Tecnológico de Monterrey

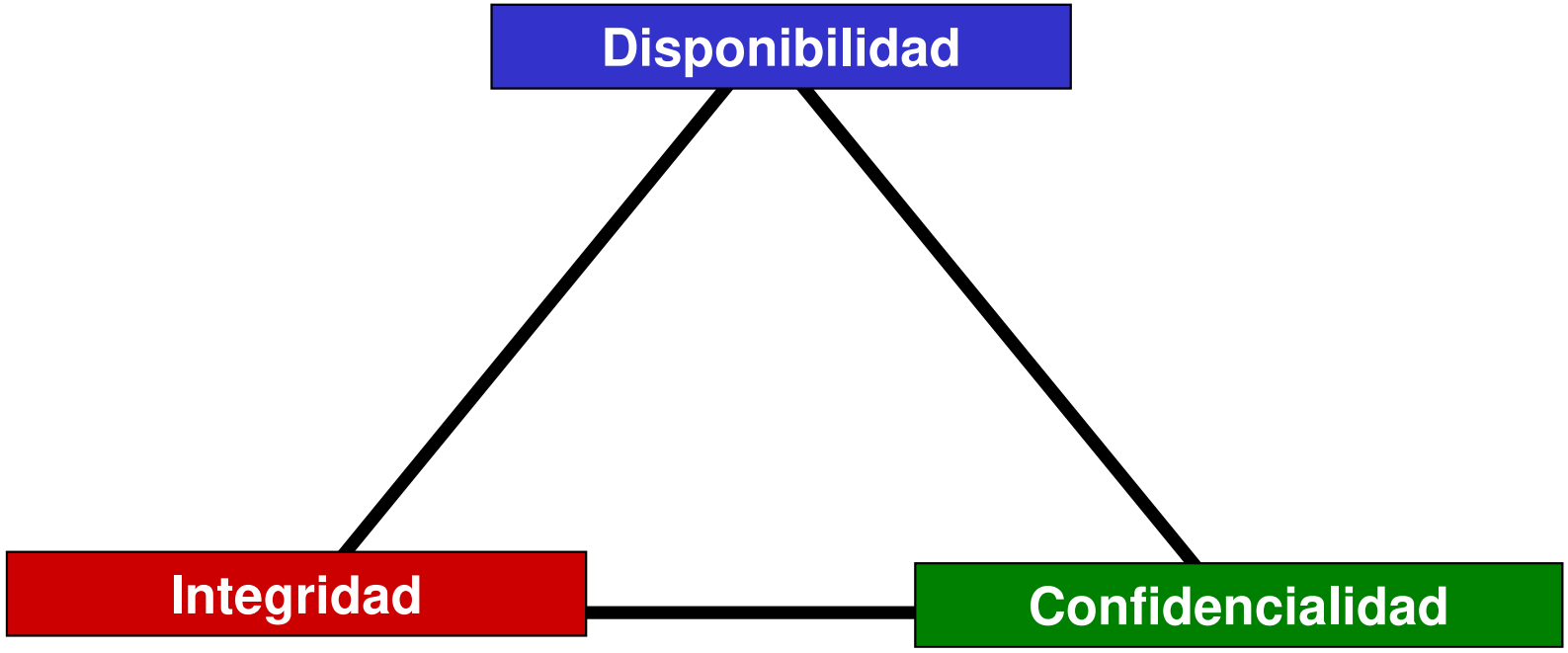
Conceptos Base, Análisis de Riesgos, Políticas, Procedimientos y SLAs

Roberto Gómez Cárdenas
rogomez@itesm.mx
http://cryptomex.org
@cryptomex

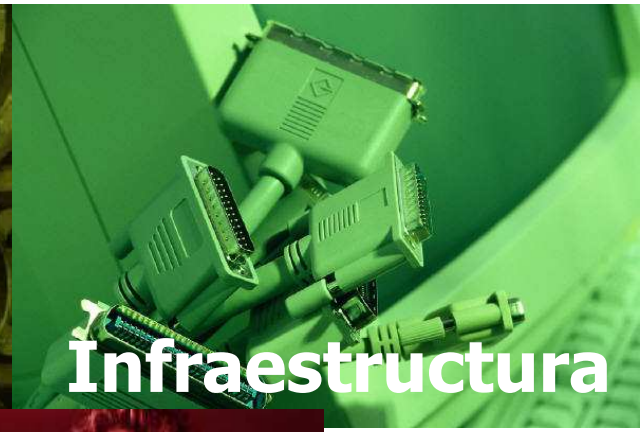
Tecnológico de Monterrey

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

Tecnológico de Monterrey

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.

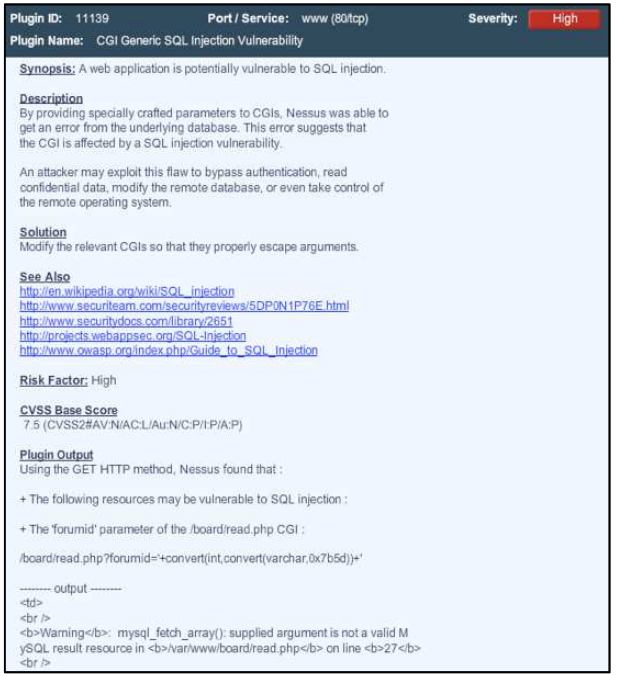
Tecnológico de Monterrey

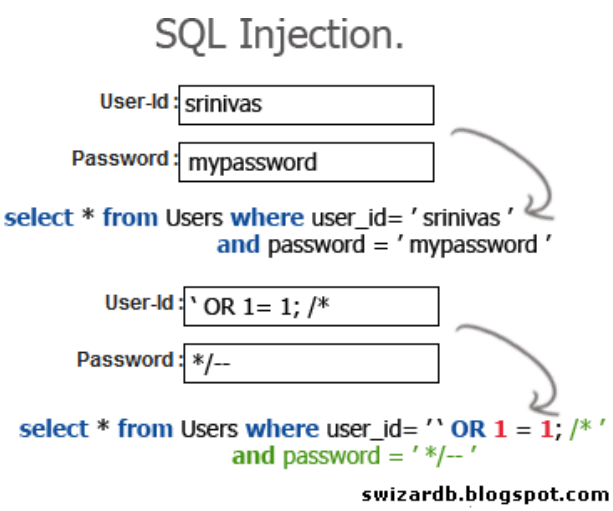
Vulnerabilidad

- 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

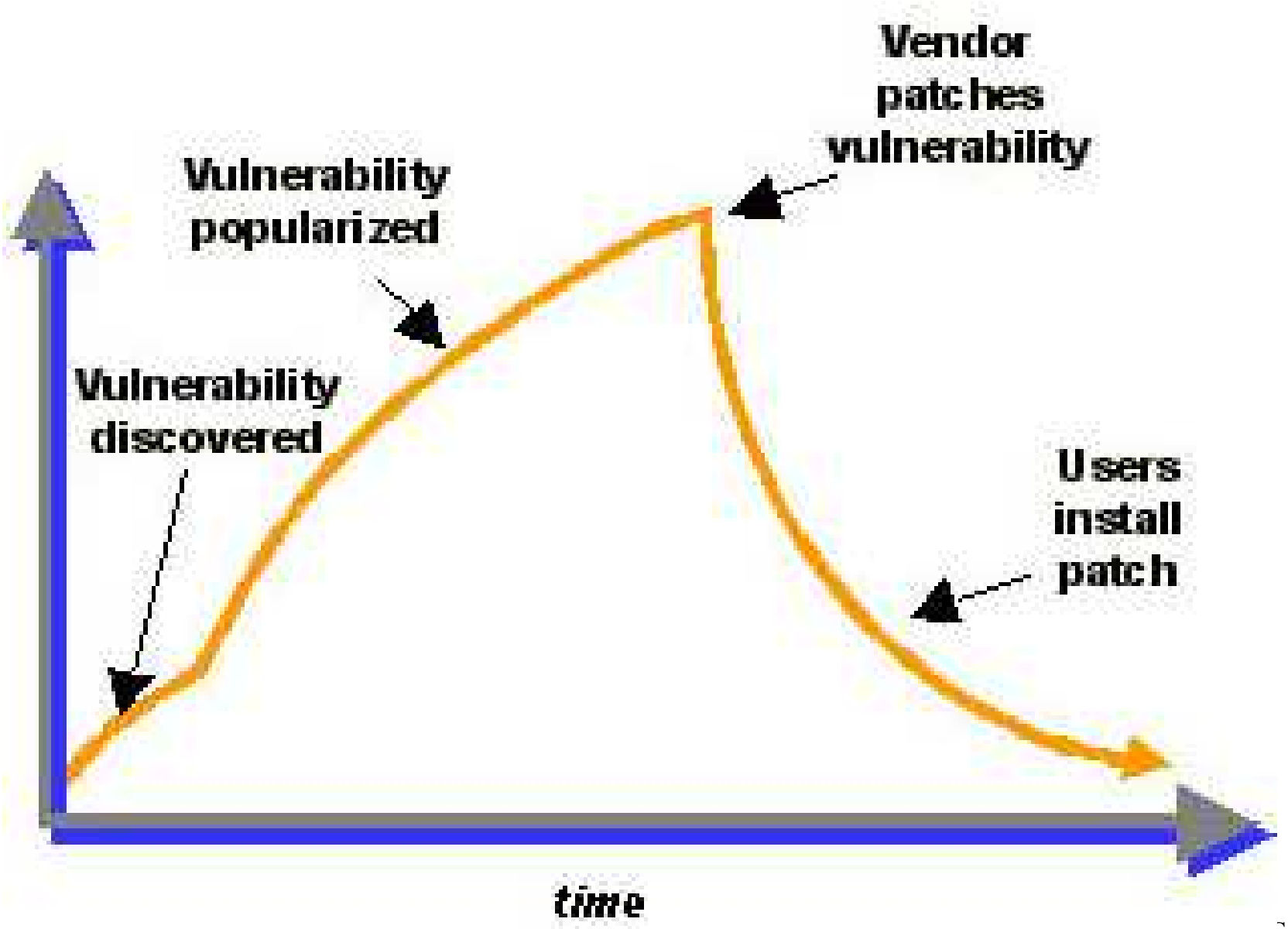
- Cuentas de usuarios sin contraseña.
- El personal externo no registra su entrada y salida a las instalaciones.
- Falta de lineamientos para la construcción de contraseñas.
- No contar con un plan de recuperación de desastres.
- Un programa que no valida los datos que introduce un usuario.





Tecnológico de Monterrey

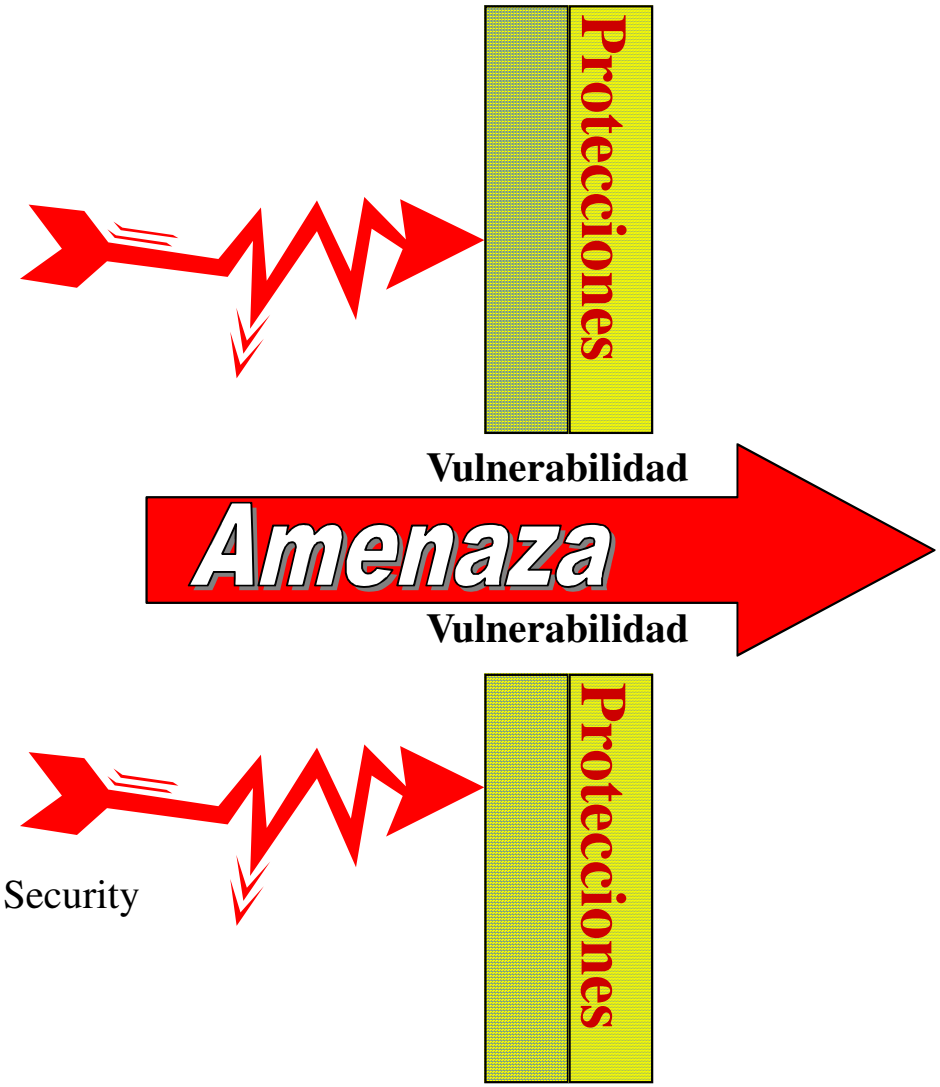
Tiempo vida vulnerabilidad



Common Vulnerabilities and Exposures: CVE

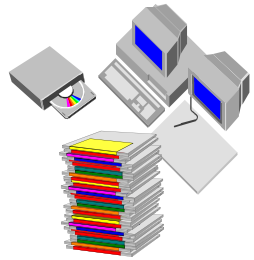
- Diccionario de nombres comunes (identificadores CVE) de vulnerabilidades conocidas públicamente.
- CCE: Commun Configuration Enumeration proporciona identificadores para aspectos de configuraciones de seguridad.
- Página: cve.mitre.org
- Otras referencias:
  - National Vulnerability Database
  - Open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

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

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

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

Tecnológico de Monterrey

Impacto

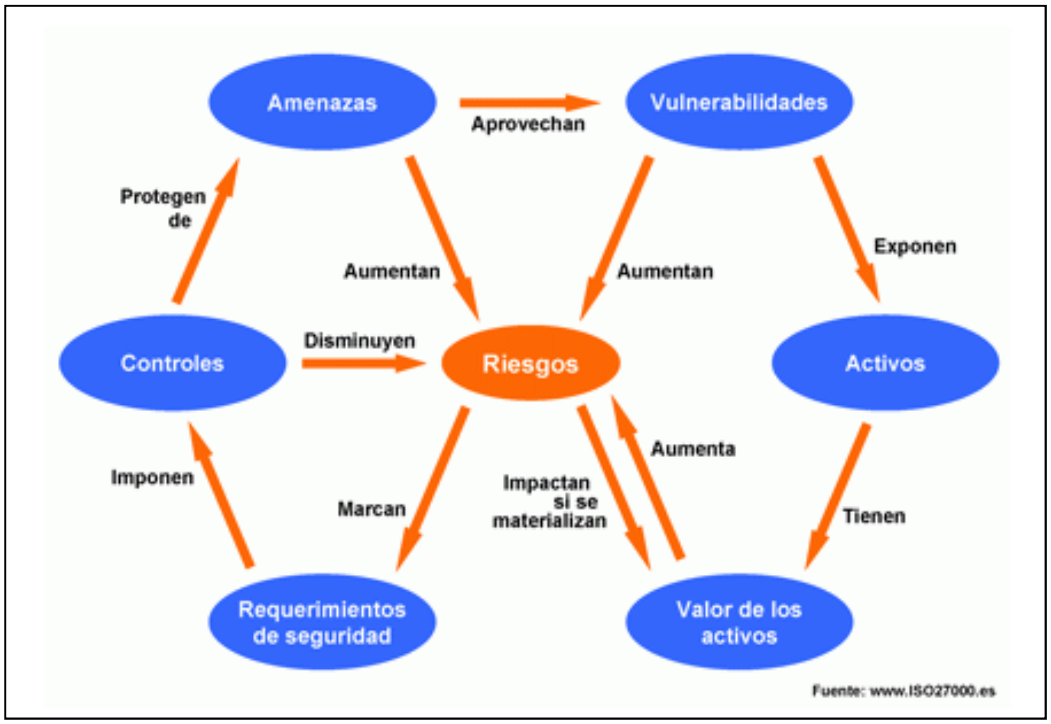
- Es la “materialización” de un riesgo.
- Una medida del grado de daño o cambio.
- Ejemplos
  - Retraso en la ejecución y conclusión de actividades de negocio.
  - Perdida de oportunidad y efectividad en la operación.
  - Falta de credibilidad frente a clientes.
  - Divulgación de información confidencial.

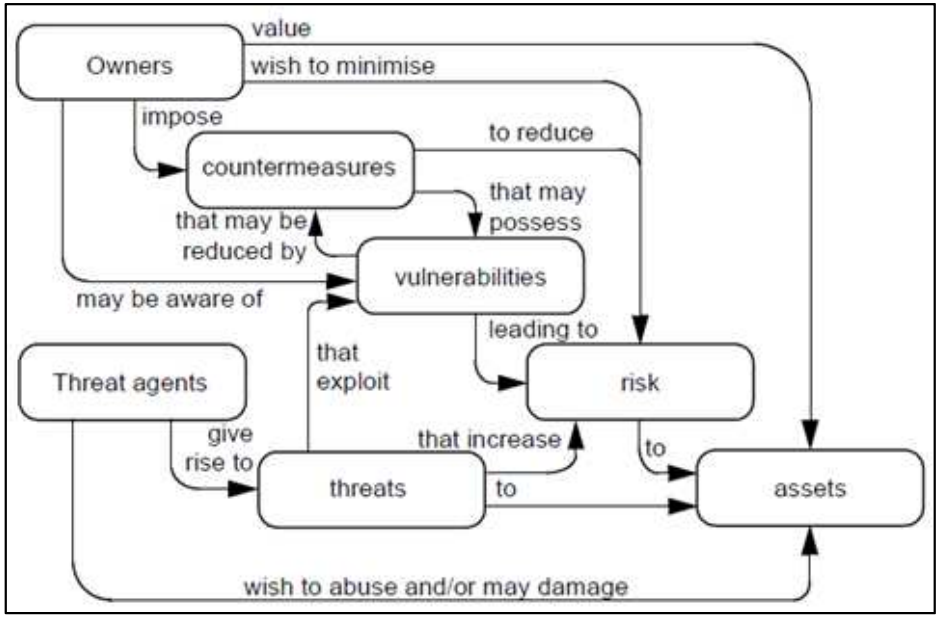
Tecnológico de Monterrey

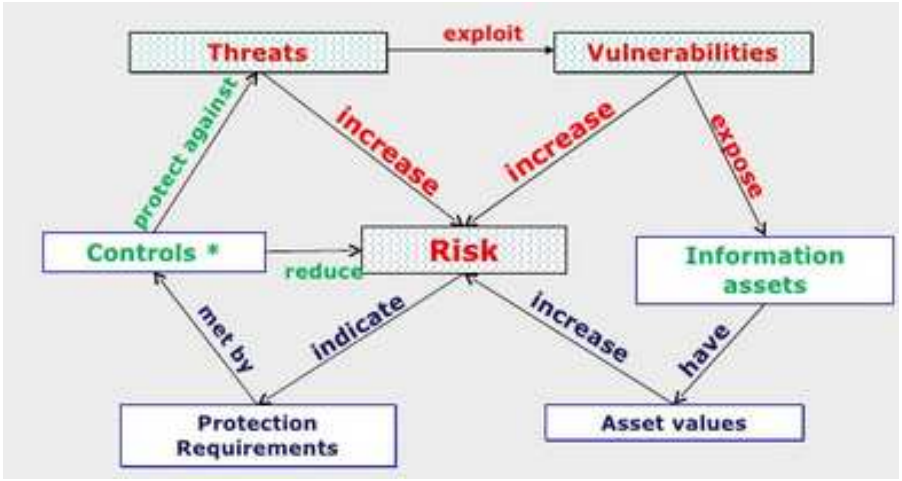
Control

- 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

Interacción de todos los conceptos





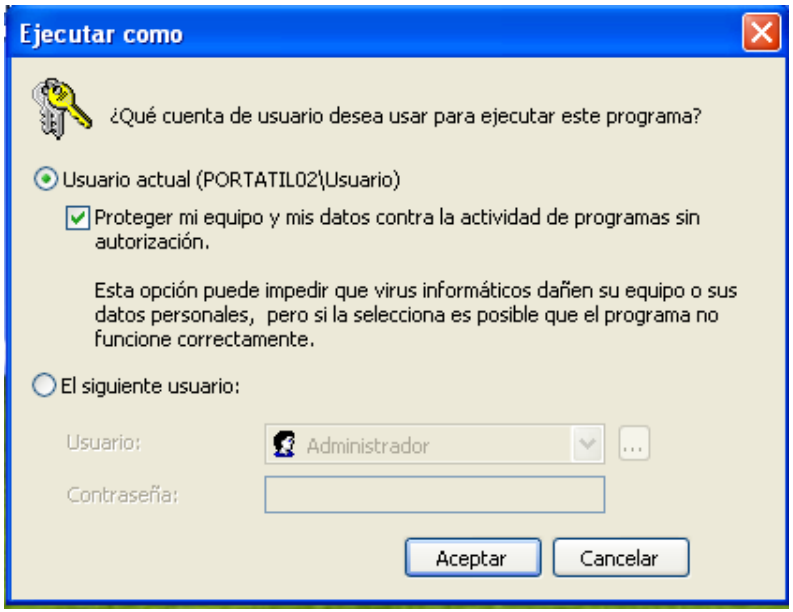


Propietarios, custodio y usuario

- 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.

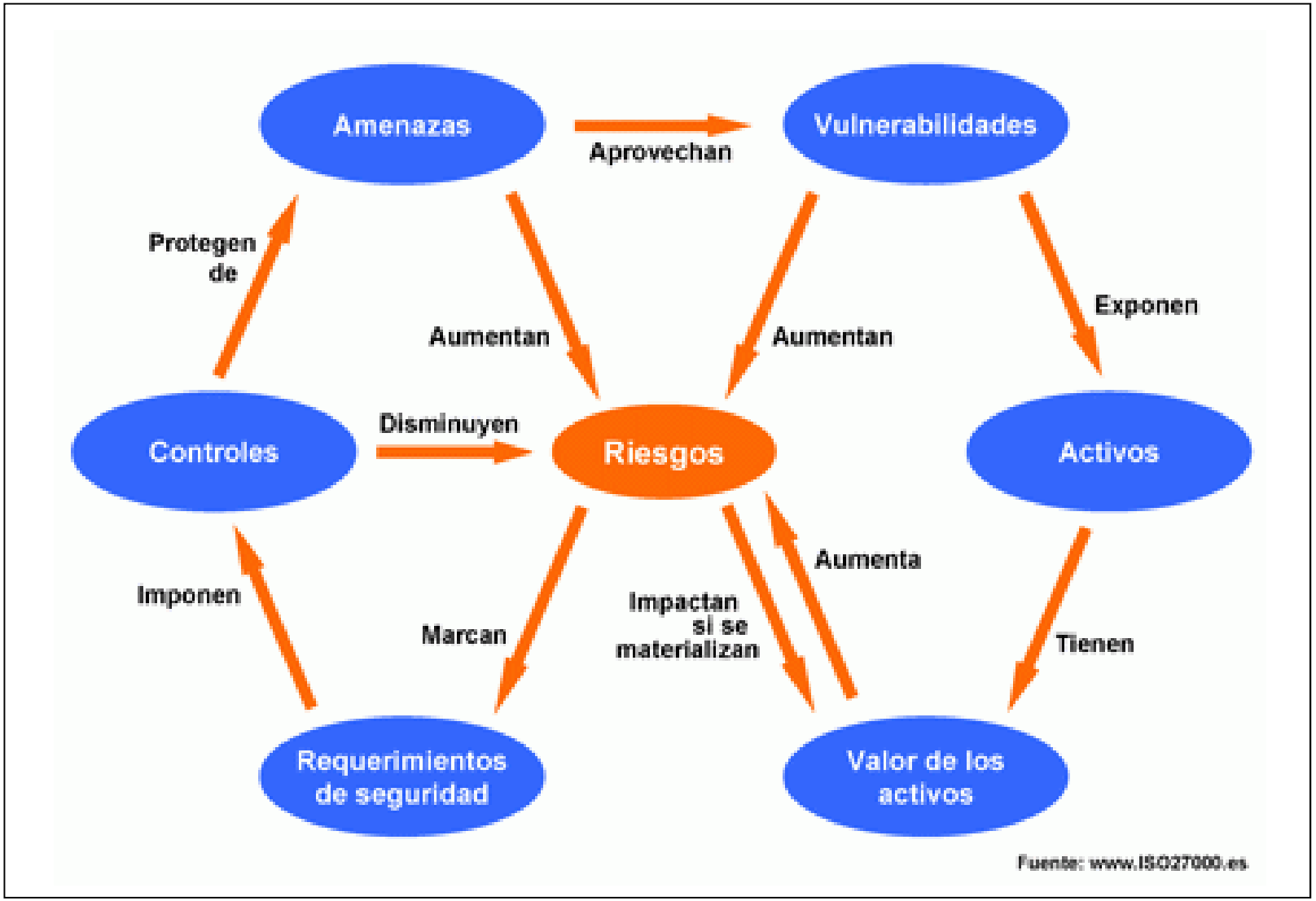
El concepto de mínimo privilegio

- 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



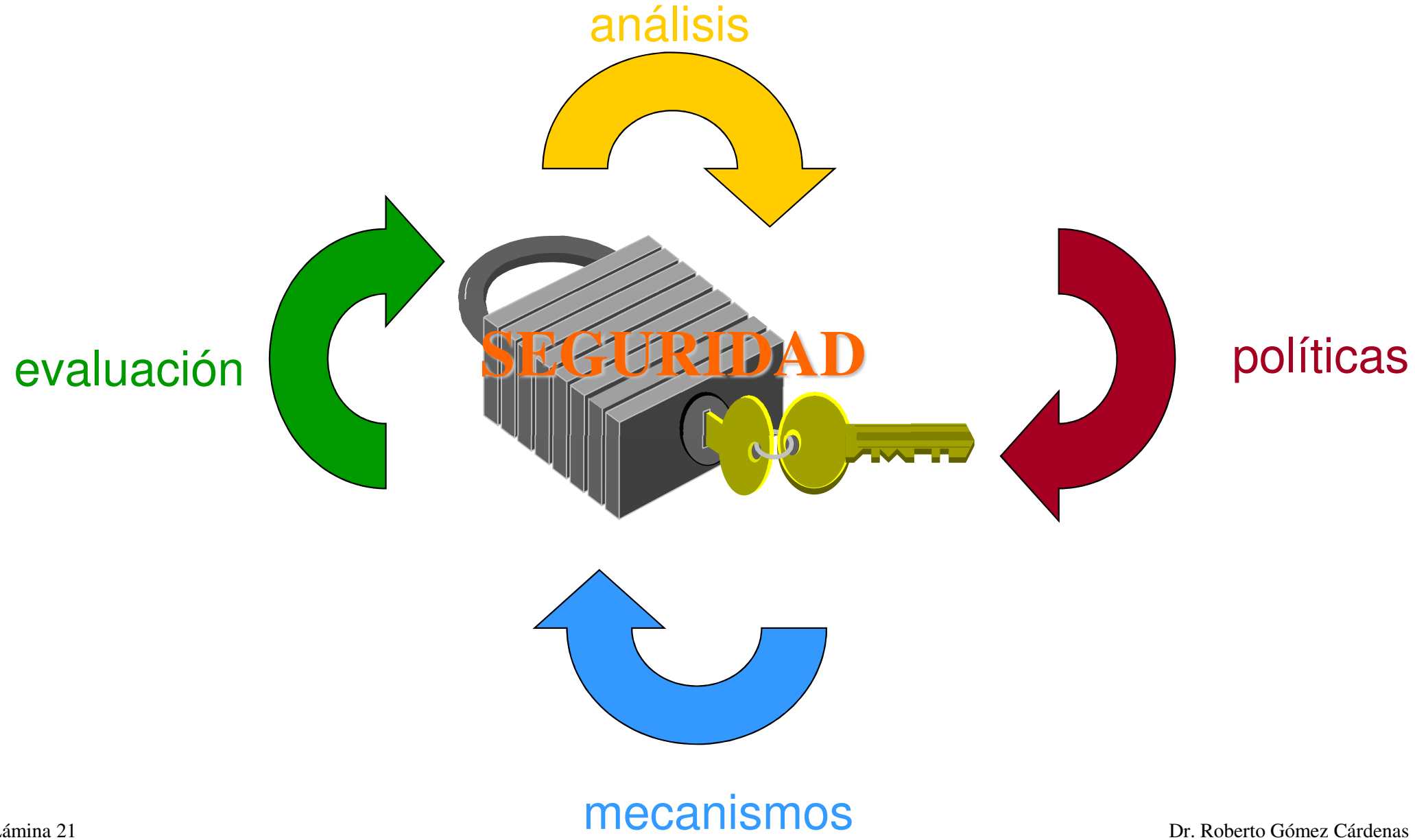
Tecnológico de Monterrey

Resumiendo



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
  - 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

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

Tecnológico de Monterrey

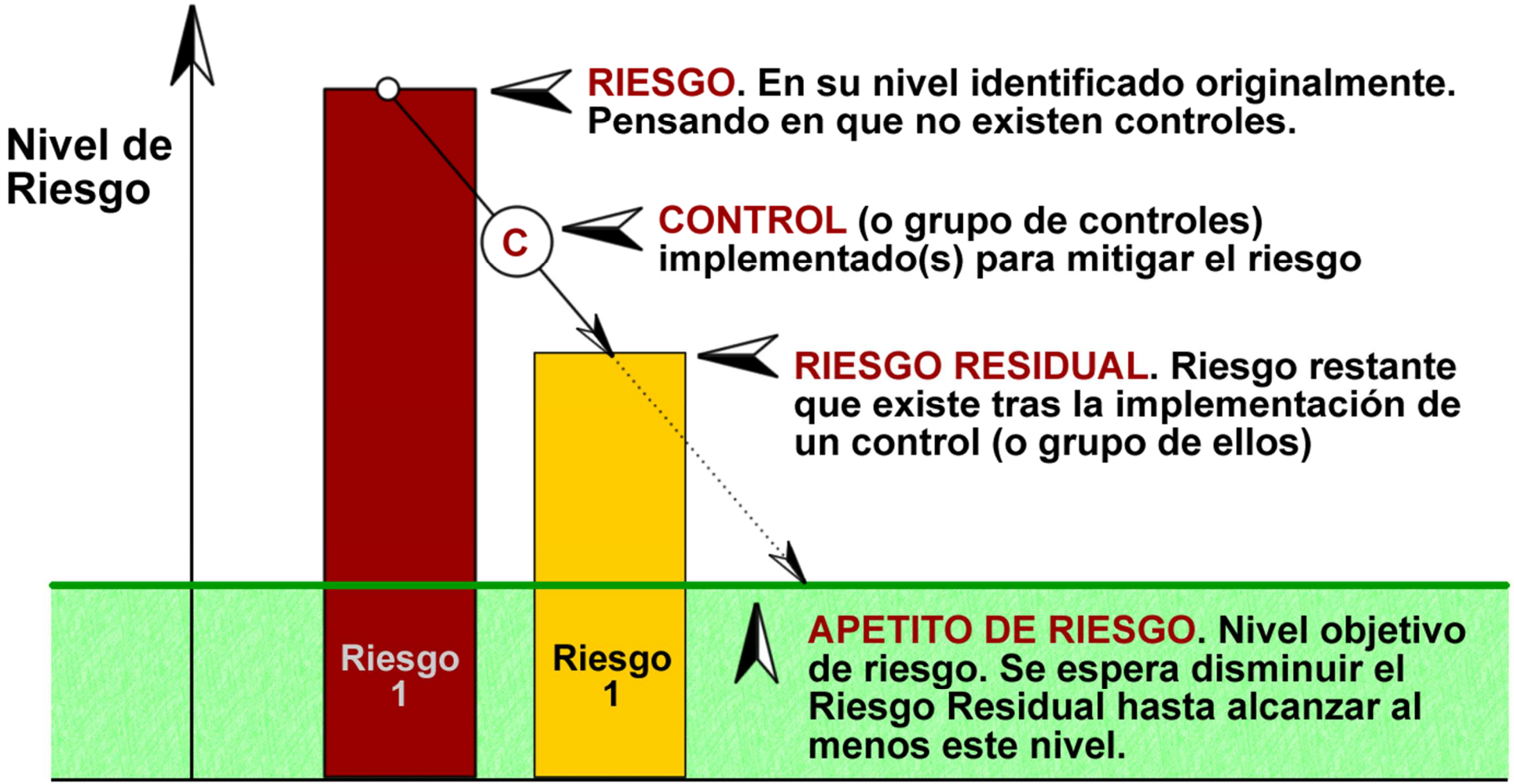
Definiciones base

Riesgo = (Impacto) x (Probabilidad de Ocurrencia)

Riesgo Residual = Riesgo – Control

Apetito de Riesgo = Máximo Riesgo Permitido
(Objetivo a donde se dirige el Riesgo Residual)

Niveles de riesgo



Tipos análisis riesgo

- Análisis riesgo cuantitativo
- Análisis riesgo cualitativo

Tecnológico de Monterrey

Enfoque Cuantitativo

- Asigna números reales y significativos a todos los elementos del riesgo
- Incluyen el valor del activo, el impacto, la frecuencia de la amenaza, etc.
- Proporciona porcentajes de probabilidad concretos para determinar la probabilidad de amenazas.
- El análisis de riesgo cuantitativo es obsoleto e impráctico

Tecnológico de Monterrey

Enfoque Cuantitativo (Definiciones)

- Factor de Exposición (EF)
  - Porcentaje de perdida de los recursos causada por amenazas identificadas
- Expectativa de Perdida Individual (SLE)
  - Valor del Recurso X Factor de Exposición
- Índice de Ocurrencia Anualizado (ARO)
  - Frecuencia estimada de que una amenaza ocurra en un año.
- Expectativa de Perdida Anualizada (ALE)
  - Expectativa de perdida Individual X Indice de Ocurrencia Anualizado

Tecnológico de Monterrey

Enfoque Cuantitativo

Recurso	Amenaza	Valor del recurso	Expectativa de perdida individual (SLE)	Frecuencia anualizada	Expectativa de perdida anualizada (ALE)
Instalación	Incendio	$560,000	$ 230,000	.25	$57,500
Secreto comercial	Robado	$43,500	$40,000	.75	$ 30,000
Servidor de archivos	Falla	$11,500	$11,500	.5	$5,750
Datos	Virus	$8,900	$6,500	.8	$5,200
Información de tarjetas de crédito del cliente	Robado	$323,500	$300,000	.65	$195,000

Tecnológico de Monterrey

Enfoque cualitativo

- No asigna números ni valores monetarios a los elementos del riesgo
- Se basan en diferentes escenarios de posibilidades de amenazas y su clasificación correspondiente
- Las técnicas del análisis cualitativo incluyen el juicio, la intuición y la experiencia
- Técnicas cualitativas:
  - Delphi, Brainstorming, Focus Groups, Encuestas, Cuestionarios, One-on-One Meetings

Tecnológico de Monterrey

Enfoque Cualitativo

AMENAZA = El acceso de un hacker a información confidencial	Severidad de la amenaza	Probabilidad de que la amenaza ocurra	Perdida potencial para la compañía	Efectividad del firewall	Efectividad del sistema de detección de intrusión	Efectividad del honeypot
Director IT	4	2	4	4	3	2
Administrador de bases de datos	4	4	4	3	4	1
Programador de la aplicación	2	3	3	4	2	1
Administrador del red	3	4	3	4	4	2
Administrador operacional	5	4	4	4	4	2
Resultados	3.6	3.4	3.6	3.8	3.0	1.4

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
- Análisis costo beneficio

Tecnológico de Monterrey

Pasos proyecto análisis riesgo

- Definir alcance
- Definir equipo
- Identificar amenazas
- Priorizar amenazas
- Impacto de la amenaza
- Determinar factor de riesgo
- Identificar controles

Tecnológico de Monterrey

Ejemplo lista amenazas

Natural	Technological	Human-caused
▪ Avalanche ▪ Animal disease outbreak ▪ Drought ▪ Earthquake ▪ Epidemic ▪ Flood ▪ Hurricane ▪ Landslide ▪ Pandemic ▪ Tornado ▪ Tsunami ▪ Volcanic eruption ▪ Wildfire ▪ Winter storm	▪ Airplane crash ▪ Dam failure ▪ Levee failure ▪ Mine accident ▪ Hazardous materials release ▪ Power failure ▪ Radiological release ▪ Train derailment ▪ Urban conflagration	▪ Biological attack ▪ Chemical attack ▪ Cyber incident ▪ Explosives attack ▪ Radiological attack ▪ Sabotage ▪ School and workplace violence

Tecnológico de Monterrey

Amenazas Informáticas

- Catalogadas en nueve grupos
  1. Fraude
  2. Malware
  3. Ingeniería Social
  4. Información comprometida
  5. Amenazas tecnológicas
  6. Acciones no autorizadas
  7. Accesos no autorizados
  8. Errores u omisiones provocados por personas
  9. Suplantación de identidad

Tecnológico de Monterrey

Definición fraude

- RAE
  - Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete.
  - Acto tendente a eludir una disposición legal en perjuicio del Estado o de terceros.
  - Delito que comete el encargado de vigilar la ejecución de contratos públicos, o de algunos privados, confabulándose con la representación de los intereses opuestos.

Fraude informático/cibernético

- El fraude cibernético e informático se refiere al fraude realizado a través del uso de una computadora o del Internet.
- Uso de una computadora con el objetivo de distorsionar datos para inducir a otra persona a que haga o deje de hacer algo que ocasiona una pérdida.
- Importante diferenciar
  - Cyber-enable crimes
  - Cyber-dependenet crimes

Cyber-enabled vs Cyber-dependent

- Cyber-enabled crimes
  - Delitos tradicionales, que pueden incrementarse en su escala o llegar mediante el uso de computadoras, redes de computadoras u otras formas de información tecnología de las comunicaciones (ICT).
  - Se pueden llevar a cabo sin el uso de ICT.
  - Ejemplos
    - Fraudes financieros electrónicos, ventas fraudulentas a través de subastas en línea o sitios minoristas, fraudes de marketing masivo y estafas de consumidores, fraudes de romance en línea (o sitio de redes sociales / citas)
- Cyber –dependent crimes
  - Un sistema digital es el objetivo, así como los medios de ataque.
  - Estos incluyen ataques a sistemas informáticos para dañar la infraestructura de TI y robar datos a través de una red utilizando malware.

Ejemplo cyber-enabled

Capturan a banda que ofertaba autos por internet y mataba a compradores

Los presuntos asesinos ofertaban los vehículos a través de la página "Segunda Mano"; su modus operandi, consistía en ofertar los autos para enganchar a clientes y posteriormente citarlos en un lugar en donde cometían el robo y asesinato

Por **Iván Mejía** - 9 septiembre, 2019 1:23 pm

Compartir en Facebook | Compartir en Twitter | G+ | tweet

Tamaño de fuente: A A A A

Fraude informático en México

- Entre los delitos en Internet más recurrentes en México, hay quejas por fraude en comercio, códigos maliciosos, suplantación de identidad, pornografía infantil acoso, hurto de contraseñas, bullying, pedofilia, trata de personas menores de edad, sextorsión y el "fraude nigeriano", denuncian cibernautas mexicanos.
- Un reporte de la Secretaría de Seguridad Pública Federal revela que en los reportes de un año (de febrero de 2014 a febrero de 2015) hubo 14 mil 731 denuncias de delitos por parte de usuarios de Internet.
- El más recurrente el fraude al comercio electrónico, con 7 mil 444 quejas; le sigue el código malicioso, con mil 345, y la difamación, con mil 050 denuncias ante la Policía Cibernética.
- Fuente: https://vanguardia.com.mx/articulo/fraude-principal-ciberdelito-en-mexico

Capítulo II del Código Penal Federal

Artículo	Descripción
Artículo 211 bis 1	Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa
Artículo 211 bis 2	Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
Artículo 211 bis 3	Al que, estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa
Artículo 211 bis 4	Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa
Artículo 211 bis 5	Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementaran en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Tecnológico de Monterrey

Malware

Amenaza	Descripción
Virus	Lleva a cabo copias de sí mismo y trata de propagarse a otros equipos.
Spyware	Recopilar todo tipo de información del equipo infectado
Adware	Muestra publicidad durante la instalación o la ejecución de un programa
Rootkit	Capacidad de ocultar la presencia de malware en el sistema
Spam	Información no deseada
Ransomware	Impide funcionamiento del equipo, y demanda un rescate para poder usar el equipo.
Criptomineria	Uso de equipo para minar
Gusano	Se pueden propagar de un equipo a otro sin la necesidad de interacción humana.
Troyano	Programa que se hace pasar por otro.
Bomba lógica	Diseñado para llevar a cabo una función cuando se cumpla una determinada condición.

Tecnológico de Monterrey

Ingeniería social

Amenaza	Descripción
Phishing	Obtener datos por medios supuestamente legitimos (tipicamente web o correo)
Vishing	Obtener datos por medios supuestamente legitimos (llamadas telefonicas)
Baiting	Dispositivos de almacenamiento infectados supuestamente extraviados
Shoulder Surfing	Observación discreta (a corta distancia) de datos secretos de terceros
Intimidacion	Obtener datos mediante amenazas físicas y verbales una persona

Tecnológico de Monterrey

Información comprometida

Amenaza	Descripción
Espionaje Remota	Acciones dirigidas a conocer informacion de competidores por distintos medios
Eavesdropping / Snooping	Escucha subrepticia de comunicaciones por medios como sniffers
Robo medios documentos	Robo de discos, USB, cintas, o documentos físicos con información sensible
Robo de equipo	Robo de laptops, desktops o similares con información sensible
Dumpster Diving	Información obtenida recuperada desde medios reciclados o desechados
Disclosure	Divulgación no autorizada de información de la empresa
Datos no confiables	Datos provenientes de fuentes de dudosa procedencia, o con posibles errores
Manipulación con hardware	Ataques de laboratorio como microprobing, reinicio en frio
Manipulación con software	Recuperación de datos borrados data recovery

Amenazas tecnológicas (1/2)

Amenaza	Descripción
Falla de Host	Falla tecnica de servidores, fuentes de poder, tarjetas, procesadores
Falla de Workstation	Falta técnica de equipos personales, laptop, desktop
Falla de Almacenamiento	Falla técnica de discos duros, arreglos de discos, memorias USB, cintas
Falla de Impresion	Falla técnicas de impresoras plotters
Falla de Componente de red	Falla de switches, routers, bridges, puntos de acceso, repetidores
Falla de Interfaces de red	Falla de ultimas millas
Falla de Servicios de red	Falla de enlaces de comunicación cortes de libra
Falla de plataformas	Falla de sistemas operativos, hipervisores, host virtuales
Falla de Suministro eléctrico	Falla de UPS, plantas de energía subestaciones eléctricas, tierra física

Tecnológico de Monterrey

Amenazas tecnológicas (2/2)

Amenaza	Descripción
Falla de controles ambientales	Falla en aire acondicionado, control de temperatura, supresión de fuego
Falla de Bases de datos	Falla en sistemas manejadores, instancias, Vistas, perfiles, triggers
Falla de Aplicaciones	Falla por incompatibilidad, desactualización, inconsistencia en funcionamiento
Negación de servicio	Ataques de inundación (protocolos), botnets, ataques distribuidos
Escalamiento de privilegios	Subir el nivel de permisos que el usuario puede llevar a cabo
Exploits	Programas que explotan vulnerabilidades conocidas en sistemas de TI
Supply chain attack	dañar una organización apuntando a elementos menos seguros en la red de suministro, p.e. infiltración en el proceso de desarrollo de empresas o proyectos de software legítimo

Tecnológico de Monterrey

Acciones no autorizadas

Amenaza	Descripción
Procesamiento ilegal datos	Utilización de datos o ejecución de procesos no debidos
Corrupción de datos	Borrado de datos, manipulación de datos
Abuso de privilegios	Aprovechar privilegios mal asignados o excesivos que ya se tengan
Uso no autorizado (Apps)	Uso no autorizado de software de la empresa (desarrollado o adquirido)
Uso no autorizado (Datos)	Uso no autorizado de bases de datos y/o documentos físicos / electrónicos)
Uso no autorizado (SO)	Uso no autorizado de sistemas operativos y sus configuraciones o utilidades
Uso no autorizado (Red)	Uso no autorizado de servicios como internet Intranet VPN

Tecnológico de Monterrey

Accesos no autorizados

Amenaza	Descripción
A las aplicaciones	Obtener privilegios en software (por cualquier medio y de cualquier nivel - RWX)
A bases de datos /file servers	Obtener privilegios en datos (por cualquier medio y de cualquier nivel - RWX)
A plataformas	Obtener privilegios en sistemas operativos (físicos o virtuales) e hipervisores
A redes	Obtener privilegios en diversos componentes de red
A localidades fisicas	Edificios o centros de datos por técnicas como piggybacking o tailgating

Errores u omisiones provocados por personas

Amenaza	Descripción
Error en uso de activos	Errores por desconocimiento en la utilización de ciertos activos
Error en la operación	No ejecución o ejecución incorrecta de tareas, actividades o procesos
Error de captura	Captura incorrecta de información desde un documento origen y hacia un SW
Omisión de datos	Datos no considerados / datos incompletos necesarios para un proceso
Errores en mantto HW	Negligencia, descuido, mal uso de herramientas o materiales
Errores en mantto SW	Vulnerabilidades intencionales o accidentales al programar el software

Suplantación de identidad

Amenaza	Descripción
Internos por internos	Cuando un usuario interno personifica a otro Usuario interno
Internos por externos	Cuando un usuario externo personifica a otro usuario interno
Ataques a autenticación	Fuerza bruta, robo de passwords o tokens, main-in-the-middle attack
Spoofing	Presentación de información falsa para obtener acceso algoritmo

Niveles de impacto

Nivel de impacto	Definición
Alto	La perdida 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 perdidas financieras mayores. • Resulta en daños severos o catastróficos para los individuos involucrando la perdida de la vida o serias amenazas a la vida.
Medio	La perdida 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 perdidas financieras significativas. • Resulta en daños significativos para los individuos pero no en la perdida de la vida o serias amenazas a esta.
Bajo	La perdida 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 perdidas financieras menores. • Resulta en una exposición menor al daño.

Nivel Impacto	Definición
Bajo	Un grupo pequeño o departamento afectado; impacto pequeño o sin impacto para los procedimientos del negocio
Medio	Dos o mas departamentos o unidades de negocio afectadas, retraso de cuatro a seis horas para cumplir los objetivos de la misión
Alto	La misión entera de la empresa es afectada

Tecnológico de Monterrey

Niveles de probabilidad

Nivel probabilidad	Definición
Bajo	• Es extremadamente poco probable que esa amenaza ocurra durante los próximos 12 meses. • La fuente de la amenaza esta motivada ni cuenta con la capacidad, o existen controles para prevenir, o al menos significativamente impedir, que la amenaza se materialice
Mediano	• Es posible que esa amenaza ocurra durante los próximos 12 meses. • La fuente de la amenaza esta motivada, pero los controles implementados pueden impedir que la capacidad se materialice.
Alto	• Es altamente probable que esa amenaza ocurra durante los próximos 12 meses. • La fuente de la amenaza esta altamente motivada y tiene la capacidad suficiente, y los controles son inadecuados para prevenir que la capacidad se materialice

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

Matriz priorización de amenazas

Amenaza	Probabilidad de la amenaza	Impacto de la amenaza	Factor de riesgo

Amenaza	Probabilidad de la amenaza	Impacto de la amenaza	Factor de riesgo
Interrupción eléctrica	Alta		Moderado Alto
Revelación deliberada	Medio		
Fraude	Alta		
Error de ingreso de usuario	Alta		

Tecnológico de Monterrey

Ejemplos de controles

Categoría de control	
Evitación	Cifrado y autenticación
	Arquitectura de la seguridad del sistema
	Proceso de análisis de riesgo
	Programa de awareness de la información
	Programa de la seguridad de la información
	Prevención de interrupciones
	Políticas, estándares, guías y procedimientos
	Infraestructura llave publica
	Arquitectura de aplicaciones seguras
	Comunicaciones seguras
Aseguramiento	Revisión de la seguridad de las aplicaciones
	Pruebas estándares
	Pruebas de penetración
	Escaneo de la seguridad perimetral
	Análisis de vulnerabilidades
Detección	Detección de intrusos
	Monitoreo de ataques remotos
Recuperación	Planeación de continuidad del negocio
	Análisis del impacto del negocio
	Planeación del manejo de crisis
	Planeación de recuperación de desastres
	Procedimientos de respuesta a incidentes
	Computo forense

IT Group	*Descriptor*	*Definition*
Operations controls	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.
Operations controls	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.
Operations controls	Risk analysis	Conduct a risk analysis to determine the level of exposure to identified threats and identify possible safeguards or controls.
Operations controls	Antivirus	(1) Ensure LAN administrator installs the corporate standard antiviral software on all computers. (2) Training and awareness of virus prevention techniques will be incorporated into the organization information protection (IP) program.
Operations controls	Interface dependencies	Systems that feed information will be identified and communicated to operations to stress the impact to the functionality if these feeder applications are unavailable.
Operations controls	Maintenance	Time requirements for technical maintenance will be tracked and a request for adjustment will be communicated to management if experience warrants.
Operations controls	Service level agreement	Acquire service level agreements to establish level of customer expectations and assurances from supporting operations.

Tecnológico de Monterrey

Integrando controles

Amenaza	*Probabilidad de la amenaza*	*Impacto de la amenaza*	*Factor de riesgo*	*Posible control*	*Costo del control*
Interrupción eléctrica	Alta	Baja	Moderado Medio	Sistema de suministro de energía sin interrupción (UPS)	$ 38 000
				Supresores de variaciones de voltaje	$ 25 por maquina
Revelación deliberada	Medio	Medio	Moderado Alto	Políticas para el manejo de información	200 horas del staff de seguridad para desarrollarlas
				Programa de awareness del usuario	20 horas para desarrollar la presentación, 1 hora por cada empleado que asista
Fraude	Alta	Medio	Alta	Listas de control de acceso	Instalación de software
				Registros de auditoria	La capacidad existente con el sistema para bitácoras
Error de ingreso de datos por usuarios	Alta	Baja	Moderado Medio	Controles de edición y validación	8 horas adicionales de programación por aplicación

¿Y que se hace con el riesgo?

- Etapa conocida como manejo o administración del riesgo
  - Risk Management
- Alternativas
  - Evitar: eliminar el factor del riesgo
  - 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

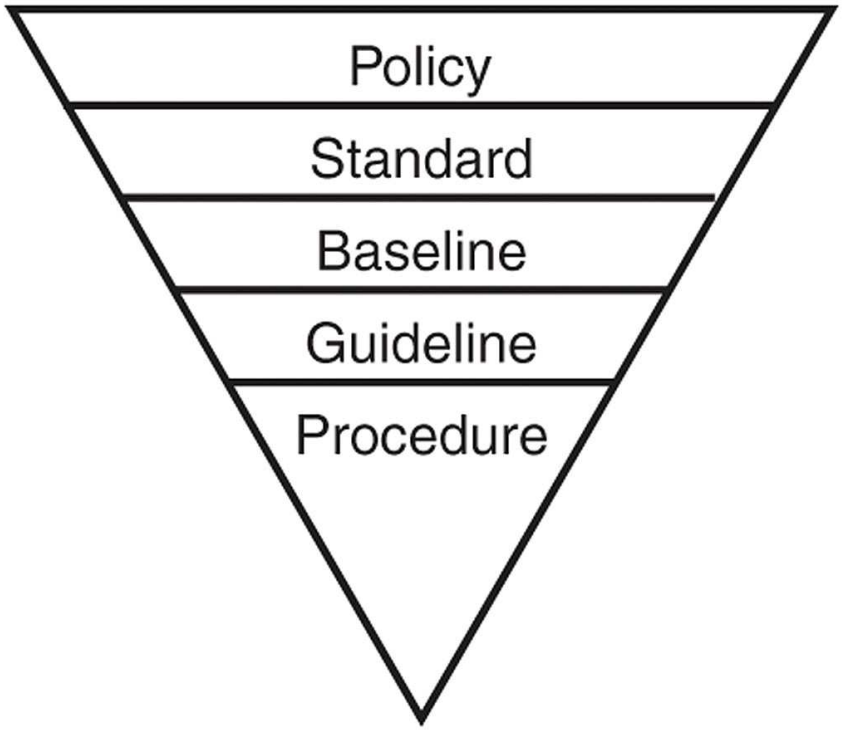
3. Identificar posibles acciones (gasto) y sus implicaciones. (B) Seleccionar acciones a implementar.

¿ B ≤ P*L ?

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

Documentación

- Política
- Estándar
- Nivel mínimo
- Guía
- Procedimiento



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

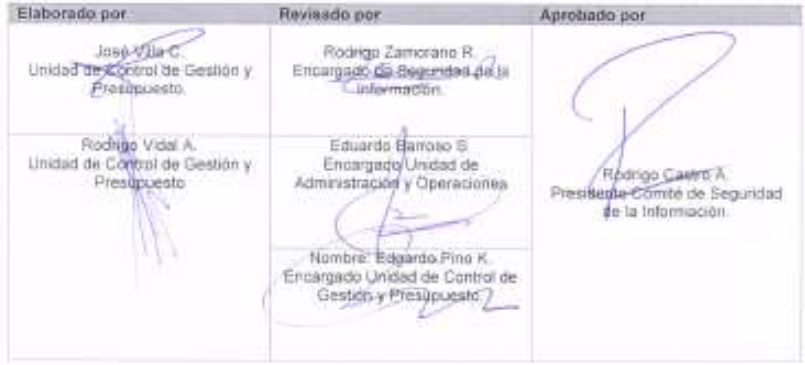
Tipos políticas de seguridad

- 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

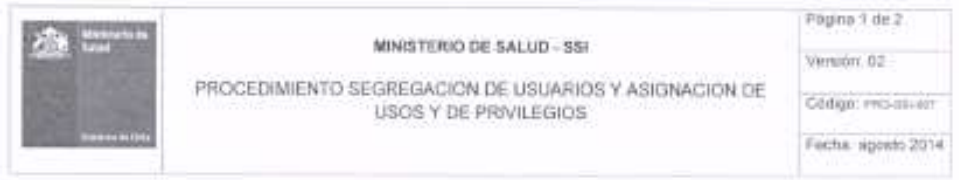
- Son la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas.

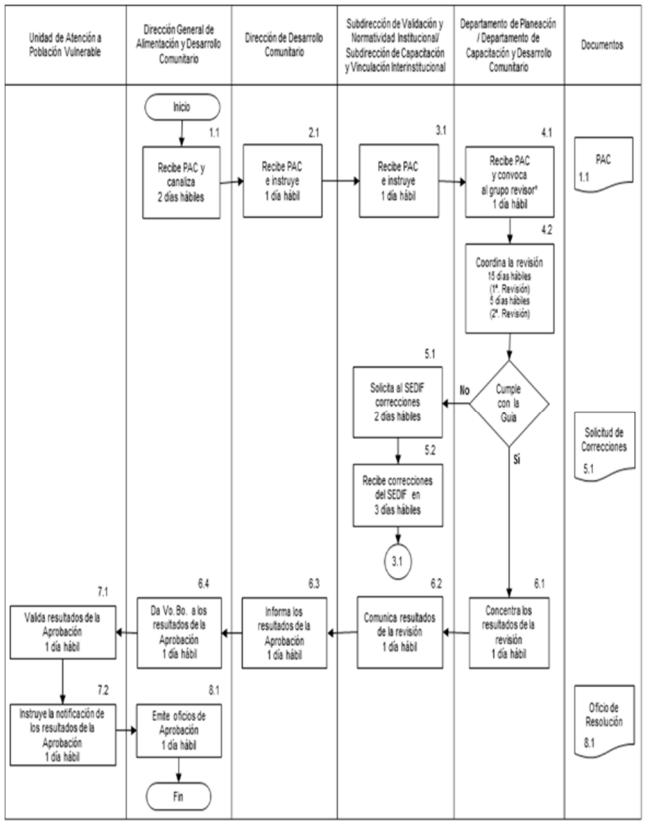
- Los Procedimientos de Seguridad permiten aplicar e implantar las Políticas de Seguridad que han sido aprobadas por la organización.

- 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



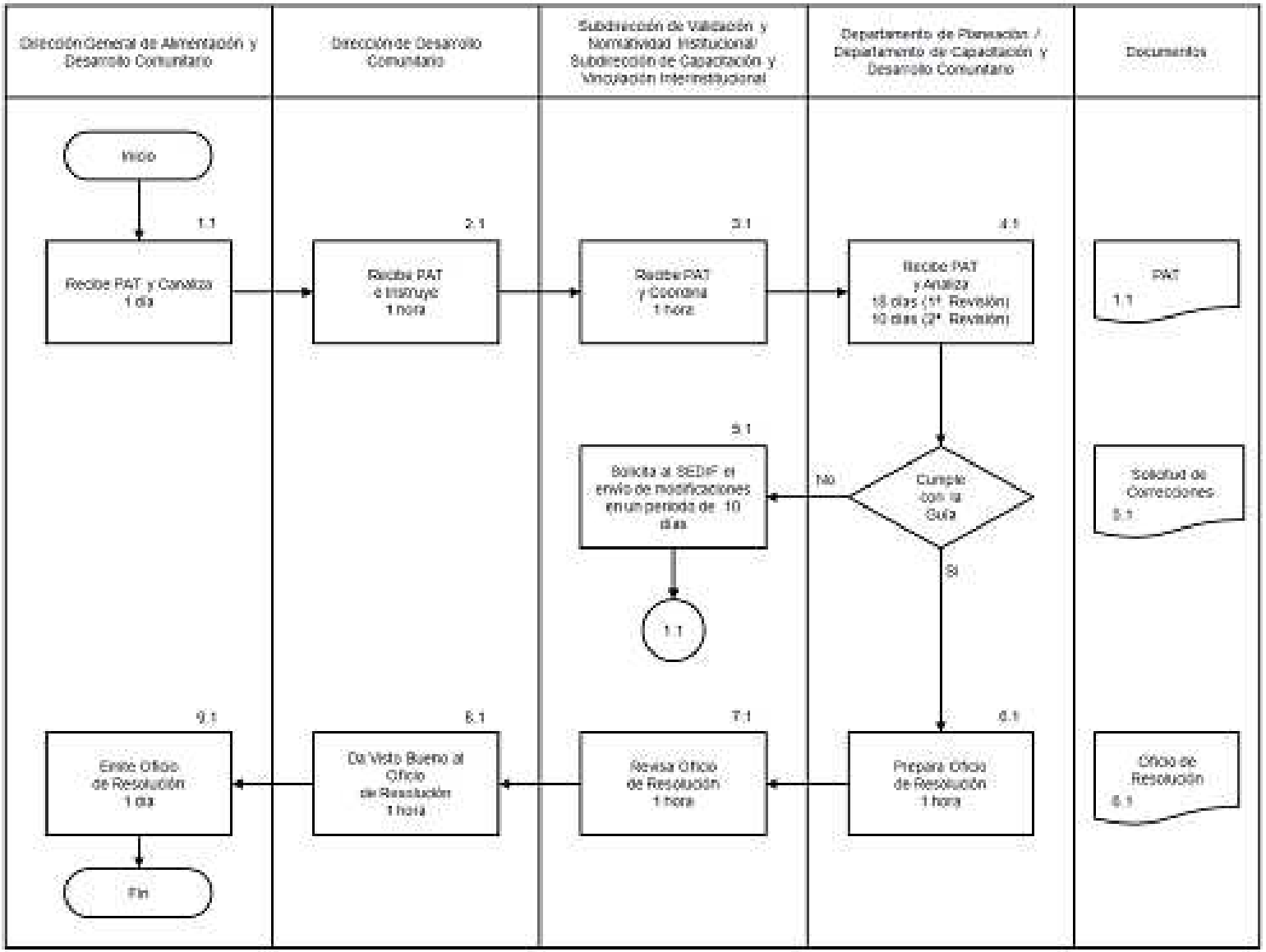


Procedimiento nº	Versión	Autor	Fecha Aprobación	Fecha última Actualización
2012/000 IGAE		ACS		marzo-2013

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



Tecnológico de Monterrey

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

Tecnológico de Monterrey

Conceptos Base, Análisis de Riesgos, Políticas, Procedimientos y SLAs

Roberto Gómez Cárdenas
rogomez@itesm.mx
http://cryptomex.org
@cryptomex