Planificación de auditoría remota

- Cómo preparar una auditoría remota?
- Competencias adicionales
  - Evaluación de riesgos – CID y Privacidad de datos
    - Legislación y normativa
    - Requisitos de Seguridad

Planificación de auditoría remota

- Cómo preparar una auditoría remota?
  - Competencias adicionales
    - Evaluación de controles
      - Tecnológicos
        - Falla de comunicación (corte/latencia)
        - Dificultad en al acceso a registros o evidencias
      - Operativos
        - Falta de muestreo o ausencia de criterio objeivo
        - Incumplimiento de horarios

Planificación de auditoría remota

- Cómo preparar una auditoría remota?
  - Competencias adicionales
    - Evaluación de controles –Elementos a tener en cuenta-
      - Tecnología
        - Videoconferencias
        - Portales
        - Acceso remoto a aplicaciones

Planificación de auditoría remota

- Aspectos a tener en cuenta
  - Situación del auditor
    - Auditorías anteriores
    - Tecnología disponible ==>
    - Nuevas pautas de auditoría ==>
  - Situación del Organismo a auditar
    - Servicios que brinda
    - Cambios en los procesos (presencial/virtual)

Planificación de auditoría remota

- Aspectos a tener en cuenta
  - Tecnología disponible
    - Equipamiento (organizacional/propio)
    - Conectividad (a través organización/propio)
    - Herramientas tecnológicas (organizacional/propio)
    - Capacitación / Competencia
  - Nuevas pautas de auditoría
    - Metodología de auditoría remota
    - Pruebas de cumplimiento y sustantivas

Planificación de auditoría remota

Guía de procedimientos en la fase de planificación

4. Elaborar el programa de Auditoría de la fase de ejecución (cont.).

- Evaluación de riesgos del área/proceso.
  - Evaluación de riesgos y controles

Guía de procedimientos en la fase de planificación

4. Elaborar el programa de Auditoría de la fase de ejecución (cont.).

Identificar Riesgos

- Qué puede suceder?
- Cómo puede suceder ?

Riesgo inherente

Identificación de Riesgos

Identificación de amenazas de cada activo

Naturales → Inundaciones, terremotos, tornados, avalanchas, tormentas eléctricas, etc.

Humanas → Eventos causados u ocasionados por el hombre.

- **Intencionales** → Ataques basados en red, software malicioso, accesos no autorizados a información, etc.
- **No intencionales** → Gestión de cambios, Complejidad de TI, errores, etc.

Ambientales → Interrupción prolongada de energía, polución, químicos, etc.

Fuente: Taller sobre Políticas de Seguridad dictado por ArCERT (ONTI) - 2005

Identificación de Riesgos

Identificación de amenazas de cada activo

ACCIONES que pueden formar parte de la materialización de la amenaza.

Por ejemplo, un acceso no autorizado a información sensible puede ser concretado mediante la implementación de técnicas como ingeniería social, intrusión, etc..

MOTIVACIÓN que puede llevar a la existencia de una amenaza

Por ejemplo, un acceso no autorizado a información sensible podría estar motivado por beneficios económicos a futuro.

CAPACIDAD que debe poseer la fuente de amenaza para llevar a cabo una acción.

En el ejemplo anterior, el atacante debe contar con los conocimientos requeridos para concretar el acceso, como ser, diversas técnicas de hacking.

Fuente: Taller sobre Políticas de Seguridad dictado por ArCERT (ONTI) - 2005

Identificación de Riesgos

Identificación de amenazas de cada activo

Sistema de Información	Componente	Fuente de amenaza	Acciones de la amenaza	Motivación	Capacidades
Sistema XXX	Programa XX	Usuarios internos	-Intrusión, etc. -Acceso no autorizado -Código malicioso, etc.	Curiosidad Venganza Inteligencia	Conocimientos de programación, redes, etc.
		Suministro de energía	Corte de energía	Desperfecto Huelga	N/A

Fuente: Taller sobre Políticas de Seguridad dictado por ArCERT (ONTI) - 2005

Identificación de Riesgos

Identificación de vulnerabilidades de cada activo

Sistema de Información	Componente	Vulnerabilidad	Fuente de amenaza	Acciones de la amenaza
Sistema XXX	Programa XX	-Errores de diseño del sistema -Falta de control de acceso	Usuarios internos	-Intrusión, etc. -Acceso no autorizado -Código malicioso, etc.
		Falta de UPS	Suministro de energía	Corte de energía

Fuente: Taller sobre Políticas de Seguridad dictado por ArCERT (ONTI) - 2005

Control de los Sistemas de Información

Políticas, métodos y procedimientos adoptados por una organización para asegurar la protección de su información, la exactitud y confiabilidad de la información, de la promoción de la eficacia y eficiencia administrativa y adhesión a los estándares de trabajo en la gestión informática.

Objetivo de Control de TI

"Una declaración del resultado a obtener o el propósito a lograr mediante la implementación de procedimientos de CONTROL en una actividad particular de TI"

Fuente: COBIT

Objetivos de control y los controles

Objetivo de control	Medida de control
Es una meta que está relacionada de manera explícita con la estrategia de la Organización.	Es una actividad que contribuye al cumplimiento del objetivo de control.

- Tanto el objetivo de control como la medida de control sirven a la descomposición de las metas de nivel estratégico en metas y actividades de bajo nivel que pueden asignarse al personal como tareas.
- La asignación puede tomar la forma de una descripción de funciones para una descripción del trabajo.

Objetivos de control y los controles Ejemplos

Objetivo de control	Medida de control
Control de Acceso	• Gestión de acceso de usuario • Responsabilidades del usuario • Control de acceso a sistemas y aplicaciones
Seguridad Física y Operativa	• Areas seguras • Seguridad del hardware • Copias de seguridad • Protección ignífuga • Control biométrico

¿ Para qué se implementan los controles ?

Los controles se implementan para mitigar los riesgos identificados.

Los pasos son:

1. Identificar riesgos
2. Seleccionar riesgos críticos – evaluar impacto y probabilidad de ocurrencia -
3. Evaluar las implicancias, costos, eficiencia, etc. de implementar controles.
4. Decidir si asumir el riesgo vs implementar controles.

Clasificación del Control

Según el momento de aplicación

- Preventivo
- Detectivo
- Correctivo

Según su desarrollo

- Discrecional
- No discrecional

Según su Imposición

- Voluntario
- Mandatorio

Clasificación del Control (Cont.)

Controles Generales	Al estar presentes, proveen control total sobre las actividades de sistemas de información	• Operaciones con los datos, de acceso • Software, de desarrollo y mantenimiento
Controles de aplicación	Proveen *controles específicos* sobre una aplicación para dar seguridad razonable que las transacciones son autorizadas y registradas y que todas son procesadas sin errores y en el período correcto	• Procesamiento completo y exacto. • Autorización y validación de las transacciones

Identificación de Controles

Identificación de controles de cada activo

Sistema de Información	Vulnerabilidad	Fuente de amenaza	Acciones de la amenaza	Control esperado	Prueba de Cumplimiento	Prueba Sustantiva	Observación
Sistema XX	-Errores de diseño del sistema	Usuarios internos		Detectivo Log del sistema			
			-Acceso no autorizado	Preventivo Mandatorio PSW / ID	•		
			-Código malicioso, etc.	Preventivo No uso dispositivo USB			
	UPS inoperativa	Suministro de energía	Corte de energía	Preventivo Mantenimiento			