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
- Plan de Contingencia
- Plan de Continuidad del Negocio
- Conclusiones

PLAN DE CONTINGENCIA
Y
PLAN DE CONTINUIDAD DEL NEGOCIO

CONSISTEN EN LOS PASOS A SEGUIR CUANDO UN SISTEMA ENTRA EN UNA SITUACIÓN DE CRISIS PARA RECUPERAR (AL MENOS EN PARTE) SU CAPACIDAD FUNCIONAL Y LUEGO CONTINUAR CON EL NEGOCIO

Es el último recurso cuando se producen fallas en la seguridad Física, Técnica o Administrativa

Plan de Contingencia

Plan de Contingencia

Concepto

CONTINGENCY PLAN

Estrategias, acciones, procedimientos, responsabilidades

minimizar impacto interrupción imprevista

funciones criticas y restaurarlas, dentro de tiempo fijado.

Se aplica a actividades de TIC

Plan de Contingencia

Concepto

Documento normativo que describe en forma
clara, concisa y completa
los riesgos, los actores y sus responsabilidades
en caso de eventos adversos

El Plan de Contingencias en un ambiente informático comprende los pasos a seguir cuando un sistema entra en una situación de contingencia para recuperar
(al menos en parte) su capacidad funcional.

Es el último recurso cuando se producen fallas en la Seguridad Física, Técnica o Administrativa

Plan de Contingencias

La existencia de un Plan de Contingencias permite:

- Apoyarse en medios técnicos y administrativos para prevenir siniestros, aumentando la confiabilidad y continuidad de los procesos computadorizados

- La recuperación total o parcial del servicio en el menor tiempo posible, mediante una detallada definición documentada de las acciones a tomar y los recursos necesarios durante y después de un siniestro

Plan de Contingencias

PASOS A SEGUIR EN SITUACIONES DE EMERGENCIA:

1ra Acción: Protección de la vida humana

2da Acción: Evaluación de daños y estimación de tiempo necesario para la recuperación

3ra Acción: Coordinación de las actividades de recuperación inmediatas

* Recuperar datos vitales y críticos
* Reconstruir bases de datos
* Instalar y probar el software en sede alternativa
* Reorientar el tráfico de comunicaciones
* Operar

Plan de Contingencias

PASOS A SEGUIR EN SITUACIONES DE EMERGENCIA:

4ta Acción: Coordinación de las actividades de recuperación definitivas

* Reinstalación del Hardware
* Restauración del software de base y de aplicación
* Reestablecer bases de datos
* Recuperación de la red y restablecer el tráfico de comunicaciones
* Reestablecer condiciones de seguridad
* Operar

5ta Acción: Gestión de aspectos legales derivados de la emergencia (incumplimiento de obligaciones - seguros)

Plan de Contingencias

SU ELABORACION

- El proceso de elaboración de un plan de contingencias implica un análisis de la explotación de los recursos y su grado de vulnerabilidad.

- Este análisis permite detectar con facilidad aquello aspectos a modificar que con carácter preventivo den a la organización oportunidades frente a las contingencias.

Plan de Contingencias

ACTIVIDADES PARA PLANIFICAR E IMPLEMENTAR UN PC

1. **Relevamiento** de: equipamiento, sistemas que se procesan, recursos que se utilizan, normas de seguridad existentes, siniestros probables, grado de criticidad de los procesos y períodos máximos con que se cuentan para el restablecimiento.

Plan de Contingencias

ACTIVIDADES PARA PLANIFICAR E IMPLEMENTAR UN PC

2. **Identificación de riesgos** ¿Qué está bajo Riesgo? Qué puede ir mal? ¿Cuál es la posibilidad que suceda?

3. **Evaluación de riesgo**

Los costos de un desastre pueden clasificarse en las siguientes categorías:

- Costos reales de reemplazar el sistema informático
- Costos por falta de producción.
- Costos por negocio perdido
- Costos de reputación.

Un seguro puede llegar a cubrir solamente el primer costo.

Plan de Contingencias

ACTIVIDADES PARA PLANIFICAR E IMPLEMENTAR UN PC

4. **Definición de las alternativas** ante cada siniestro, acciones a seguir y sus responsables

5. **Asignación de prioridades** a las aplicaciones

6. **Establecimiento de requerimientos** de recuperación.

Plan de Contingencias

ACTIVIDADES PARA PLANIFICAR E IMPLEMENTAR UN PC

7. **Elaboración de documentación** con actividades y procedimientos a seguir ante cada contingencia probable hasta restablecer el servicio del normal procesamiento de la información

8. **Verificación e implementación del plan**: entrenamiento del personal responsable y usuario y pruebas del correcto funcionamiento del Plan

9. **Distribución y mantenimiento del plan** con la realización de los simulacros previstos

Plan de Contingencias

CONTENIDO DEL PLAN

I. Determinación de prioridades en materia de recuperación de aplicaciones, software de base y archivos de datos, en función al grado de tolerancia con respecto a la interrupción

II. Detalle del orden de procesamiento de tareas

III. Listas de notificación, números de teléfono, mapas y direcciones de responsables

IV. Mecanismos de acoplamiento a los sistemas manuales durante interrupciones cortas

Plan de Contingencias

CONTENIDO DEL PLAN

V. Operaciones del mainframe y de las sedes remotas

VI. Disponibilidad de hardware alternativo: Propios o de Terceros (Hot sites, Warm sites, Cold sites)

VII. Disponibilidad capacidad de telecomunicaciones: Rutas alternativas y Rutas diversificadas

El Plan por sí solo no sirve si no hay:

CAPACITACION

RECURSOS

PRUEBA DEL PLAN

Plan de Contingencia
Capacitación

- ¿ Qué debo hacer?
- ¿ Qué deben hacer los demás?
- ¿ Cuándo debo hacerlo ?
- ¿ Cómo debo hacerlo ?
- ¿ Con qué recursos debo hacerlo ?

Plan de Contingencia
Recursos

- Análisis de las Necesidades
- Inventario de recursos disponibles
- Solicitud y Adquisición de recursos faltantes
- Verificar el correcto funcionamiento de los recursos

¿ Le parece costoso ?

Pruebe con no tener capacidad de respuesta

Plan de Contingencia
Prueba

- Ejercicio de simulación
- Simulacro
- Emergencia / desastre

EVALUACION

Plan de Continuidad del Negocio

Plan de Continuidad del Negocio

Concepto

BUSINESS CONTINUITY PLAN

Estrategias, acciones, procedimientos, responsabilidades

minimizar impacto interrupción imprevista

funciones criticas toda la empresa

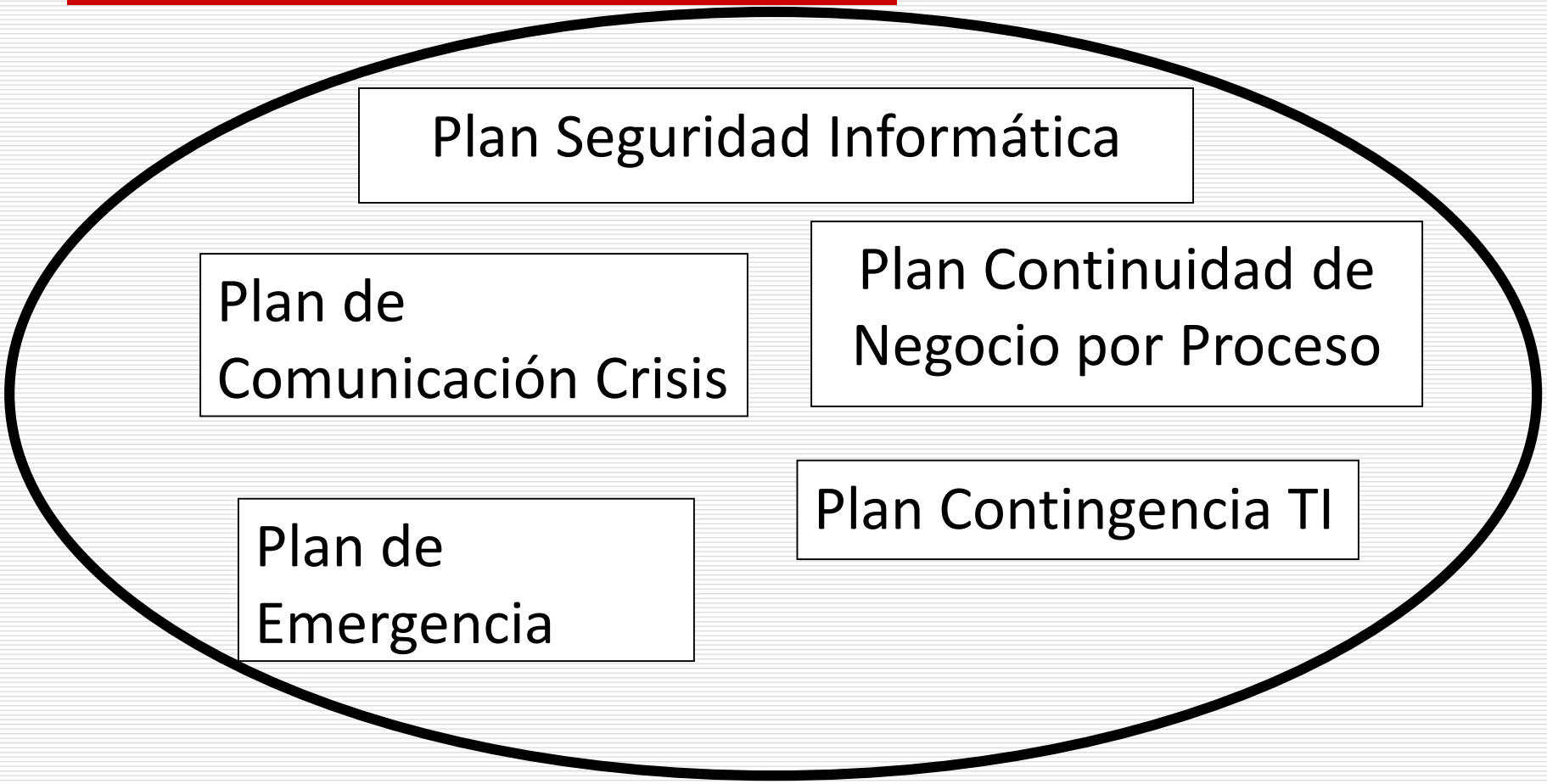
y restaurarlas, dentro de tiempo fijado.

Se aplica a todas actividades de la empresa

Plan de Continuidad del Negocio PCN

Sostiene funciones del negocio de una empresa durante y después de una interrupción a los procesos críticos del negocio

Plan de Continuidad del Negocio PCN



Plan de Continuidad del Negocio Integrantes

PLAN COMUNICACIÓN DE CRISIS

Procedimientos internos y externos

Comunicación al personal y público

Plan de Continuidad del Negocio Integrantes

PLAN DE EMERGENCIA

Procedimientos evacuación ante amenaza seguridad del personal, ambiente, etc.

Plan de Continuidad del Negocio Integrantes

PLAN DE CONTINUIDAD POR PROCESO DE NEGOCIO

Restaurar funciones críticas de negocio

Plan de Continuidad del Negocio Integrantes

PLAN DE CONTINGENCIA DE TI

Método alterno para sistemas generales y aplicaciones importantes

Plan de Continuidad del Negocio
ESTRUCTURA

- Evaluación de Riesgos
- Análisis de Impacto del Negocio
  Estrategia de Continuidad
- Estructura organizativa PCN
- Procesos y Procedimientos PCN
- Plan de Pruebas PCN

Plan de Continuidad
Fases

FASE I - ADMINISTRAR EL RIESGO

- Evaluación del riesgo de interrupción
- Análisis del impacto sobre el negocio

FASE II - CREAR EL PLAN

- Estrategia de Recuperación alternativas
- Requerimientos críticos Recursos de recuperación
- Plan de Continuidad del Negocio

FASE III - PROBAR Y ADMINISTRAR EL PLAN

- Administración del Plan
- Prueba del Plan

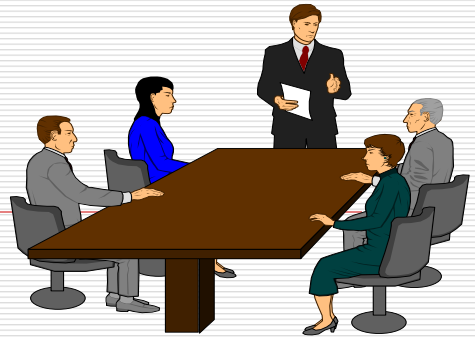
QUIEN ES EL RESPONSABLE

del Plan de Continuidad ?

El/los gerente/s deberá/n asegurarse de que el Plan de Continuidad de Negocio sea:

Un proyecto estratégico de toda la organización

Para que la información no deje de fluir garantizando llegue a los responsables de llevar adelante el negocio



Quien se ocupa de que: …

Análisis del Riesgo del Negocio

Objetivos del Análisis de riesgo

- Análisis y reducción de riesgos a los que está expuesta la organización
- Identificación de amenazas y vulnerabilidades
- Identificación de riesgos potenciales – probabilidad – frecuencia - consecuencias
- Determinar los niveles de aceptabilidad de riesgo – Alternativas
- Compromiso de la Dirección

Análisis del Impacto en el Negocio

Objetivos del Análisis de Impacto

- Definir los tipos de impacto (económicos, jurídicos, comercial, operacional, de imagen, etc)
- Identificar las funciones críticas de la organización y su interdependencia
- Identificar impacto ente la interrupción de cada una de ellas
- Identificar las funciones de recuperación y logística
- Identificar los recursos para recuperar funcionalidades mínimas y normales

Análisis del Impacto en el Negocio

Tipos de Impacto

- Incremento de costos y gastos – cuantitativa
- Peligro para las personas – cualitativa (bajo – medio – alto) cuantitativa
- Impacto operacional – cualitativa – cuantitativa
- Impacto comercial – continuidad – confiabilidad – jurídica – cualitativa – cuantitativa
- Impacto en calidad – en corto o largo plazo
- Pérdidas de ingresos y beneficios – cuantitativa

Análisis del impacto en el Negocio

Tipos de Impacto (Cont.)

- **Impacto ambiental – en la población o medio ambiente – sanciones – multas – imagen – cuantitativo**
- **Impacto en la imagen – cualitativo en el corto plazo – cuantitativo en el largo plazo**
- **Impacto en la moral del personal – cualitativa - cuantitativa**

Selección de Estrategias

Objetivos del desarrollo de estrategias:

- Estudiar alternativas posibles, ventajas, inconvenientes, costos incluyendo medida de reducción de riesgo
- Contrastar con las áreas factibilidad de las estrategias
- Necesidades externas, guardas de Back ups, centros de operación alternativos (Cold/Warm/Hot Sites)
- Consolidar todas las estrategias con el OK de las unidades de negocios
- Aprobación por la dirección

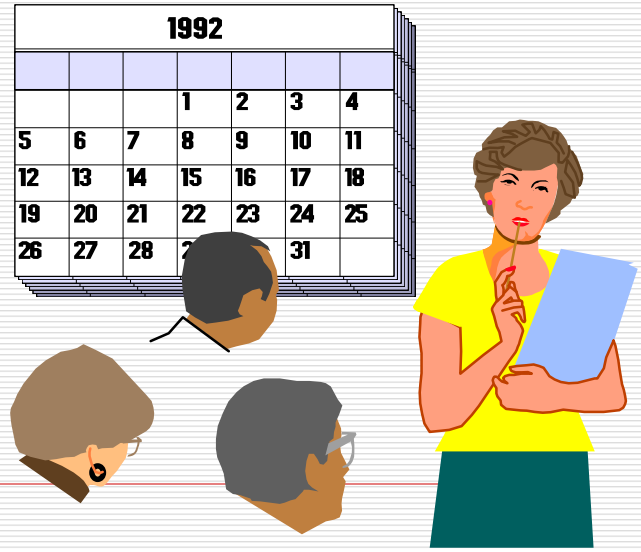
Pruebas y Mantenimiento

Objetivos:

- Mantenimiento actualizado del Plan
- Preparación adecuada del personal

Y contar con:

- Revisiones periódicas
- Ejercicios de entrenamiento
- Pruebas



Normativas Legales

Argentina:

Ley 25.326 – Protección de Datos Personales

-Procedimientos para efectuar copias de respaldo y de recuperación de datos

-Copias de respaldo: externas. Deberá disponerse de un procedimiento de recuperación de información y su tratamiento en caso de contingencias que pongan no operativo el/los equipos de procesamiento habituales.

Mundial:

Normas ISO/IEC contienen capítulos íntegros dedicados a la Continuidad del negocio (ISO 27006; BS 25999)

Normativas Legales

Argentina:

BCRA, ente regulador del sistema financiero

Contingencia del PED (Com. A 4609)

Crear, mantener y probar un plan de recuperación del PED operable y funcional, acorde a los requerimientos de negocio y de los organismos de control.

Riesgo Operacional (Com. A 4854)

Contar con planes de contingencia y continuidad de la actividad que aseguren la prosecución de su capacidad operativa y la reducción de pérdidas en caso de interrupción de la

actividad. Pruebas periódicas planes de recuperación y de continuidad del negocio.

Gestión Integral de Riesgos (Com. A 5203)

Plan Contingencia de todos los riesgos del negocio.

Conclusiones

¿Podríamos como gerente de seguridad ver el futuro?
Saber que se aproxima un ataque, podríamos al menos mitigar su impacto.
El hecho es que si se puede ver lo que está en el horizonte. Muchas pistas están ahí fuera, y son obvias.

Fin de la presentación

Muchas Gracias!!