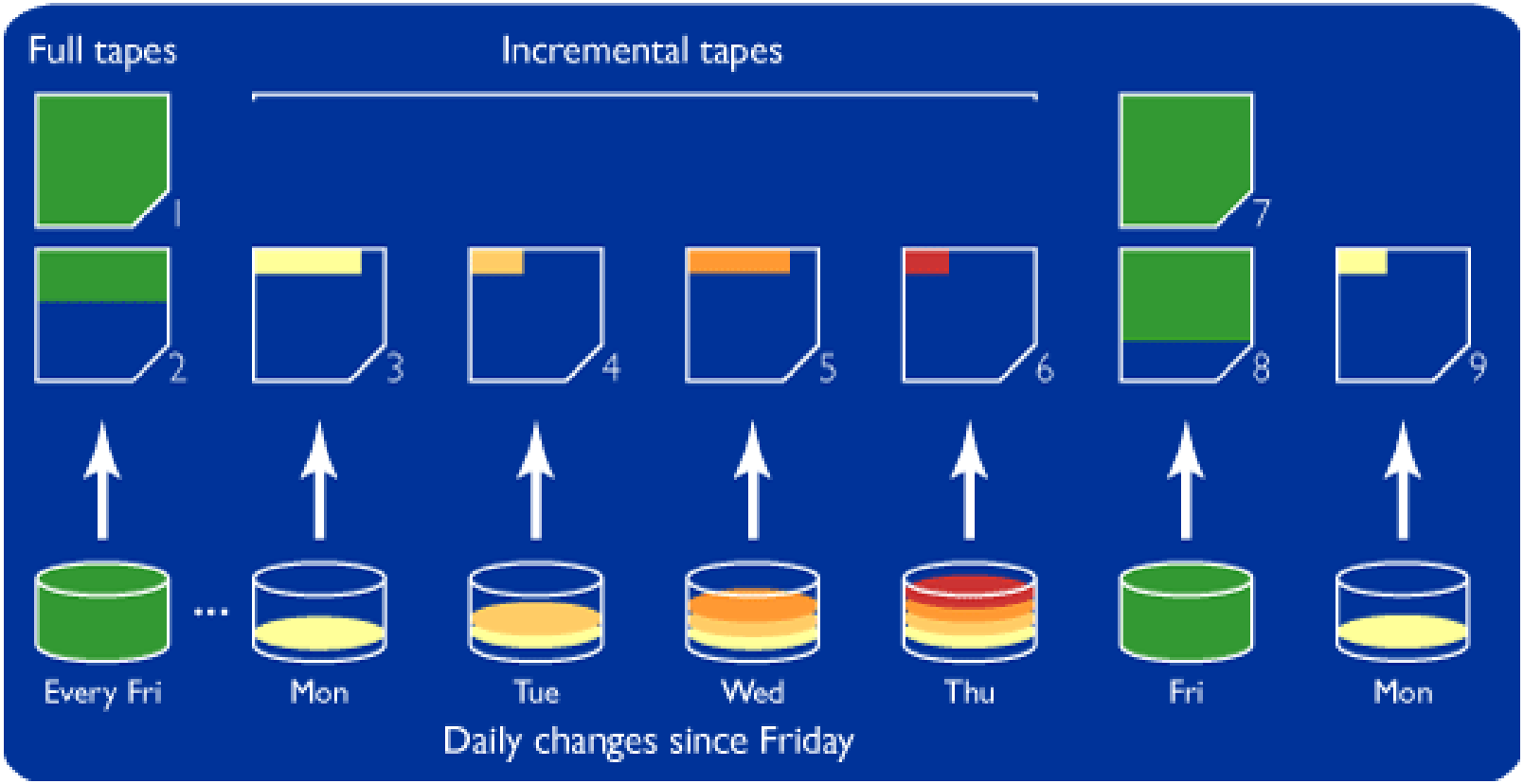
Ejemplos de respaldos completos y diferenciales.



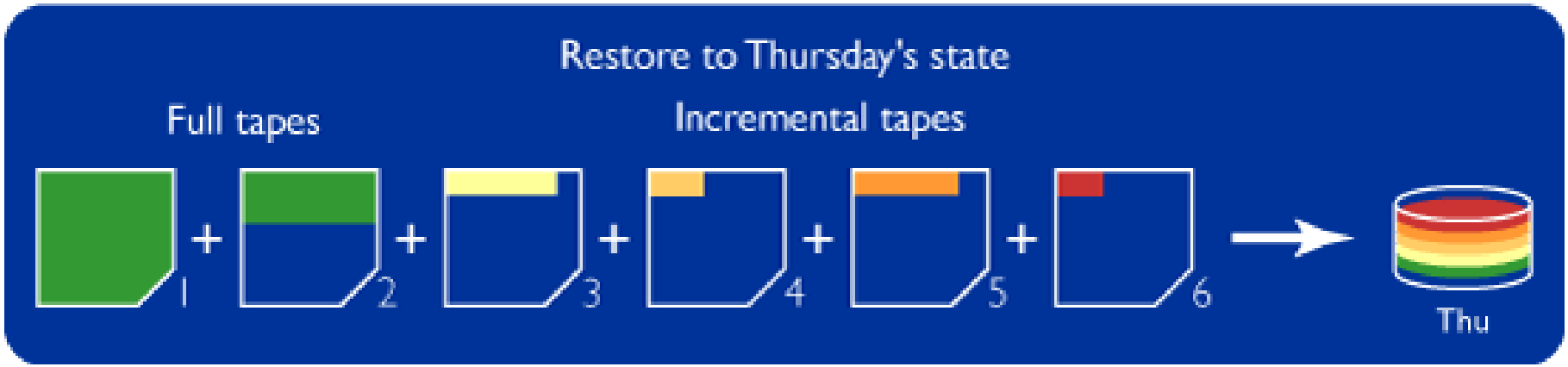
Ejemplo de una restauración diferencial



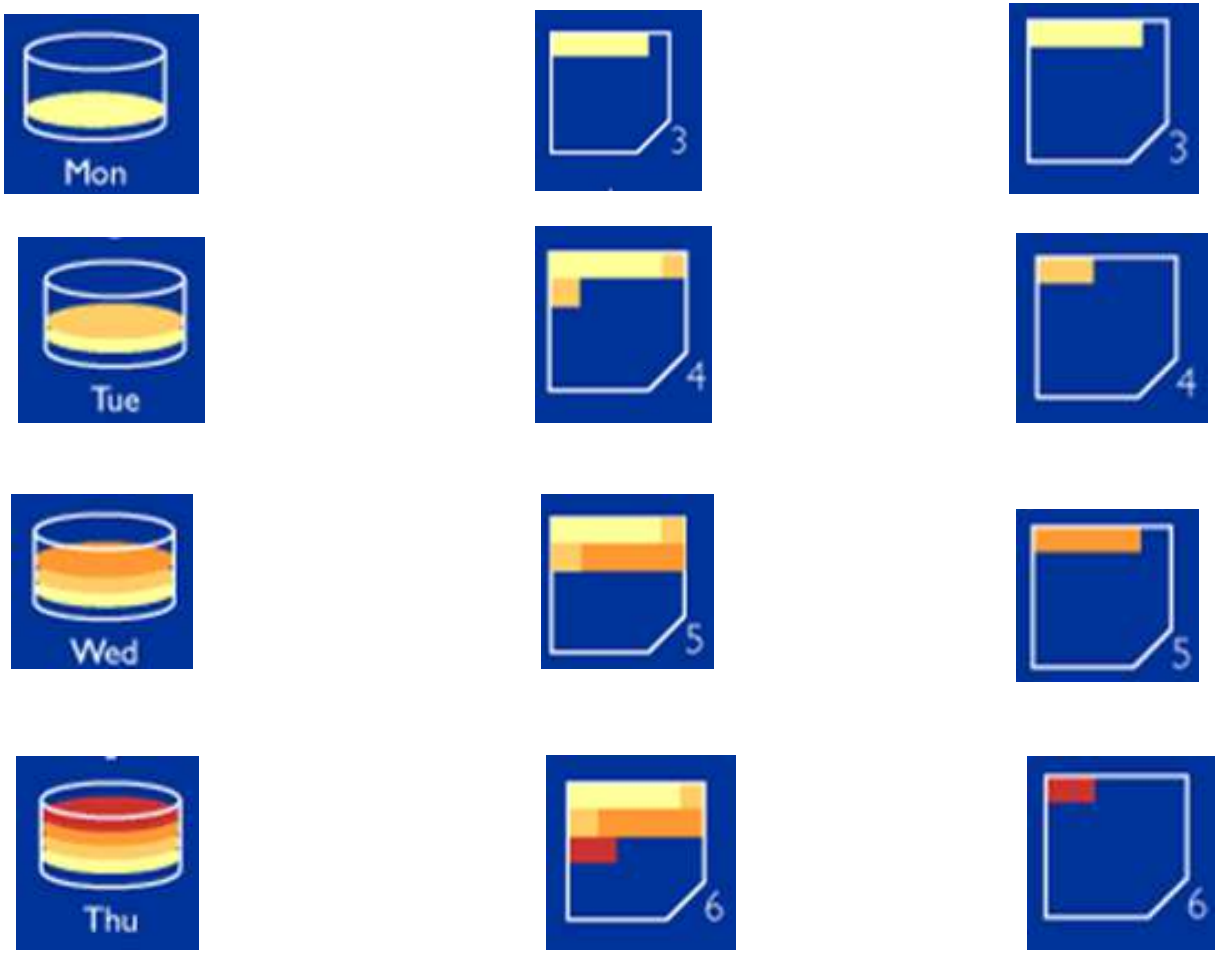
Ejemplo de un respaldo incremental



Ejemplo de un restablecimiento incremental



Diferencial vs incremental



Archivos modificados

Respaldo Diferencial

Respaldo Incremental

Tecnológico de Monterrey

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

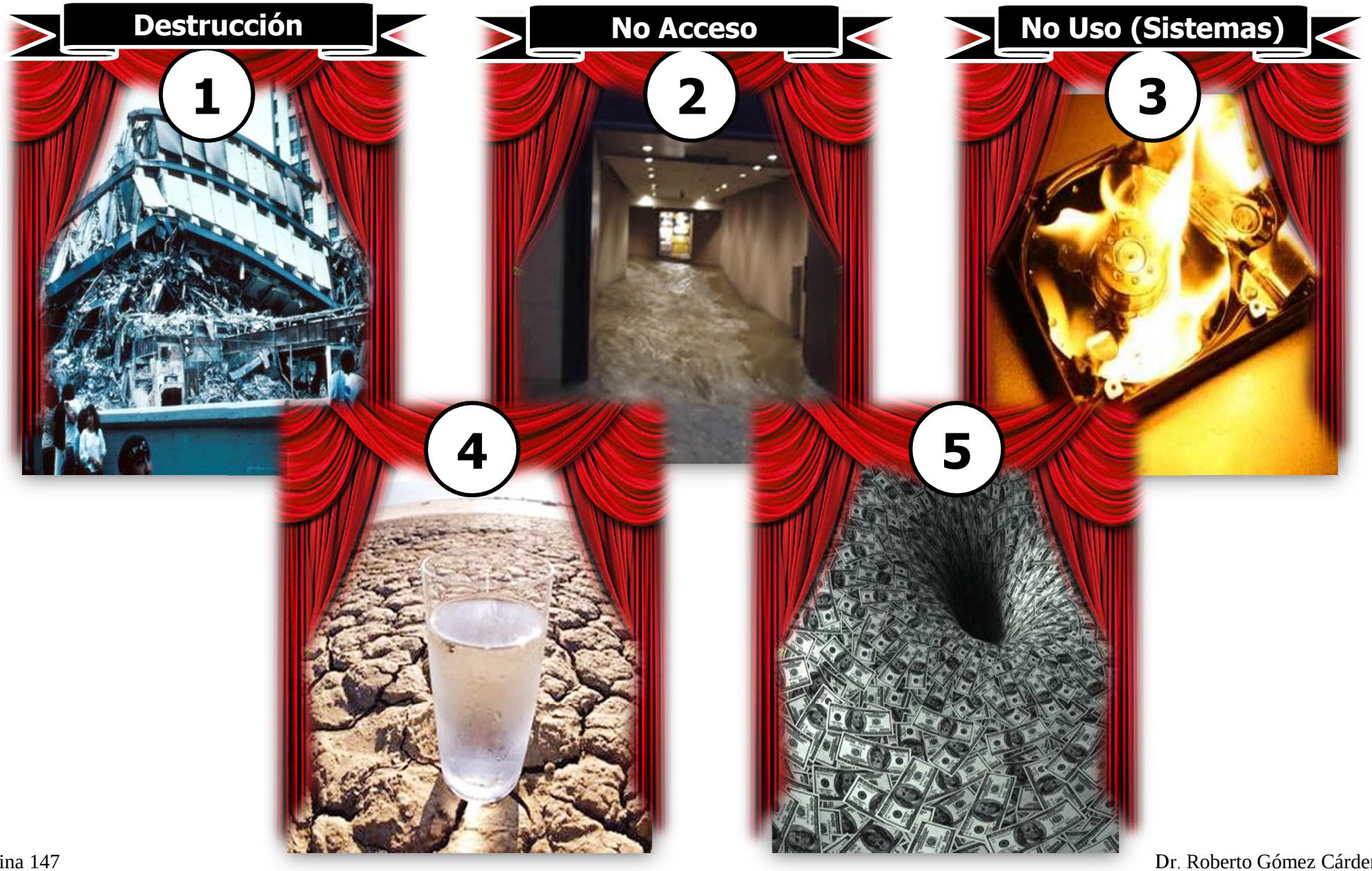
DRP y BCP

- 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.

¿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



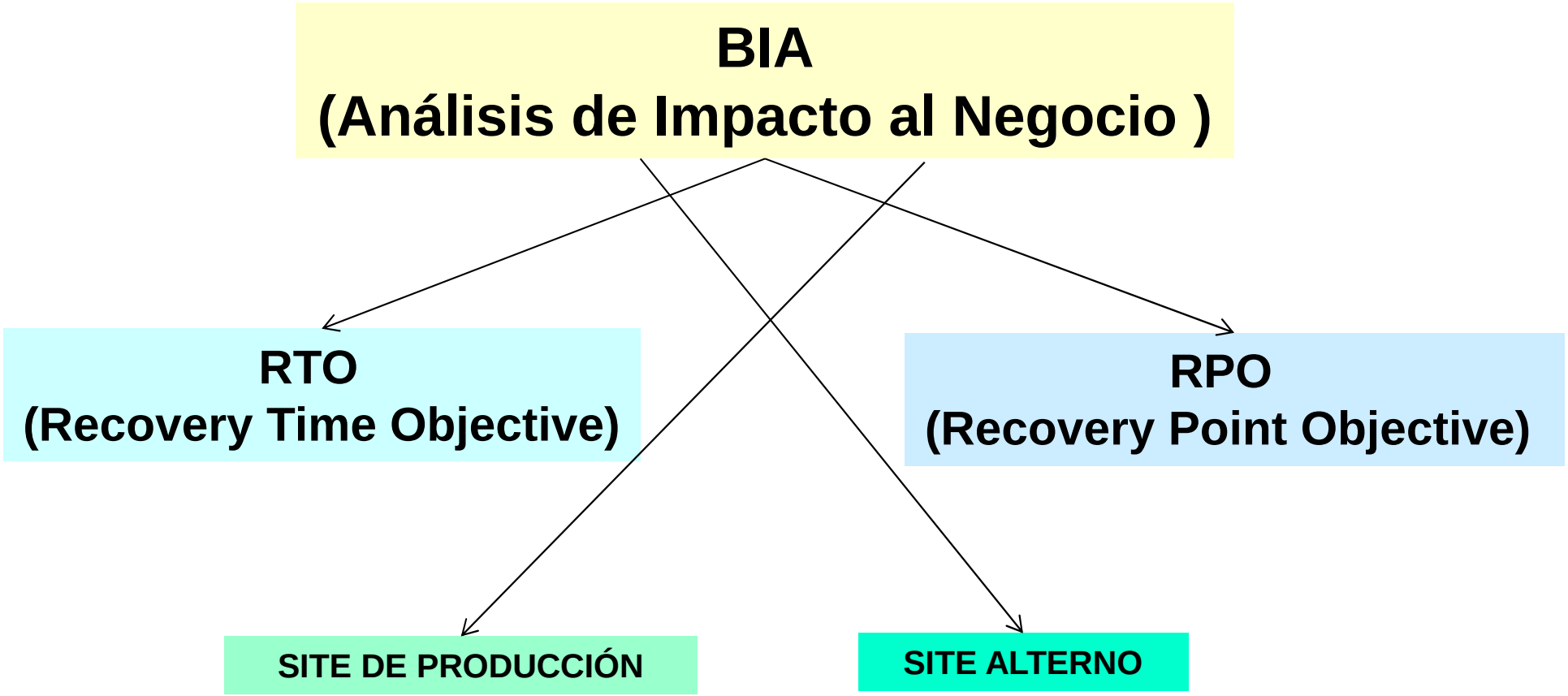
Tecnológico de Monterrey

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

Elementos BCP/DRP



Tecnológico de Monterrey

Site Producción

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

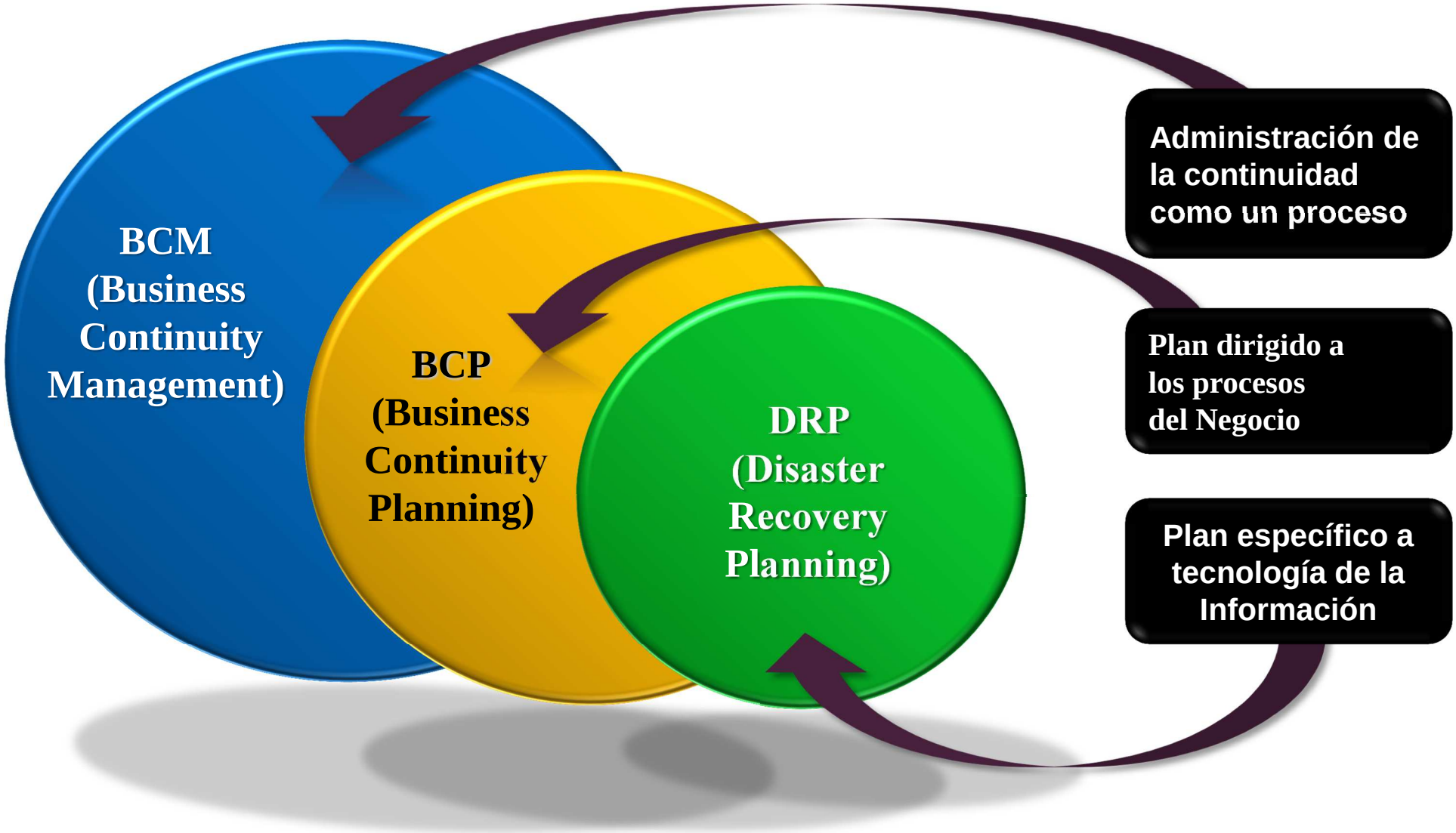
- Una sala o instalación de cómputo alterna con acondicionamiento eléctrico y ambiental la cual tiene preinstalado algún equipo periférico e interfaces de comunicaciones mas no el procesador central o servidores, los cuales, normalmente son los equipos más caros y que son indispensables para poder realizar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

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

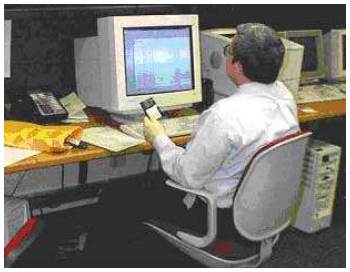
El computo forense

- 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

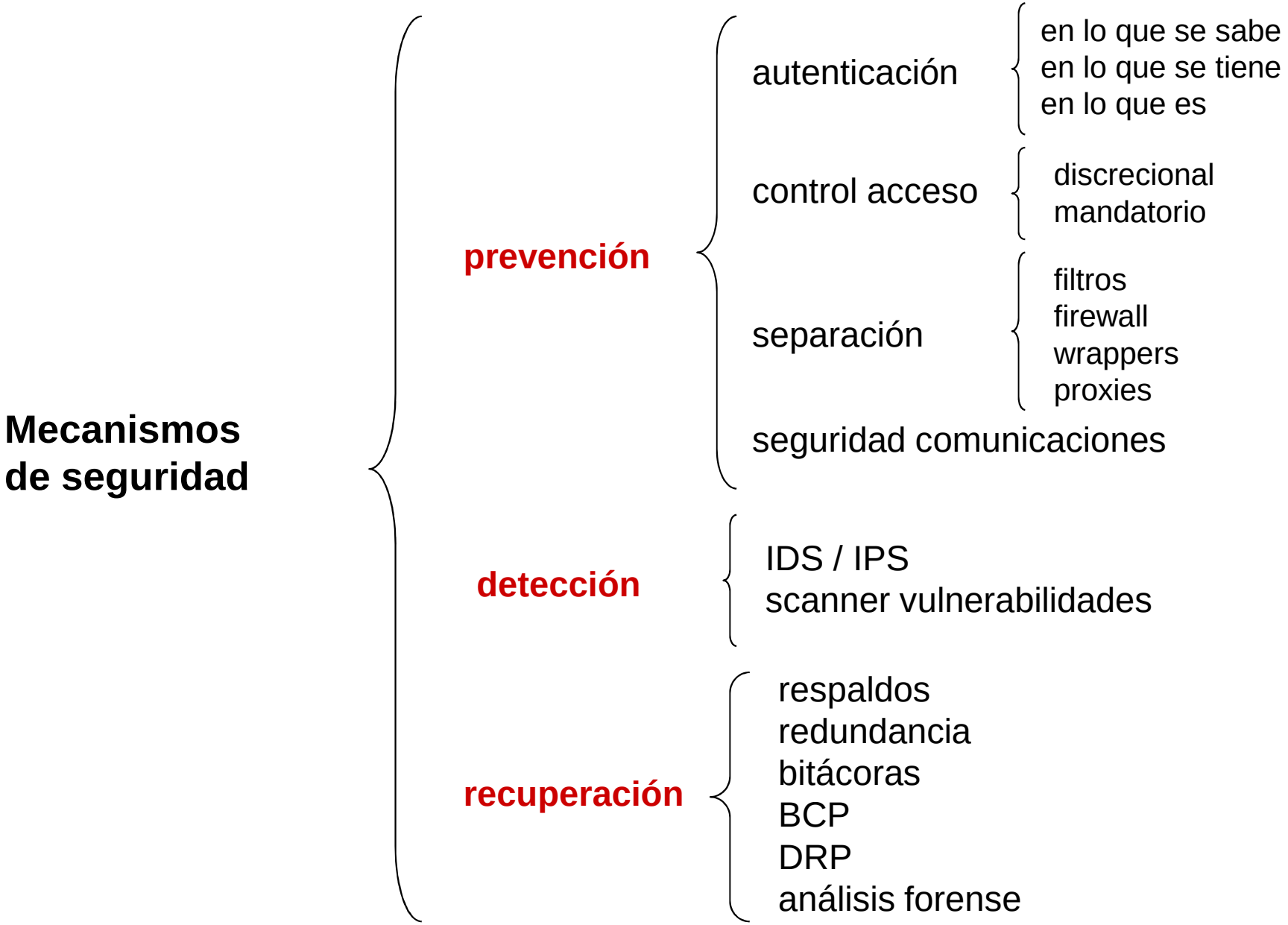
Preservar evidencia



Analizar evidencia

Presentar evidencia

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)

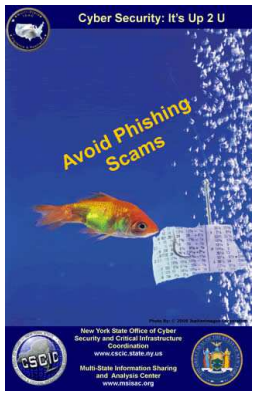
Awareness (Sensibilización)

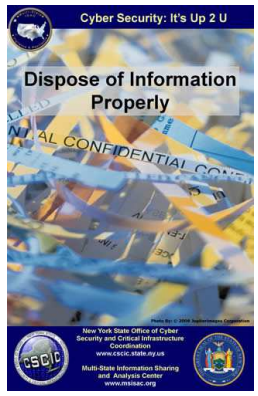
- Todas las partes deben poder conocer las medidas de seguridad, practicas y procedimientos.
- Una motivación para este principio es forzar la confianza en los sistemas de información.

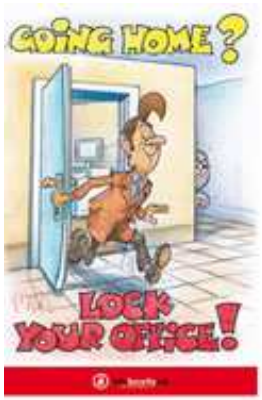
Ejemplos awareness

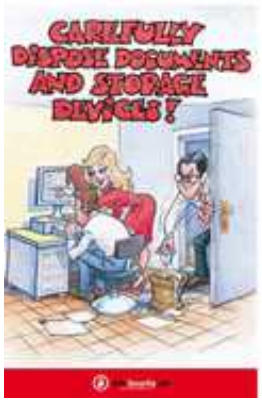
Tips de Seguridad para el uso de Internet

- **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

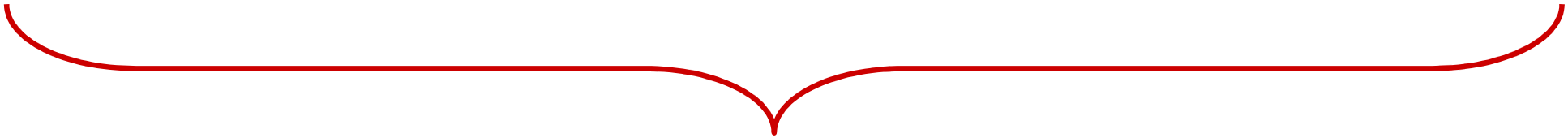
- Authentication, authorization, y accounting
  - consiste de un framewok que proporciona los tres servicios
- El objetivo del grupo de trabajo AAA es definir un protocolo que implemente autenticación, autorización y accounting lo suficientemente general para ser usado en aplicaciones diferentes.
- Definición 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