Gestión de Tecnologías de la Información - SIG

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 evaluar 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
- Resiliencia Operacional
- Plan de Continuidad del Negocio
- Plan de Contingencia
- Conclusiones

RESILIENCIA OPERACIONAL

CAPACIDAD DE UNA ORGANIZACIÓN PARA CONTINUAR CON SUS OPERACIONES CRÍTICAS DURANTE SITUACIONES DISRUPTIVAS DE CUALQUIER NATURALEZA.

Abarca personas, procesos, tecnología e información

RESILIENCIA OPERACIONAL

CAPACIDAD DE PERMANECER VIABLE EN UN ENTORNO VOLATIL.

PLAN DE CONTINUIDAD DEL NEGOCIO
Y
PLAN DE CONTINGENCIA

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

RESILIENCIA OPERACIONAL
PLAN DE CONTINUIDAD DEL NEGOCIO
PLAN DE CONTINGENCIA

RESILIENCIA OPERACIONAL
PLAN DE CONTINUIDAD DEL NEGOCIO
PLAN DE CONTINGENCIA

Aspecto	Resiliencia Operacional	PCN/PC
Enfoque	Continuidad y adaptación	Recuperación
Naturaleza	Estratégica y transversal	Procedimental
Objetivo	Mantener operaciones bajo cualquier condición	Restablecer funciones críticas
Activación	Opera todo el tiempo	Se activa ante incidentes

Plan de Continuidad del Negocio

Plan de Continuidad del Negocio PCN

Recopilación documentada de procedimientos e información para su uso en un incidente con el objetivo de permitir que una organización continúe entregando sus productos y servicios críticos a un nivel aceptable

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

Plan de Continuidad del Negocio
PCN - Componentes

Plan Seguridad de la Información

Plan de Comunicación Crisis

Plan Continuidad de Negocio por Proceso

Plan de Emergencia

Plan Recuperación ante Desastres

Plan Contingencia TIC

Plan de Continuidad del Negocio
Componentes

PLAN COMUNICACIÓN DE CRISIS

Procedimientos internos y externos
Comunicación al personal y público

Plan de Continuidad del Negocio Componentes

PLAN DE EMERGENCIA

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

Plan de Continuidad del Negocio Componentes

PLAN DE CONTINUIDAD POR PROCESO DE NEGOCIO

Restaurar funciones críticas de negocio

Plan de Continuidad del Negocio Componentes

PLAN DE CONTINGENCIA DE TI

Método alterno para sistemas generales y aplicaciones importantes

Plan de Continuidad del Negocio Componentes

PLAN DE RECUPERACION ANTE DESASTRES (PRD)

Plan reactivo ante una posible catástrofe, mayor enfoque en lo técnico.

Plan de Continuidad
Fases de elaboración

FASE I - ADMINISTRAR EL RIESGO

FASE II - CREAR EL PLAN

FASE III - PROBAR Y ADMINISTRAR EL PLAN

Plan de Continuidad
Fases de elaboración

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 - TESTEAR Y ADMINISTRAR EL PLAN

- Capacitación, concientización, mantenimiento del Plan
- Testeo del Plan

Plan de Continuidad del Negocio

CONTENIDO DEL PLAN

a) **Procedimientos para la declaración de una situación de crisis y los criterios para activar planes vinculados.**

b) **Asignación de responsabilidades para la ejecución de planes de recuperación.**

c) **Procedimientos detallados de recuperación, identificación de la infraestructura, los sistemas y componentes críticos, y su prioridad**

Plan de Continuidad del Negocio

CONTENIDO DEL PLAN

d) **Procedimientos para el traslado de actividades esenciales a ubicaciones alternativas.**

e) **Establecimiento de canales de atención alternativos para clientes.**

f) **Medidas que aseguren integridad y confidencialidad de la información crítica durante los procesos de recuperación.**

Plan de Continuidad del Negocio ESTRUCTURA

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

QUIEN ES EL RESPONSABLE del Plan de Continuidad ?

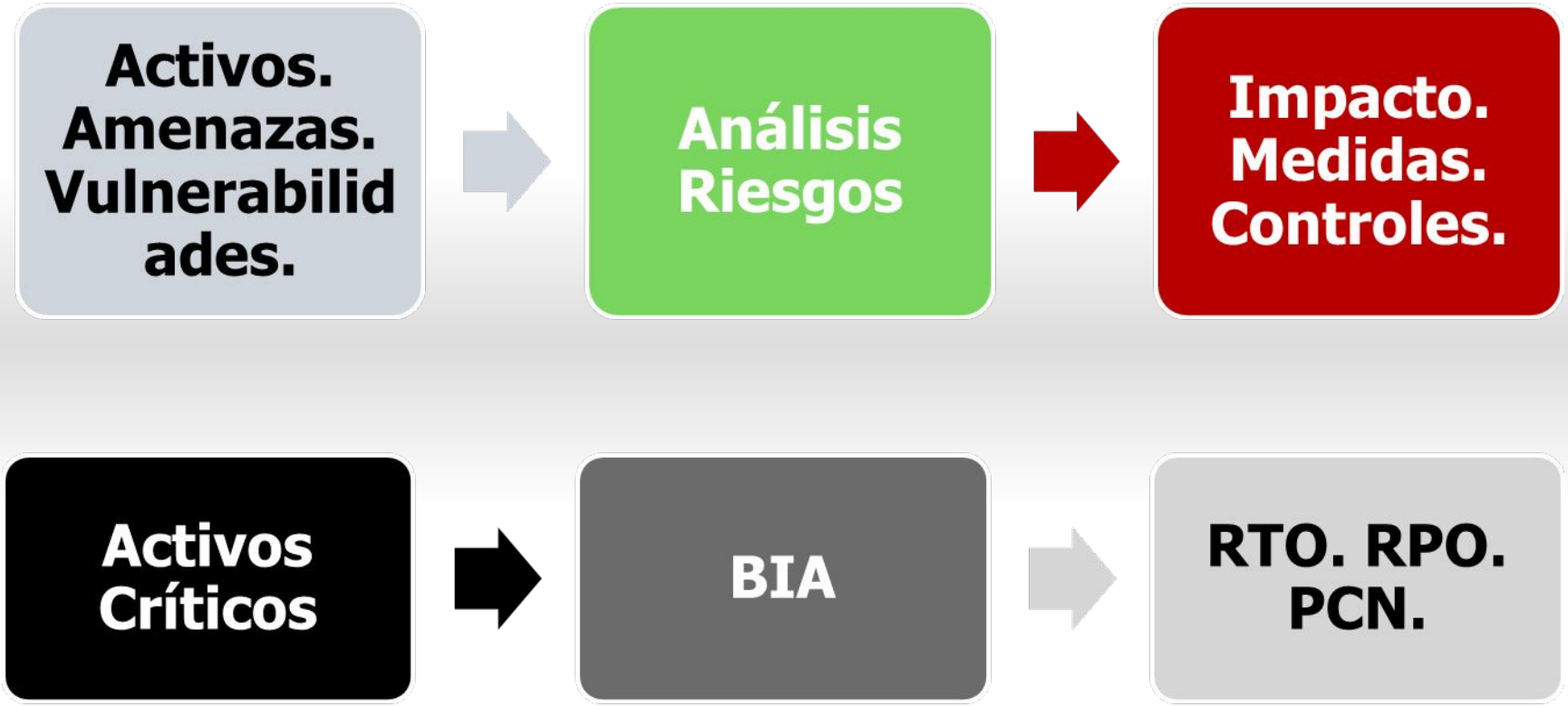
El/los gerente/s deberá/n asegurarse de que el Plan de Continuidad de Negocio sea:

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 de Riesgos (AR) versus Análisis de Impacto del Negocio (BIA)



Análisis del Impacto en el Negocio (BIA)

Objetivos del Análisis de Impacto del Negocio (BIA)

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

Análisis del Impacto en el Negocio (BIA)

Tipos de Impacto

- Incremento de costos y gastos (cuantitativo)
- Peligro para las personas (cualitativo – cuantitativo)
- Impacto operacional (cualitativo – cuantitativo)
- Impacto comercial (cualitativo – cuantitativo)
- Impacto reputacional (cualitativo en el corto plazo – cuantitativo en el largo plazo)
- Impacto ambiental (sanciones – multas)

Análisis del Impacto en el Negocio (BIA)

Proceso BIA

1) Definir criterios para evaluar impactos relevantes para la resiliencia y la continuidad.
2) Identificar actividades que soportan la prestación de los productos y servicios.
3) Identificar interconexiones e interdependencias internas y externas de los procesos críticos.
4) Identificar posibles incidentes disruptivos y la evaluación de su impacto.
5) Objetivos de recuperación en relación con el tiempo y a la pérdida de datos (RTO/RPO).
6) Comunicar resultados obtenidos a la Dirección Superior

Selección de Estrategias

Objetivos del desarrollo de estrategias:

- Estudiar alternativas posibles, ventajas, inconvenientes, costos incluyendo medida de reducción de riesgo
- Contrastar con las áreas, la 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 superior

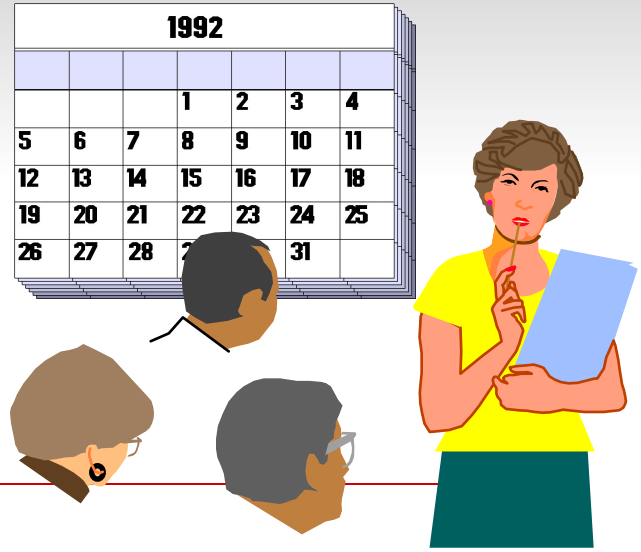
Capacitación, Testeo y Mantenimiento

Objetivos:

- Capacitación y Concientización del personal
- Mantenimiento actualizado del Plan

Y contar con:

- Revisiones periódicas
- Ejercicios de entrenamiento
- Pruebas



Plan de Contingencia

Plan de Contingencia

- ✔ **Concepto**
- ✔ **Objetivos**
- ✔ **Implementación**
- ✔ **Contenido**

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

Objetivos

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

- **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
Objetivos

Definir:

RPO (Recovery Point Objective -Objetivo de Punto de Recuperación-): pérdida máxima de información tolerable en caso de interrupción.

RTO (Recovery Time Objective -Objetivo de Tiempo de Recuperación-): Tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio.

Plan de Contingencias

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

IMPLEMENTACION

1. **Relevar**
2. **Identificar Riesgos**
3. **Evaluar Riesgos y Escenarios**
4. **Definir Estrategias**
5. **Asignar prioridades**
6. **Establecer Requerimientos**
7. **Documentar**
8. **Implementar, Testear y Capacitar**
9. **Distribuir y Mantener plan**

Plan de Contingencias

IMPLEMENTACION

1. **Relevamiento**: 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

IMPLEMENTACION

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

3. **Evaluación de riesgos y escenarios**

Asociados con:

- **Ubicación geográfica**
- **Susceptibilidad a amenazas**
- **Proximidad con infraestructuras críticas de todas las instalaciones, incluidas terceras partes.**
- **Eventos de interrupción simultáneos.**

Plan de Contingencias

IMPLEMENTACION

3. Evaluación de riesgos y escenarios

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

IMPLEMENTACION

4. **Definición de estrategias** 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

IMPLEMENTACION

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. **Implementación, Testeo y Capacitación del plan**: entrenamiento del personal responsable y usuario; pruebas del correcto funcionamiento del Plan

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

Plan de Contingencias

CONTENIDO MINIMO DEL PLAN

I. Prioridades de recuperación de activos de información críticos 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

Plan de Contingencias

CONTENIDO MINIMO DEL PLAN

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

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 y CONCIENTIZACION

RECURSOS

TESTEO DEL PLAN

Plan de Contingencia
Programa de Capacitación y Concientización

- ✓ ¿ 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
Testeo de la Contingencia

- Ejercicio de simulación
- Simulacro
- Emergencia / desastre

EVALUACION

Plan de Emergencia

PASOS A SEGUIR:

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 Emergencia

PASOS A SEGUIR:

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)

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.**

Normativas Legales

Argentina:

BCRA, ente regulador del sistema financiero

Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información (Com. A 7724)

Ciberresiliencia en la continuidad del negocio

Medidas proactivas en el diseño de operaciones y procesos que permitan mitigar el riesgo de eventos disruptivos y mantener la confidencialidad, integridad y disponibilidad.

Lineamientos Respuesta y Recuperaciones ante Ciberincidentes (Com. A 7266)

Prácticas efectivas de respuesta y recuperación ante ciberincidentes con el fin de limitar riesgos en la estabilidad financiera e impulsar la ciberresiliencia del ecosistema en su conjunto.

Normativas Legales

Argentina:

BCRA, ente regulador del sistema financiero

Gestión Integral de Riesgos (Com. A 8249)

Resiliencia Operacional. Plan Contingencia de todos los riesgos del negocio.

Mundial:

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

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!!