Sistemas de Información para la Gestión

UNIDAD 5

Temas: Seguridad en los Sistemas de Información: Seguridad, Privacidad e Integralidad. Plan de Contingencia de los sistemas de información. Tecnologías y herramientas para proteger los recursos de información. Aspecto económico de las medidas de seguridad.

Unidad 5: SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

Contenidos:

Seguridad en los Sistemas de Información: Seguridad, Privacidad e Integralidad: Objetivos de la seguridad en la información Análisis de Riesgos de los sistemas de información. **Tecnologías y herramientas para proteger los recursos de información.** Medidas de controles generales, de aplicación, y en comunicaciones. Firma Digital. **Plan de Contingencia de los sistemas de información.** Plan de reanudación de negocios Medidas de recuperación. **Aspecto económico de las medidas de seguridad.** Estructura de control: Costos Beneficios.

Unidad 5: SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

Objetivos específicos:

- Entender las vulnerabilidades de los Sistemas de Información
- Conocer los componentes de un marco de trabajo organizacional para definir la seguridad y el control adecuados
- Conocer las herramientas y tecnologías para salvaguardar los recursos de información y áreas de TI para el aseguramiento de la disponibilidad la información sistemas
- Analizar y avaluar las políticas y procedimientos relativos a la planificación para la atención de contingencias y devolver a la gestión capacidad de respuesta y retorno a la normalidad

Unidad 5: SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

Bibliografía Básica:

- Sistemas de información gerencial / Laudon, Kenneth C. (2012) Sistemas de información gerencial [texto impreso] / Laudon, Kenneth C.; Laudon, Jane P.. - 12a. ed.. - México: Pearson Educación, 2012. ISBN 978-607-32-0949-6. Nota de contenido: Cap. 8. Seguridad en los sistemas de información

Unidad 5: SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

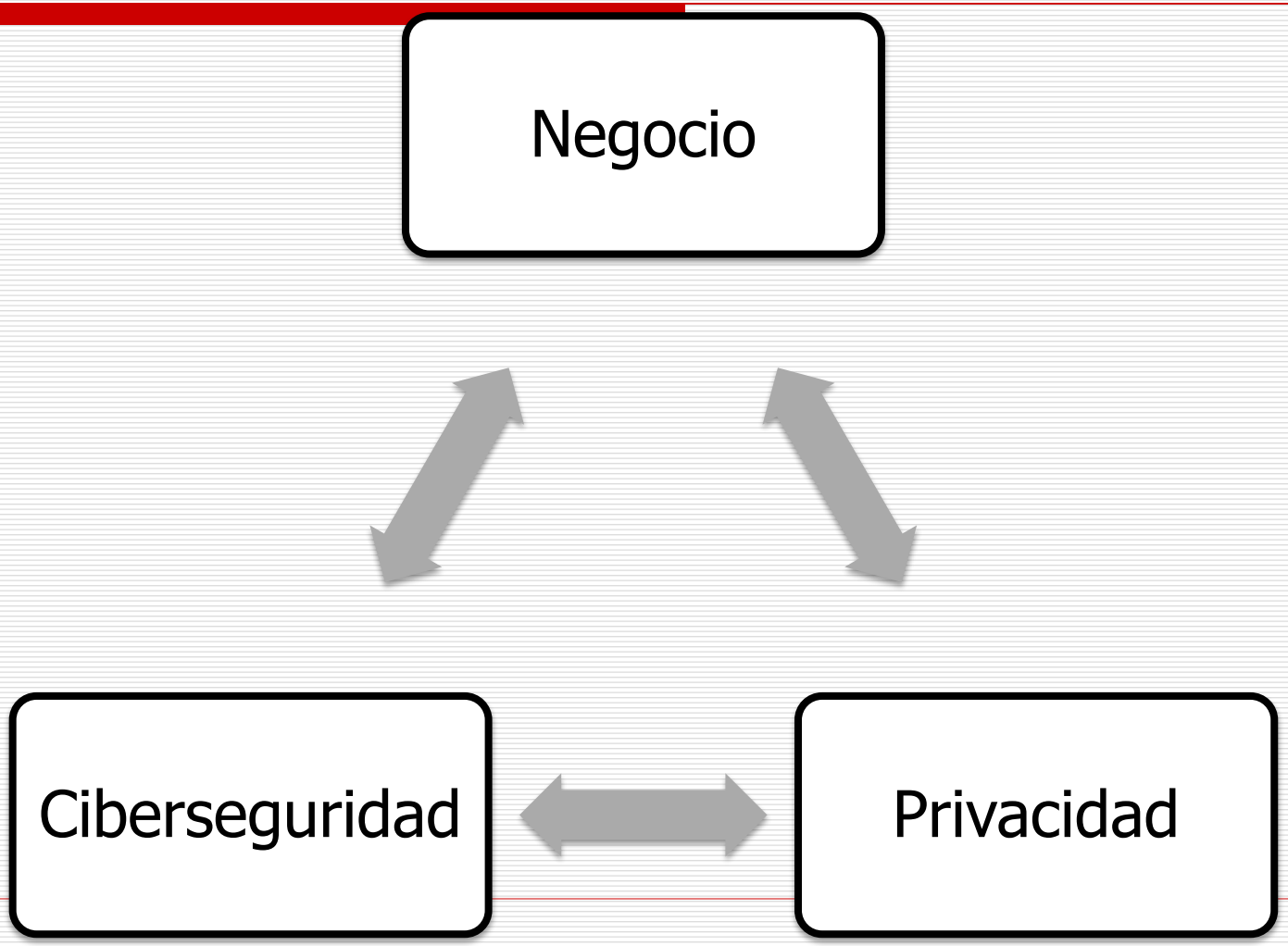
Bibliografía Básica:

- Sistemas de información para la gestión empresaria / Lardent, Alberto R. (2001) Sistemas de información para la gestión empresaria : procedimientos, seguridad y auditoría [texto impreso] / Lardent, Alberto R.. - Buenos Aires : Pearson Educación, 2001. . ISBN 987-9460-51-0. Nota de contenido: II: Seguridad y auditoría informática : 19. Seguridad informática 22. Controles de accesos lógicos y físicos - 23. Seguridad en los sistemas de base de datos - 24. Seguridad de redes y sistemas distribuidos 29. Recuperación de desastres. Continuidad de operaciones.

Plan de clase

- Introducción
- Importancia y Objetivos Seguridad de la información
- Análisis de Riesgos
- Aspecto económico de las medidas de seguridad
- Tecnologías y herramientas para proteger los recursos de información
- Plan de Seguridad
- Conclusiones

Para empezar….. Era Digital



Seguridad de los Sistemas de Información

El gerente deberá asegurarse de que los sistemas de su empresa son

Confiables, seguros

Y

estén disponibles

Sistemas de Información

Confiables, Operativos y Seguros

NEGOCIOS TRADICIONALES

RELACIÓN ENTRE OPERATIVIDAD Y SEGURIDAD

$$\text{OPERATIVIDAD} : \frac{1}{\text{SEGURIDAD}}$$

COMPUTADORA SEGURA: A 20 METROS BAJO TIERRA, EN RECINTO DE HORMIGÓ, AISLADA DE OTRAS COMPUTADORAS Y CON SISTEMA ELÉCTRICO AUTÓNOMO TRIPLE

El desafío es contar con medidas de seguridad que minimicen los riesgos sin afectar la operatividad de los sistemas

Sistemas de Información

Confiables, Operativos y Seguros

NEGOCIOS DIGITALES

RELACIÓN ENTRE AGILIDAD SUSTENTABLE Y CIBERSEGURIDAD

AGILIDAD SUSTENTABLE = CIBERSEGURIDAD

El desafío es contar con medidas de seguridad que minimicen los riesgos sin afectar la operatividad de los sistemas

Seguridad de los Sistemas de Información

Retos:

Diseñar sistemas que no estén sobrecontrolados ni subcontrolados:
Las violaciones internas de seguridad son mas numerosas pero las externas van en aumento.

Encontrar un equilibrio en cuanto a protección vs molestias de control

¿ Por qué es necesario prever la Seguridad de los Sistemas de Información ?

Objetivos Seguridad de la Información

Objetivos Seguridad Informática

- Disponibilidad
- Integridad
- Confidencialidad

¿ Por qué es necesaria la Seguridad en Sistemas de Información ?

Información y Sistemas de Información elementos **fundamentales** en las organizaciones.

Alta Dependencia de sistemas de información para operar

Disponibilidad de sistemas informáticos elemento crucial para la gestión. Por otra parte los procedimientos manuales, si existen, son útiles por un corto periodo.

Interrupción prolongada de Sistemas de Información puede llevar a **pérdidas significativas** (financieras, de reputación, del negocio)

¿ Por qué es necesaria la Seguridad en Sistemas de Información ?

Imaginemos que efecto tendrían en una organización situaciones tales como:

- El robo de información estratégica referida a un nuevo producto a lanzar al mercado
- La interrupción del sistema de facturación durante una semana o un mes;
- La pérdida de todos los datos de la empresa, o de sus clientes.
- Un incendio o una inundación que afecte los equipos de computación

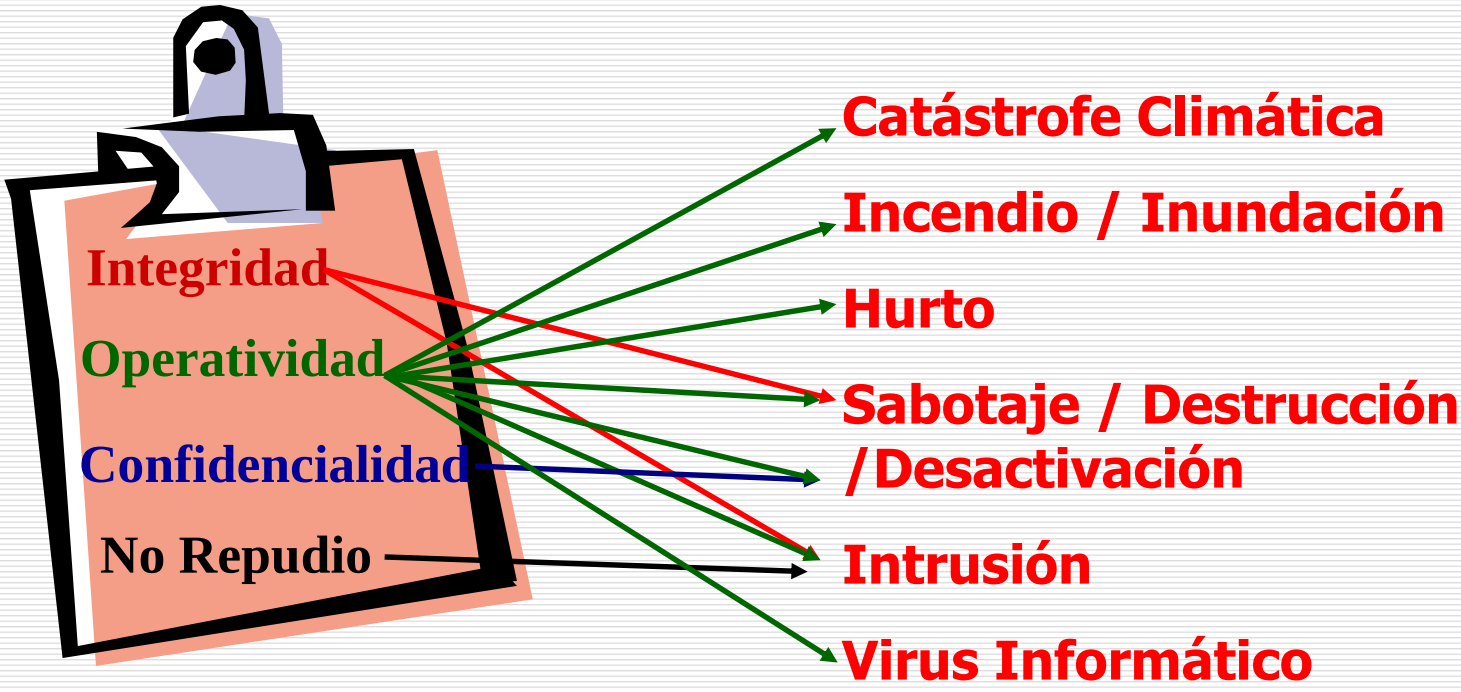
Objetivos de la Seguridad Informática

a) Reducir los riesgos que amenazan estas características de la Información

b) Mantener:

- **Integridad de la Información**: sólo puede ser creada y modificada por personas autorizadas
- **Disponibilidad / Operatividad de la Información**: debe estar disponible en el momento oportuno
- **Confidencialidad de la Información**: puede ser conocida sólo por las personas definidas.
- **No Repudio de la Información**: debe ser transmitida de manera segura, a través del intercambio de certificados digitales.

Principales Factores de Riesgo para un Sistema Informático



Un Sistema de Seguridad **solo está completo** cuando incluye los siguientes Planes:

Seguridad

Prevenir Minimizar los riesgos de ocurrencia de un Desastre

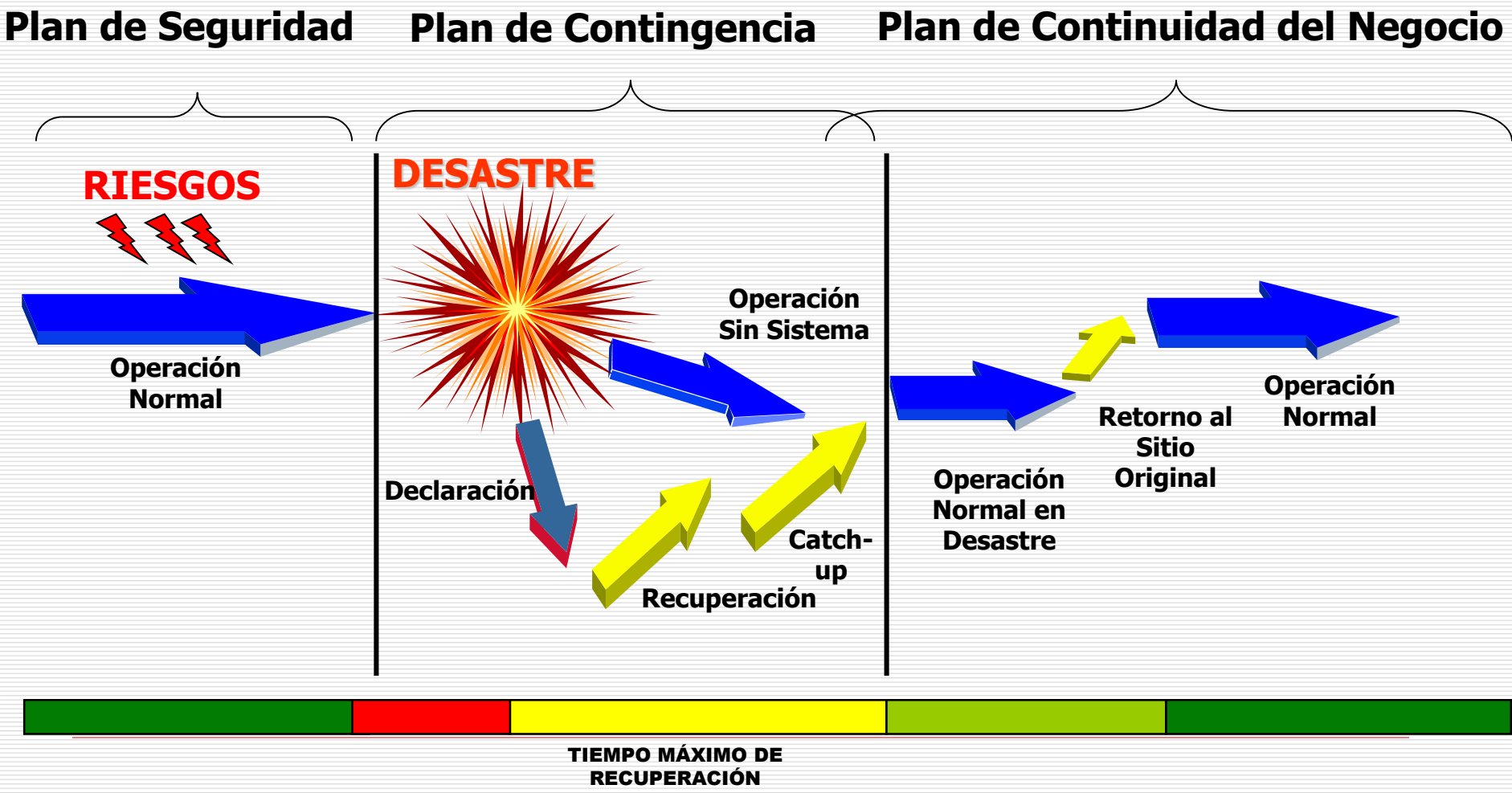
Contingencia

Operar cuando se produce un Desastre hasta Salir de la Crisis

Continuidad del Negocio

Continuar con el negocio luego de la crisis

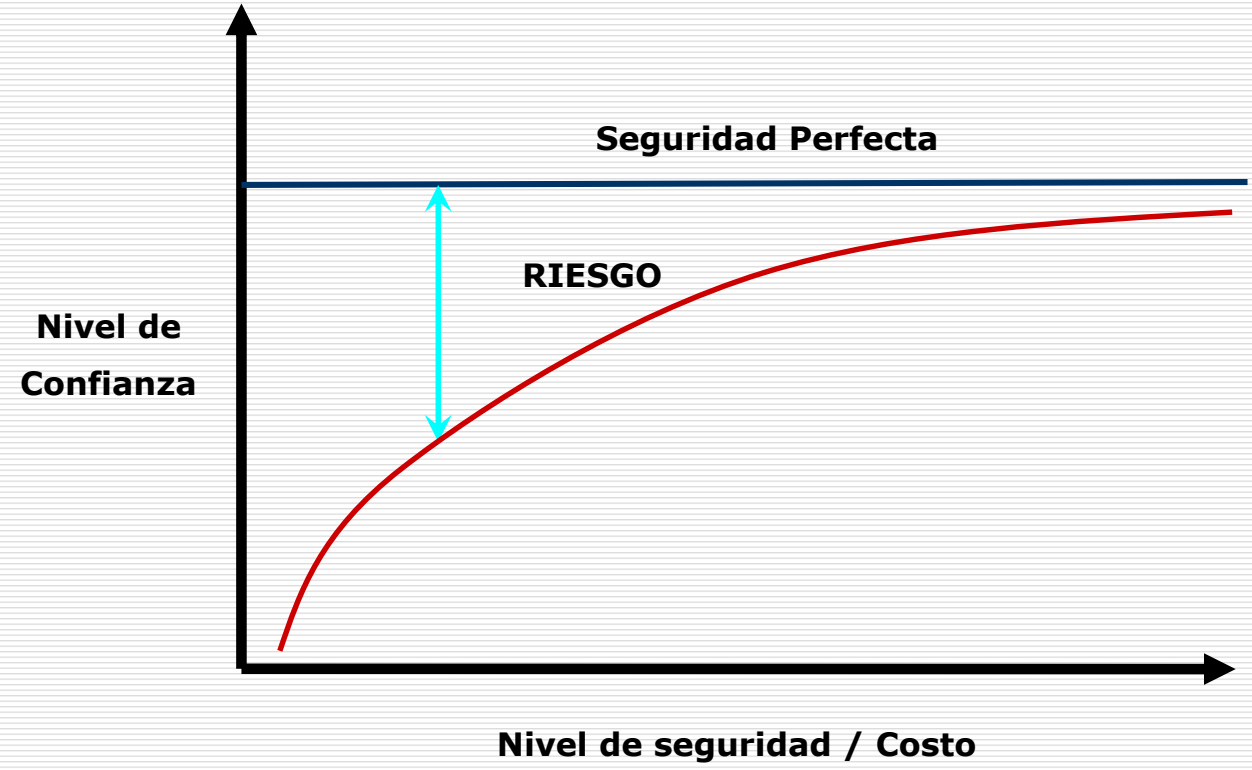
Alcance de la Estrategia de Seguridad



Análisis de Riesgos

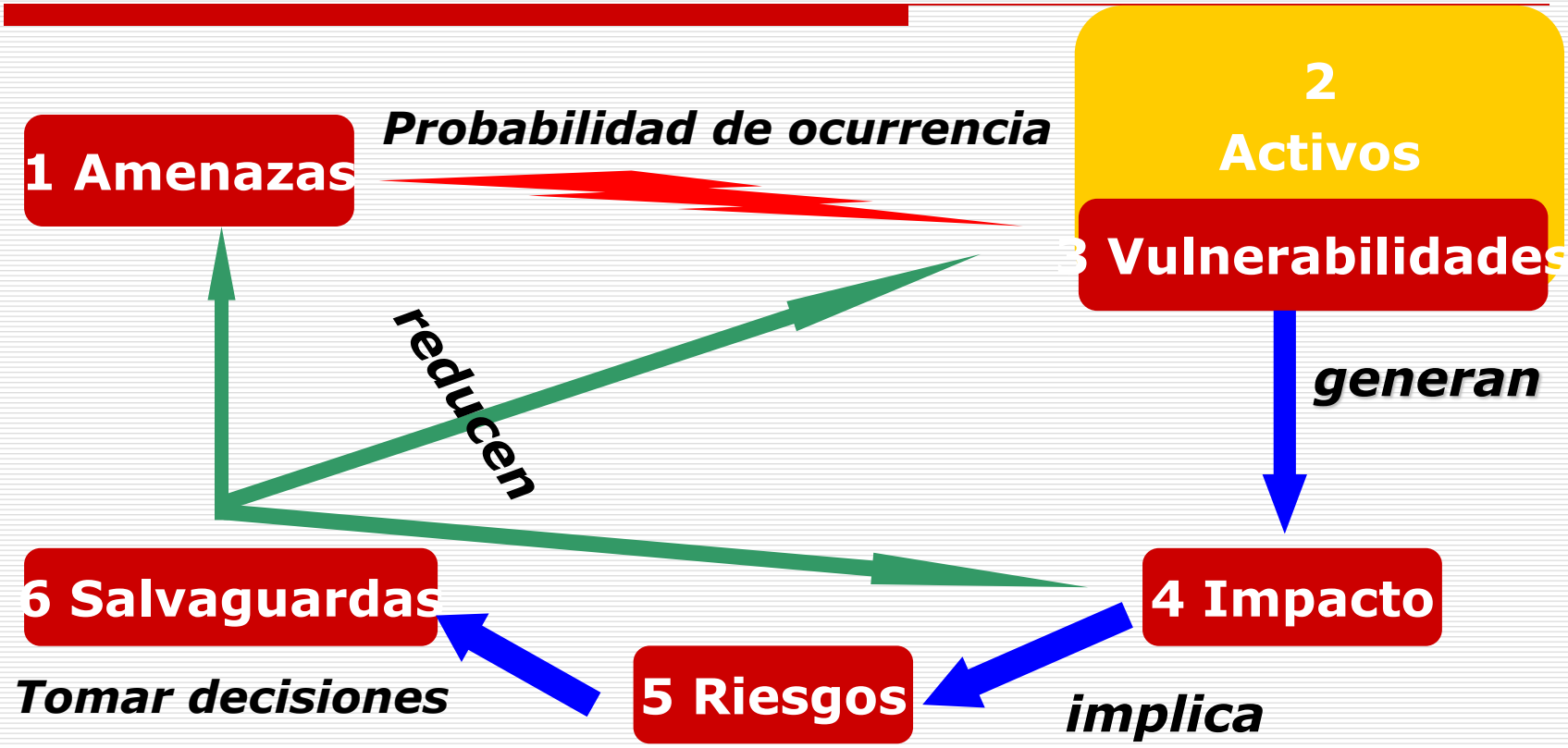
Análisis de Riesgos

El Riesgo NO SE PUEDE ELIMINAR

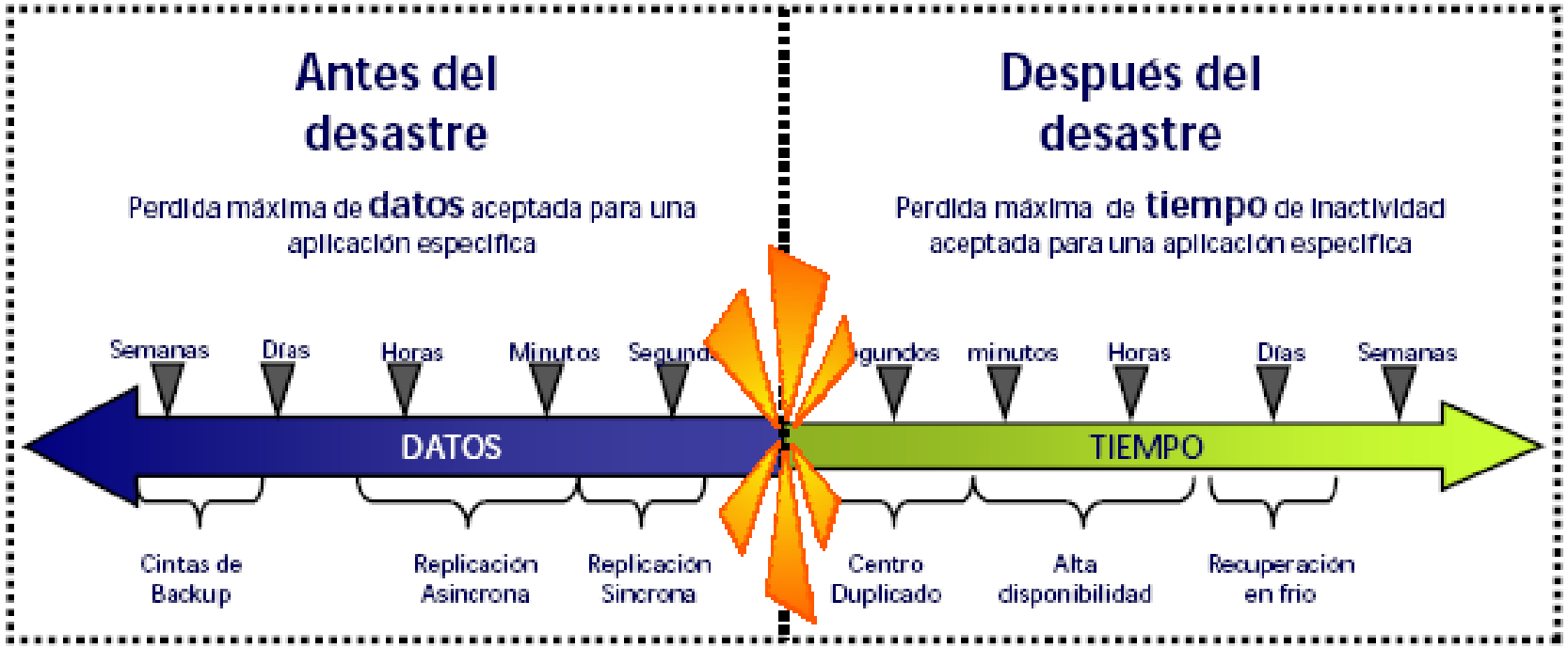


El análisis permite a la organización definir el nivel de riesgo aceptable

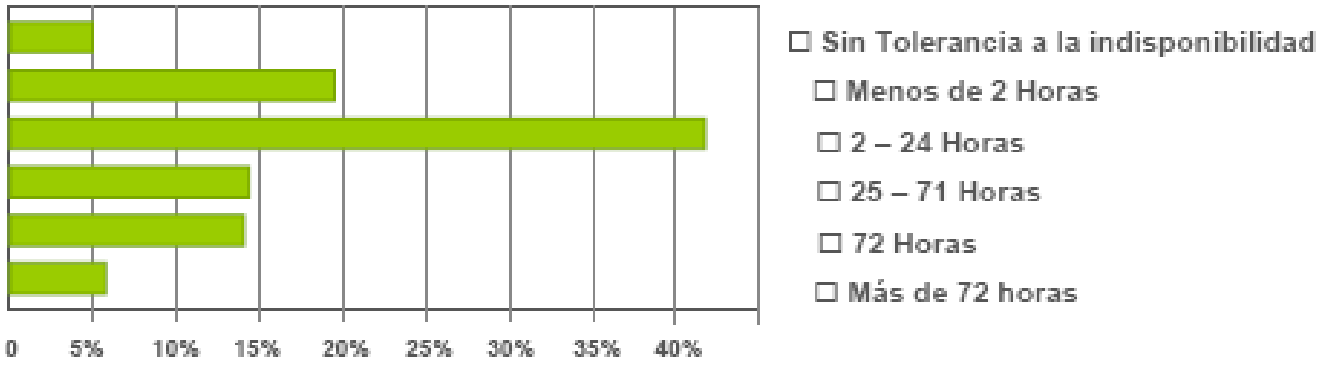
Análisis de Riesgo del Negocio



Análisis de Riesgo



Cuando se interrumpe una función, ¿Cuál es máximo tiempo de inactividad?



Fuente Business Continuity 2004 Deloite

Análisis de riesgos

- Proceso de identificación y evaluación del riesgo a sufrir un ataque y perder datos, tiempo y horas de trabajo, comparándolo con el costo de la prevención de esta pérdida.

- Su análisis no sólo lleva a establecer un nivel adecuado de seguridad: permite conocer mejor el sistema que vamos a proteger.

Análisis de riesgos

Información a Obtener del Análisis

- Identificación recursos críticos de la empresa.
- Identificación amenazas del sistema.
- Identificación vulnerabilidades del sistema.
- Identificación posibles pérdidas.
- Identificación probabilidad de ocurrencia de una pérdida.
- Derivación contramedidas efectivas.
- Identificación herramientas de seguridad.
- Implementación sistema de seguridad eficiente en costos y tiempo.

Análisis de riesgos
Elementos a Evaluar

- Probabilidad de ocurrencia de una amenaza
- Impacto del la ocurrencia en el sistema/negocio
- Costo de la Implementación de medidas preventivas

¿ Costo <> = Probabilidad * Impacto ?

Análisis de riesgos
¿Cuánto y Cuando invertir en Medidas de Seguridad?

$$\text{Costo} \leq \text{Probabilidad} * \text{Impacto}$$

Hay que implementar una medida de prevención.

$$\text{Costo} > \text{Probabilidad} * \text{Impacto}$$

La medida de prevención es antieconómica

Análisis de riesgos
Efectividad del Costo del Control

- El control ha de tener menos costo que el valor de las pérdidas debido al impacto de ésta si se produce el riesgo.

- Ley básica: el costo del control ha de ser menor que el activo que protege.

Tecnologías y herramientas para proteger los recursos de información

Tratamiento Riesgos

Mitigación del Riesgo

- **Controles Disuasivos**
- **Controles Preventivos**
- **Controles de Detección**
- **Controles Correctivos**

Creación de un Entorno de Control

Se necesita un programa de Seguridad empresarial integral que cubra todos los elementos

Gerenciamiento

Administración

- Políticas & Standarts
- Procedimientos
- Clasificacion & Control
- Planeamiento de Sistemas
- Gestión de Equipos
- Desarrollo& Mantenimiento

Organización

- Infraestructura
- Personal
- Roles & Responsibildades
- Entrenamiento & Concientización
- Acceso de Terceros

Monitoreo

- Logging & Reportes
- Respuestas ante incidentes
- Cumplimiento de normativa legal
- Gestión de Riesgos

Control de Accesos

Validar Accesos

- Autorización
- Autenticación
- Administracón

Asegurar

- Confidencialidad

Transacciones confiables

- Integridad
- No Repudio
- Responsabilidad

Acceso para el Medio Circundante

Red Perimetral

- Internet
- Extranet
- Wireless
- Dial-Up

Red Interna

- Estaciones de Trabajo
- Servers
- LAN
- WAN

Aplicaciones

- Web/eMail
- Empresa
- Middleware
- Bases de Datos

Accesibilidad

- Areas
- Equipamiento
- Soportes de Datos

Integridad de la Infrastructura

Protección

- Virus
- Contenidos
- Intrusión / Pérdidas
- Físico

Configuración

- Sistemas Operativos
- Equipamiento de Redes
- Segmentación

Disponibilidad

- Recuperación
- Continuidad
- Backup
- Redundancia

Creación de un Entorno de Control

Controles Generales

Controles globales que establecen un marco de trabajo para controlar el diseño, el uso de programas de computación a lo largo de la organización

Creación de un Entorno de Control

Controles de Aplicaciones

Controles específicos, únicos de cada aplicación

Creación de un Entorno de Control

Controles de seguridad de los datos

Para asegurar que los archivos no sean objeto de accesos no autorizados, cambios o destrucción

Creación de un Entorno de Control

Controles Administrativos

Estándares, reglas, procedimientos y disciplinas formalizados para garantizar que los controles se ejecuten y apliquen adecuadamente.

Medidas de Seguridad

Seguridad Física vs. Seguridad Lógica

- **Seguridad Física**: protección del sistema ante las amenazas físicas, planes de contingencia, control de acceso físico, políticas de backups, etc.

- **Seguridad Lógica**: protección de la información en su propio medio mediante el enmascaramiento de la misma usando técnicas de criptografía.

Medidas de Seguridad Física para Sistema de Información

Amenaza	Medidas de Seguridad
Falla hardware Error mantenimiento HW Problema eléctrico Problema telecomunicación Temperatura/Humedad inadecuada	Cloud Computing Virtualización de PC Suministro ininterrumpido de corriente (UPS). Toma de tierra Líneas de comunicación redundantes Sistema refrigeración

Medidas de Seguridad para Sistema de Información

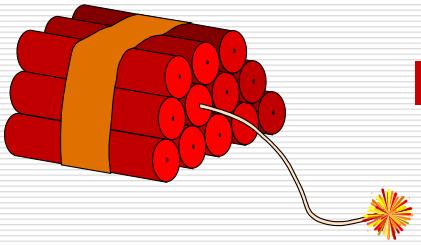
Amenaza	Medidas de Seguridad
Indisponibilidad del personal	Segregación funcional
Abuso privilegio de acceso	Concientización uso TI
Ingeniería Social	Políticas de Seguridad para Personal
Celular personal	Capacitación
Amenaza de correo electrónico	Bloqueo de conexiones para dispositivos de copia de datos
Ransomware	
Fuga de información	

Medidas de Seguridad para Desastres naturales

Desastres naturales	Medidas de Seguridad
■ Tormenta ■ Inundación ■ Incendio ■ Tornado	■ Emplazamientos adecuados ■ Protección fachadas, ventanas, puertas ■ Sistema de doble piso ■ Materiales ignífugos ■ Prohibición de fumar ■ Backups en lugar distinto al centro de cómputos ■ Sistemas ininterrumpidos de energía ■ Líneas de comunicación redundantes

Medidas de Seguridad para Vandalismo informático

Vandalismo informático	Medidas de Prevención
Terrorismo Sabotaje Robo	Proteger entradas Guardia Circuito cerrado TV Control de accesos
Virus Programas malignos	Protección con Antivirus, Firewalls, Antispayware, Antiphishing



Medidas de Seguridad para Accesos no autorizados

Accesos no autorizados	Medidas de Prevención
Acceso Físico	Control de acceso Físico Control de terminales
Acceso a Datos y Aplicaciones	Nombres de Usuarios y claves privadas Encriptado de datos Derechos de usuarios sobre datos y archivos Detector de Intrusos

Medidas de Seguridad para Ciberamenazas Negocios Digitales

Ciberamenazas	Medidas de Prevención
■ Amenazas resultantes de la adopción de nuevas tecnologías ■ Amenazas por la convergencia de redes sociales y plataformas online dentro de la red corporativa	■ Antimalware ■ Cifrado Archivos en Dispositivos Móviles (File encryption for mobile devices) ■ Tecnología Prevención Pérdida de Datos (Data loss prevention technology) ■ Dispositivos Almacenamiento Cifrado (Encrypted storage devices)

Plan de Seguridad

Importancia de contar con Planes Formales

- La empresa gana en conocimiento real de sus fortalezas y debilidades.
- Reacción con mayor rapidez ante la ocurrencia de un desastre
- Reducir exposición a sufrir una pérdida irreparable mucho más costosa que contar con el plan.

Plan de Seguridad

Concepto

Documento normativo que describe
las medidas de seguridad
y controles internos adoptados
para minimizar los riesgos
a los que están expuestos los Sistemas de Información
de una organización

Plan de Seguridad

Componentes

- ✓ Seguridad del Medio
- ✓ Seguridad Desarrollo, Mantenimiento y Operación de Sistemas Informáticos
- ✓ Seguridad de Datos y Programas
- ✓ Seguridad en las Comunicaciones
- ✓ Protección contra el Personal

Plan de Seguridad
Componentes

SEGURIDAD DEL MEDIO

El objetivo principal es proteger los recursos contra la destrucción accidental o intencional, corrupción, interrupción, robo de datos.

Plan de Seguridad
Componentes

SEGURIDAD DEL MEDIO

Principales recursos a tener en cuenta:

- Personal
- Inmueble: inundaciones, incendios, temblores
- Computadoras: Proteja con materiales aislantes en los muros, pisos y techos
- Soporte de datos y programas (Discos magnéticos, cartuchos, CD, etcétera)
- Documentación
- Suministros: insumos, energía

Plan de Seguridad
Componentes

SEGURIDAD EN EL DESARROLLO, MANTENIMIENTO Y OPERACIÓN DE LOS SISTEMAS INFORMATICOS

Los numerosos problemas que surgen al momento de procesar los datos, con frecuencia se atribuyen a la técnica utilizada en el diseño del sistema durante el desarrollo y a la forma de controlarlo durante la operación.

Plan de Seguridad
Componentes

SEGURIDAD EN EL DESARROLLO, MANTENIMIENTO Y OPERACIÓN DE LOS SISTEMAS INFORMATICOS

Objetivos:

• Garantizar desarrollo de sistemas y programas eficaces.

•Prevenir o detectar manipulación fraudulenta de datos durante el procesamiento e impedir mal uso de datos confidenciales.

• Proteger registros contra destrucción accidental (o intencional) y asegurar continuidad.

Plan de Seguridad
Componentes
SEGURIDAD DE DATOS Y PROGRAMAS

Medios de acceso y manipulación ilegal de datos y programas a tener en cuenta:

- Robo soporte de hardware (Discos magnéticos, CDs, Pen Drives) donde están almacenados los datos

- Acceso o manipulación del sistema computacional y del software operativo

- Acceso ilegal a sistemas de entrada de datos y a mecanismos que permiten modificar datos

- Uso ilegal de una estación de trabajo

Plan de Seguridad
Componentes

SEGURIDAD EN LAS COMUNICACIONES

Un fraude en la comunicación de datos representa la modificación o intercepción de mensajes mediante el uso de un sistema de comunicación en línea.

Las técnicas más comunes son:

- Usurpación de puestos de trabajo
- Intercepción de líneas telefónicas
- Suplantación de personalidad
- Usurpación de líneas telefónicas

Plan de Seguridad
Componentes

SEGURIDAD EN LAS COMUNICACIONES

Medidas y controles Aconsejables:

- Encriptación de datos
- Verificar autenticidad
- Numerar transacciones y medir tiempos
- Interrumpir en forma automática estaciones de trabajo
- Vigilar líneas telefónicas y detectar anomalías en líneas de comunicación
- Identificar y certificar identificación del usuario

Plan de Seguridad
Componentes
PROTECCIÓN CONTRA EL PERSONAL

Elaboración de un método de control: Implementar técnica de selección y determinar capacitación para el personal que utilizará equipos de cómputos.

Reglamentos estrictos de autorización: Reforzar operaciones básicas para reducir manipulación de datos.

Sesiones de Capacitación y Concientización Personal:

- Exponer y explicar reglamentos
- Informar a empleados sobre la utilidad medidas de seguridad
- Fomentar participación del personal en la detección de cualquier anomalía

Conclusiones

¿Podríamos como gerente de seguridad ver el futuro?
Saber que se aproxima un ataque, podríamos detenerlo, o al menos mitigar su impacto y ayudar a garantizar que lo que se necesita para proteger a la mayoría sea seguro.
El hecho es que si se puede ver lo que está en el horizonte. Muchas pistas están ahí fuera, y son obvias.

Pero….

¿Qué pasa si el entorno de seguridad falla?

Fin de la presentación

Muchas Gracias!!