Seguridad y Auditoría Informática

Principios de Auditoría, Evaluación de Riesgos y Reportes Efectivos

Objetivos

- Identificar términos básicos de Auditoría
- Comprender el Rol de la Auditoría en la mitigación de Riesgos
- Integrar herramientas de Identificación de Riesgos y Causa Raíz
- Reconocer los pasos del Proceso de Auditoría

Metodología General

¿Cómo auditar la Seguridad en una empresa?

- "Empezar por auditar algo pequeño"

Proceso de Auditoría basado en Riesgos

- Auditar desde afuera hacia adentro
- Pequeñas piezas del total

Términos de Auditoría

Auditoría

Medir algo contra un estándar

Los 3 lugares más comunes para aplicar **auditoría** en tecnología de la información y **seguridad** de la información son:

- Nivel de Política
- Nivel de Procedimiento
- Nivel de Sistema (o Nivel de Aplicación)

Términos de Auditoría (2)

Tipos de Auditoría

- Auditoría de Conformidad
- Auditoría de Seguridad
- Auditoría Financiera

Preguntas de Auditoría

- Política de Seguridad Implementada
  - ¿Se cumple?
  - ¿Es efectiva?
- Nuevo Firewall (o sistema de seguridad)
  - ¿Está realmente protegiéndonos?
- Si nos dicen que los sistemas están totalmente parchados y asegurados…
  - ¿Qué pregunta realizamos en cada caso?

Objetivo Principal de la Auditoría

- La función del auditor es actuar como una herramienta de la Dirección para medir y reportar sobre riesgos
- Una función secundaria es reducir el riesgo a través de la concientización

Términos de Auditoría (3)

Evaluación

- Medición/Estimación
  - Riesgo
  - Amenaza
  - Vulnerabilidad
  - Costo de Exposición

¿Qué tan bien aseguramos un sistema? ¿Qué más puede salir mal?

Términos de Auditoría (4)

Alcance

- Lo que estamos auditando o evaluando
  - También conocido como "Entidad Auditable"
  - Área de Autoridad
  - Área de Responsabilidad - Definir el **Qué**

¿Quién Define el Alcance?

- Definido por:
  - Solicitante de la Auditoría
  - La Dirección
  - ¿El Auditor?
- Tener cuidado con "Arrastrar el Alcance"
- ¡Tener más cuidado con exceder su autoridad!

El "Qué" versus el "Cómo"

- Qué = Alcance
  - ¿No necesito considerar el "Cómo"?
    - Si, pero en una etapa posterior

¿Cómo hacer una validación técnica de un firewall?

Validación Técnica de Firewall

- Si revisa las reglas, solamente sabe lo que las reglas dicen
  - ¿Están funcionando bien en realidad?
  - ¿Cómo saberlo?
- Un firewall "validado" debe ser testeado
  - Disparando paquetes al firewall
  - Disparando paquetes a través del firewall
  - Entendiendo cómo la información debe moverse a través del firewall
- ¿Es este "Cómo" más difícil que solamente ver las reglas?

El "Cómo"

Considerando el "Cómo" de manera temprana

- ¿Si no sabemos el "Cómo", que vamos a hacer?
  - En muchos casos, ¡ajustamos el alcance o los objetivos de auditoría!
- Si cambiamos el alcance u objetivos (el “Qué”), estamos limitando o modificando los riesgos que queríamos medir originalmente.

Términos de Auditoría (5)

Objetivo

- La meta o fin de:
  - Política
  - Procedimiento
- o:
  - La auditoría
  - La evaluación

Objetivos de la Política

Objetivo de la Política

- ¿Por qué existe esta política?
- ¿Cómo se relaciona a la misión?
  - ¿Cómo protege a la misión?

"Todos los usuarios deben autenticarse con un usuario y contraseña"

- **¿Qué objetivo sugerirían?**

Términos de Auditoría (6)

Control

- Indica cómo alcanzamos nuestros objetivos
  - Responde la pregunta "Cómo sabemos que..."
  - (Ejemplo) **Objetivo**: Autenticación de usuario requerida
    - **Control**: Controlador de Dominio Active Directory
    - **Control**: Registro de Eventos (logon/logoff/fallas de autenticación)

Términos de Auditoría (7)

Excepción de Auditoría

- Elemento que falla el cumplimiento del criterio de auditoría
- Control que falla para cumplir su objetivo

Términos de Auditoría (8)

Remediación

- ¿Qué hacemos para corregirlo?
  - Recomendaciones basadas en mejores prácticas
  - Recomendaciones basadas en políticas
  - Recomendaciones basadas en procedimientos

Términos de Auditoría (9)

Mitigación

- Qué hacemos para reducir pérdidas/daños
  - Recomendaciones basadas en mejores prácticas
  - Recomendaciones basadas en políticas
  - Recomendaciones basadas en procedimientos

Términos de Auditoría (10)

Causa Raíz

- Lo que realmente salió mal…
  - No necesariamente está conectado de manera directa con la excepción de auditoría.

Si las auditorías realizadas periódicamente continúan produciendo las mismas excepciones, no se está identificando la causa raíz.

Síntesis

- Auditoría…
  - … es una medición de conformidad (contra un estándar)
  - ... es Cómo verificar algo
  - ... puede incluir Evaluaciones

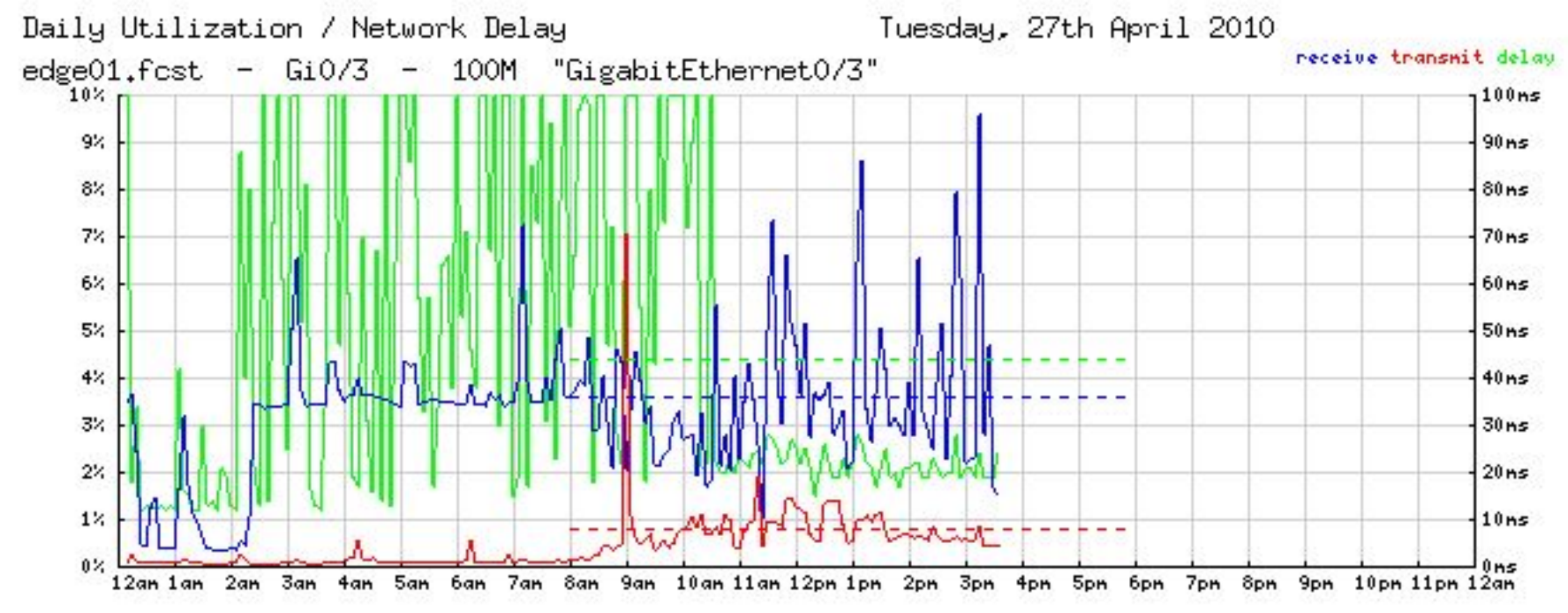
Líneas de Base

- Medición de un Sistema en un Estado Bueno Conocido
- Usado para medir el estado actual de un Sistema
- Una de las mejores herramientas/métodos de Auditoría
- "Línea de Base" es también usada para describir la configuración de un sistema

Usando Líneas de Base

- ¡Las Líneas de Base son de gran ayuda para la automatización!
  - Permiten auditar procesos en lugar de configuraciones
- Para éste trabajo, la línea de base debe ser confiable
  - También debe ser útil…
  - Ser creativo en lo que se usa como punto de referencia y tener en claro el por qué

Línea de Base de Tráfico de Red



Seguridad Basada en Tiempo (TBS)

- Auditar o Evaluar a través del tiempo como una dimensión primaria
- La Auditoría típicamente mide en qué medida uno sabe
- TBS mide qué tan bien/cuánto tiempo
- TBS puede medir pérdidas potenciales/reales

Seguridad Basada en Tiempo (TBS) - Ejemplo - Air Canada y WestJet

- WestJet obtiene cierta “inteligencia competitiva”
  - Un antiguo empleado de Air Canada trabaja ahora para WestJet
  - Air Canada le suministró acceso a un sitio interno
    - Información de carga de pasajeros, etc.
    - Intentado para ser usado en reserva de vuelos para empleados
  - El antiguo empleado le permite a WestJet usar su cuenta
- WestJet extrae información masivamente de 200.000 transacciones durante más de tres meses
- ¿Se puede detectar? ¡Por supuesto, las transacciones tenían logs!
  - La pregunta real es qué tan rápido y qué tan bien

COBIT

- Objetivos de Control para Tecnologías de la Información (**C**ontrol **OB**jectives for **I**nformation and related **T**echnology)
  - Estándar aceptado para Seguridad de Tecnologías de la Información
  - Provee un Marco de Trabajo
  - Provee Prácticas de Control
  - http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

Estándares de Seguridad

- ¿Se puede decir que se repiten?
  - FIPS, FISMA, DIACAP, GLB, HIPAA, C&A, ISO-27001, SARBOX, etc.
- ¿Cuál implemento?
  - ¿Cómo?
  - ¿Qué pasa si estoy sujeto a más de uno?
- ¡Evaluación de Riesgos!

Estándares y Listas de Control

Los estándares proveen una buena base para las listas de control

- Listas de Control propias de los Estándares
- Listas de Control para comprobar controles
- Listas de Control que buscan medir la conformidad

Listas de Control

- Declaración de Propósito/Alcance
- Mejor Práctica
- Qué Comprobar/Medir
- Cómo Comprobar/Medir

Política y Auditoría

- Una Buena Política es necesaria para una Buena Auditoría
  - La Política responde quién, qué y por qué
  - El Procedimiento dice quién hace qué, cuándo y cómo
  - La Auditoría mide el rendimiento de la organización con respecto a la Política y el Procedimiento
  - El Manejo de Incidentes y la Auditoría pueden también servir como herramientas de evaluación de Políticas/Procedimientos.

Política -> Procedimiento -> Auditoría

- **Política**: “Todos los equipos de escritorio **deben** tener software antivirus con las firmas más recientes cuando son desplegados. Adicionalmente, todos los sistemas **deben** ser configurados para actualizar automáticamente las firmas de virus semanalmente.”

Política -> **Procedimiento** -> Auditoría

- **Procedimiento de TI**: ”El Administrador se asegurará que todos los nuevos sistemas desplegados tengan instalado el software antivirus XXXX. El sistema debe ser configurado para obtener nuevas firmas desde xxxx.xxxx.com cada semana, 1 hora después de que el sistema es iniciado.”

Política -> **Procedimiento** -> Auditoría

- **Procedimiento de la Organización**: ”Los empleados no deberían deshabilitar el software antivirus instalado por el Departamento de TI. Si el software reporta la detección de un virus, llamar al número xxxx y hablar con xxxx para reportar el incidente.”

Prueba de “Límite de Velocidad”

- **Objetivo**: Incrementar la seguridad vial, reducir accidentes fatales
- **Control**: Límite de velocidad
- ¿Son estas señales de tráfico suficientes?
- **“¡Llamar a éste número si usted está yendo rápido!”**

Síntesis

- Nombramos algunos estándares de Auditoría
- Estrategias de Auditoría
  - Líneas de Base
  - Seguridad Basada en Tiempo
- Definimos Alcance
- Política como una Herramienta de Auditoría
  - Política -> Lista de Verificación
  - Lista de Verificación -> Política

¿Cómo ayuda la Auditoría?

Amenazas: Identificación y Evaluación

Vectores de Amenaza

- Internos
  - Intencional
  - Accidental
- Externos
  - Intención de Pérdida o Daño
  - Accidental

Amenazas Internas

Intencional	Accidental
Eliminación de un Sistema de Archivos	Eliminación de un Sistema de Archivos
Exposición de Propiedad Intelectual	Exposición de Propiedad Intelectual
Lanzamiento de “Malware”	Lanzamiento de “Malware”
Uso inapropiado de activos	Uso inapropiado de activos

Amenazas Internas (2)

- **La Amenaza**: El Administrador recibe un correo indicando que un archivo adjunto infectado ha sido puesto en cuarentena en el servidor de correos corporativo.

Amenazas Internas (3)

- **La Amenaza (Toma 2)**: El Administrador está logueado como Administrador de Dominio aunque en realidad no está realizando tareas que requieran acceso administrativo.

Amenazas Internas (4)

- **La Amenaza (Toma 3)**: El Administrador hace doble click en el adjunto infectado para ver qué tiene adentro.

Amenazas Internas (5)

- **La Vulnerabilidad**: Como Administrador de Dominio, todos los controles de acceso sobre archivos se vuelven ineficaces.

Amenazas Internas (6)

- **La Exposición**: El virus corre contra el controlador de dominio, los recursos compartidos que están montados y otros dispositivos montados.

Amenazas Internas (7)

- ¿Cuáles objetivos no fueron alcanzados?
- ¿Cuáles controles fallaron?
- ¿Cuál fue la causa raíz?

Amenazas Internas (8)

Un empleado puede ser malicioso debido a:

- Castigo
- Despido
- Rebeldía

Evaluación Práctica de Riesgos

Objetivos

- Entender la Aplicación de Controles y Estándares
  - ¿Por qué lo que hacemos hoy no funciona?
- Comprender los Resultados de la Evaluación de Riesgos
  - Selección de una Estrategia
- Definir una Evaluación de Riesgos que funciona
  - Utilizándose para Especificar Controles

Controles y Estándares

Las organizaciones requieren cumplir con estándares

- Método Típico
  - Crear un equipo
  - Revisar el estándar y asignar tareas
  - Progresivamente aplicar los controles a la organización

Las Organizaciones Fallan en las Auditorías

¿Por qué fallamos luego de seguir este método?

- Controles…
  - Han sido aplicados sin analizar previamente riesgos
  - Son aplicados sin una consideración real de su propósito
  - Son aplicados solo por aplicarlos
  - Son aplicados a la porción incorrecta de un proceso
  - No controlan causas raíz de las excepciones

La Hipótesis

- Las organizaciones aplican los controles de forma incorrecta
- ¿Qué podemos hacer con eso?

El Proceso Correcto

Identificar un Estándar

- Esto ya está prácticamente hecho…
  - FISMA, PCI/DSS, ISO-17799/27001…
- Identificar Procesos Críticos
  - Misión organizacional, procesos de negocio centrales
- Realizar Evaluaciones de Riesgo Progresivas (sobre Confidencialidad, Integridad y Disponibilidad)
  - Empezar a alto nivel e ir descendiendo
- La salida de la Evaluación de Riesgos debería identificar causas reales de riesgo
  - Para reducir los riesgos, ¡seleccionar controles desde el estándar que controlen los riesgos!

Resultados de la Evaluación de Riesgos

Para que ésto funcione, la Evaluación de Riesgos debe…

- ... ser usable y repetible
- ... identificar riesgos inaceptables
- ... identificar causas subyacentes de estos riesgos
- ... establecer puntos de control para el riesgo evidente

Selección de la Estrategia

Lo que necesitamos:

- Identificar riesgos inaceptables (con respecto a **C.I.D.**)
  - Fallas de controles críticos
- Identificar causas subyacentes de fallas
  - Nos muestran dónde son necesarios los controles
  - Nos ayudan a identificar la causa raíz

Sobre la Causa Raíz

Hay una tentación real de culpar a la gente

- Evitar culpar a la gente
- Aún si la gente fuera la causa obvia, debemos estar perdiendo controles (detectivos, preventivos, correctivos) ya que la gente tuvo permitido comportarse como lo hizo

Primer Tipo de Evaluación

Árbol de Eventos

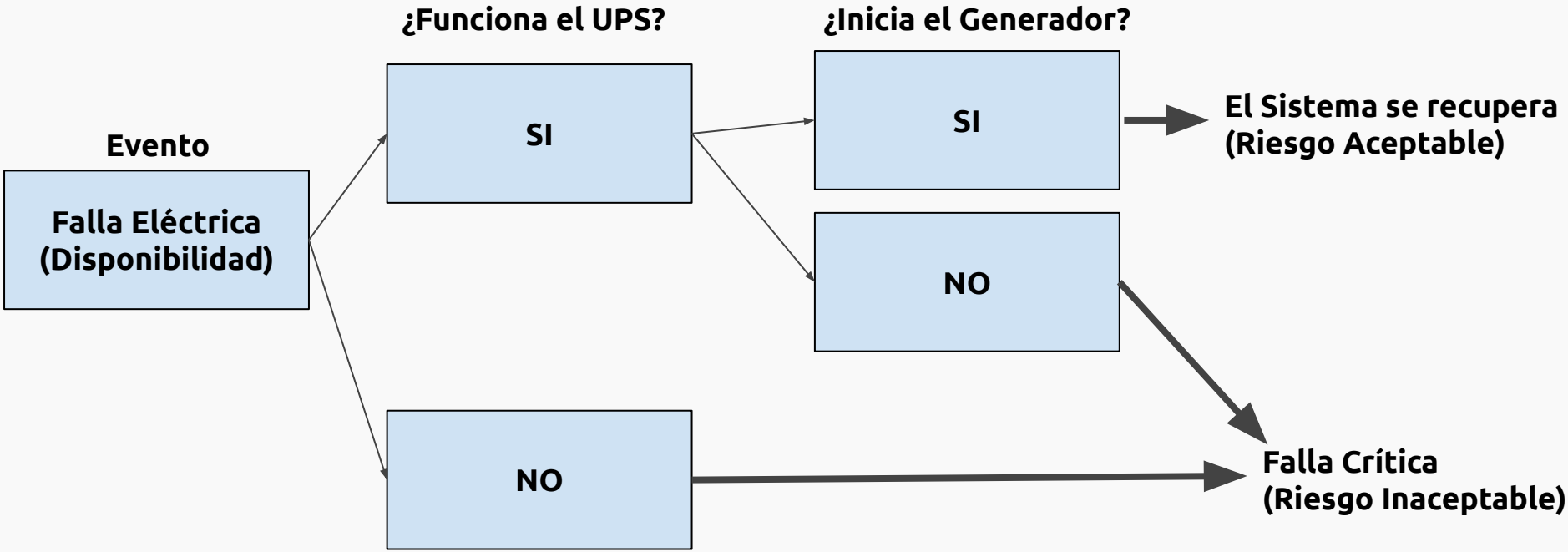
- Analizar un Sistema para identificar…
  - Controles detectivos
  - Controles reactivos
- **Objetivo**: Identificar fallas críticas

Cómo Hacerlo

Diagramar un escenario de fallas posible

- “Para los auditores ésto es fácil…”
  - ¿Si hay una excepción de auditoría, no significa eso que un control ha fallado?
  - ¿No significa ésto que tenemos una falla crítica?
- Identificar controles detectivos y correctivos rodeando al sistema
  - Deben existir más de uno
  - Encontrar todos y evaluar si detectan y reaccionan o no lo suficientemente temprano para prevenir una falla crítica

¿Qué debería mostrar un Árbol de Eventos?



Los Árboles de Eventos no son Suficientes

- Los Árboles de Eventos pueden mostrarnos donde nuestro punto de falla crítica estaba
  - Algunas veces la falla crítica real ocurrió más temprano de lo que los controles detectaron o reaccionaron
  - ¿No significaría ésto que los controles están en el lugar incorrecto en el proceso?
- Aún no nos dice por qué falló.

Árboles de Fallas

Analizan una falla específica y determinan qué hechos subyacentes deben ser verdaderos

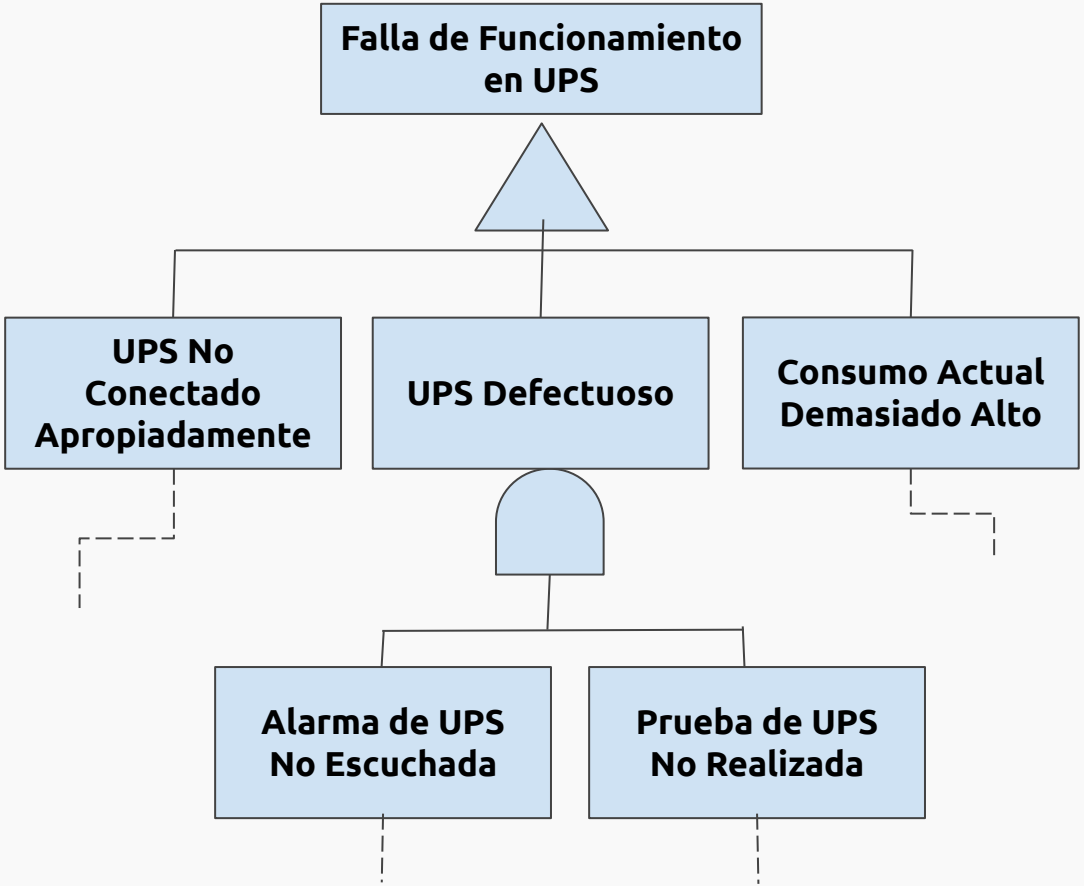
- El resultado de la evaluación serán todas las causas (razonables) de la falla.

Cómo Hacerlo

Identificar el evento crítico

- Para el evento preguntar, “Para que esto suceda, ¿qué causa subyacente debe ser verdadera?”.
- Repetir ésto para cada causa subyacente hasta encontrar algo que está fuera de su control

Ejemplo de Árbol de Fallas



Uniendo las partes

- Análisis de Causa Consecuencia (CCA)
  - Los Árboles de Eventos analizan las consecuencias de una falla, particularmente fallas críticas
  - Los Árboles de Fallas analizan las causas o fallas subyacentes, identificando idealmente la causa raíz.
- Una vez que se identifican las causas subyacentes, se pueden escribir planes de tratamiento para controlar los problemas subyacentes

¿Qué pasa con los auditores?

Estamos en una gran posición para encontrar fallas en los controles

- Mejor que escribir el mismo problema cada seis meses es recomendar una manera de repararlo
- Las remediaciones requieren evaluación de riesgos

Evaluación de Riesgo

- **Amenaza X Vulnerabilidad X Probabilidad** es lindo pero muy básico
  - No hace más que decirnos que algo es realmente arriesgado.
  - No ayuda a identificar dónde necesitamos controles
- ¡Muchos métodos de evaluación de riesgos son similares cuando se trata de controles!

¿Es necesario…

- … hacer una evaluación de riesgos para cada excepción?
  - ¡No! Elegir las fallas más críticas. Listas de “Top 10” funcionan bastante bien.
- … realmente tener nuevos controles de seguridad?
  - ¡No! Las chances son que el problema ya esté controlado a través de política o a través de un marco de referencia de alto nivel al que la organización necesita estar adherido. ¡Aplique esos controles!

El Proceso de Auditoría

Objetivos

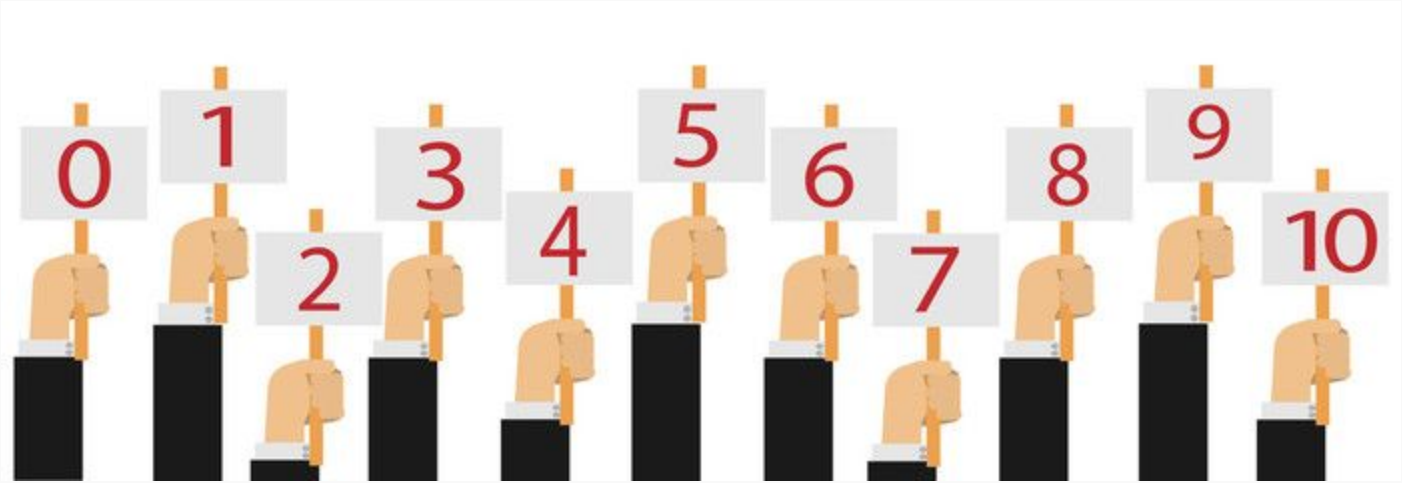
- Entender los Objetivos del Auditor
- Comprender el Proceso de Auditoría de 6 Pasos

Objetivo Principal del Auditor

- El objetivo principal del Auditor es medir y reportar sobre riesgos
  - Midiendo y reportando efectivamente sobre qué tan bien un sistema o proceso mide contra una “Mejor Práctica” o Política Corporativa
- Nuestro objetivo secundario is influir sobre los demás en reducir riesgos
  - Mediante la concientización

Objetivo Principal del Auditor

- Puede ser pensado como una especie de Jurado, pero cuando se expresa debe ser “políticamente correcto”



El Proceso de 6 Pasos

1. Planificación de la Auditoría
2. Conferencia de Entrada
3. Trabajo de Campo
4. Preparación del Reporte
5. Conferencia de Salida
6. Informe a la Gerencia

Planificación de la Auditoría

Actividades pre-auditoría

- Investigación
- Definición Inicial del Alcance
- Definición de la Estrategia de Auditoría
- Creación de la Lista de Verificación
- Formulación de los Procedimientos de Auditoría

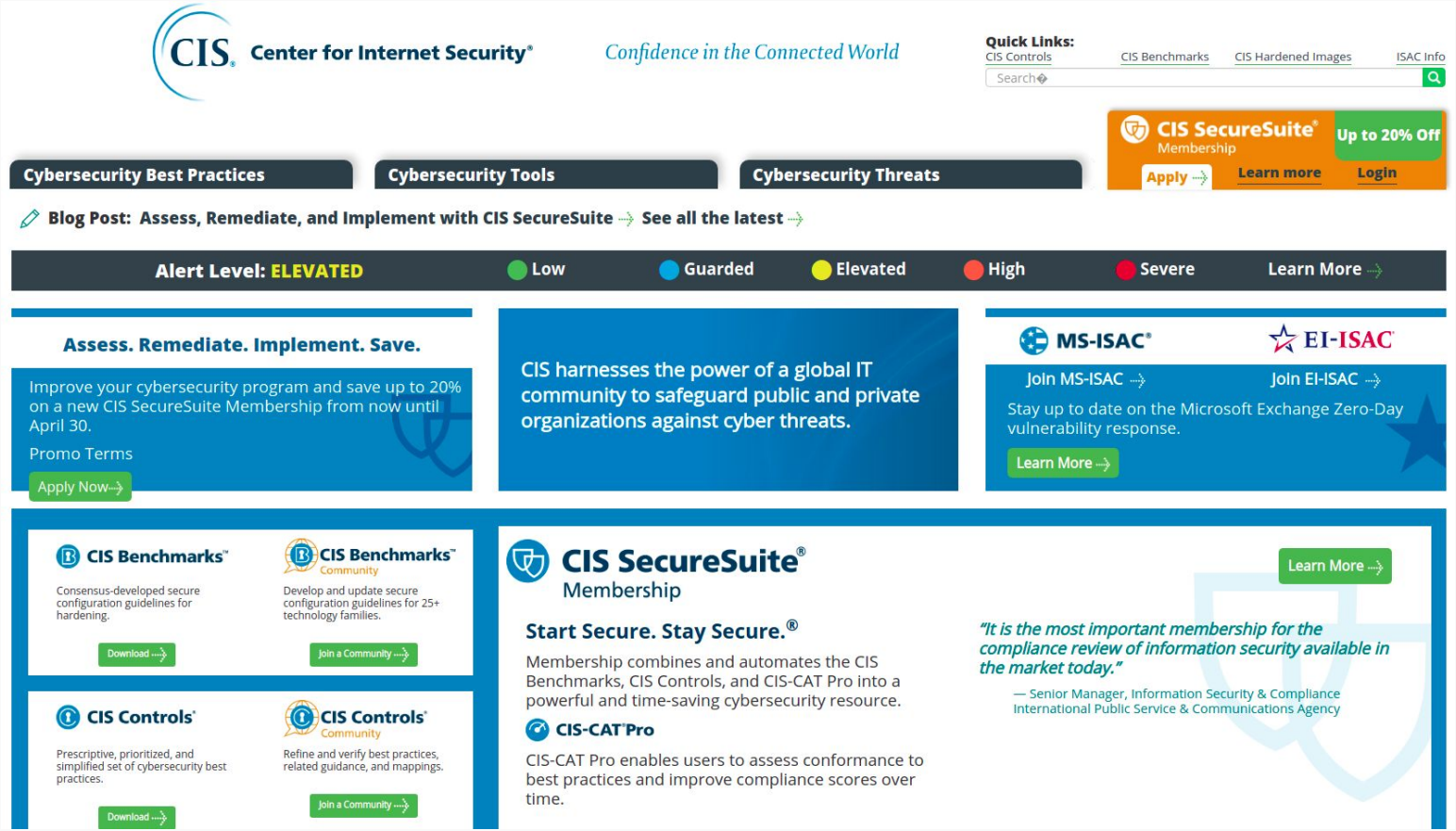
Planificación de la Auditoría (2)

- Si no construímos una buena fundación, vamos a perder la batalla en la auditoría
- Si estamos confiando en la auditoría como una parte integral de nuestra estrategia de Defensa en Profundidad, una planificación pobre de la auditoría significa que hemos perdido antes que alguien nos ataque

Planificación de la Auditoría: Investigación

- ¿Dónde investigo?
  - Política Corporativa
  - Mejores Prácticas de la Industria
  - Marcos de Referencia de Auditoría
- Una excelente referencia es el Center for Internet Security: http://www.cisecurity.org
  - Provee documentos con mejores prácticas y procedimientos paso a paso para asegurar ciertos sistemas. Estos documentos pueden ser transformados fácilmente en listas de verificación de auditoría y procedimientos

Planificación de la Auditoría: Investigación (2)



Planificación de la Auditoría: Alcance

- ¿Quién lo determina?
  - Auditor
  - La Gerencia
- El propósito cae en el Alcance

Planificación de la Auditoría: Alcance (2)

- Tratar de definir el alcance/propósito primero.
- Intentar no volver más de una vez.

Planificación de la Auditoría: Estrategia

- La Investigación respondió el “Qué”.
- La Estrategia responde el “Cómo”.

Conferencia de Entrada

- ¿Quién debería venir?
- ¿Qué debería ser cubierto?
- ¿Qué no debería hacerse?

Conferencia de Entrada (2)

¿Quién debería venir?

- Representante de la Dirección
- Administradores de Sistemas
- Usuarios de Sistemas (algunas veces)
- Representante de Seguridad de Sistemas

Conferencia de Entrada (3)

¿Qué debería ser cubierto?

- Alcance/Objetivos de la Auditoría
- El Rol del Auditor
- El Rol de los otros participantes
- El Proceso de Auditoría
- El Período de Tiempo

Conferencia de Entrada (4)

¿Qué **NO** debería hacerse/transmitirse?

- “Yo estoy a cargo aquí”.
- “Yo estoy aquí para ver qué están haciendo mal”.
- “Mi informe a la gerencia reflejará qué tan bien es su desempeño”.

Trabajo de Campo

- Con Integridad
- Profesional
- Enfocado
- Razonable

Trabajo de Campo (2)

Razonable

- Informar lo que se encuentra
- Analizar el por qué se encontró
- Explicar por qué es o no es una amenaza

Trabajo de Campo = Trabajo de Equipo

- Movilizar sus Fuerzas (Comunicación y Liderazgo)
- Confiar en las Fortalezas de Otros (Humildad)

Preparación del Reporte

- Resumen Ejecutivo
- Claro y Conciso
- Desarrollo Lógico
- Buenas Habilidades de Lenguaje son obligatorias

Resumen Ejecutivo (Lo último en ser escrito)

- Describir el Propósito
- Describir el Alcance
- Puntos importantes de los hallazgos
- Describir los Riesgos y el Impacto

Conferencia de Salida

- ¿Quién debería venir?
- ¿Qué debería ser cubierto?
- ¿Que no se debería hacer?

Conferencia de Salida (2)

¿Quién debería venir?

- Representante de la Gerencia
- Administradores de Sistemas
- Usuarios de Sistemas (a veces)
- Representante de Seguridad de Sistemas

Conferencia de Salida (3)

¿Qué debería ser cubierto?

- Alcance/Objetivos de la Auditoría
- El Rol del Auditor
- El Rol de los otros participantes
- El Proceso de Auditoría
- Los Resultados de la Auditoría

Conferencia de Salida (4)

- ¿Qué **NO** debería hacerse/transmitirse?
  - “Aquí está lo que ustedes están haciendo mal”
  - “Muchos administradores saben mejor que nadie que… “
  - Inquietudes de los Administradores hacia la Gerencia

Reporte a la Gerencia

- Claro y Conciso
- Resumen Ejecutivo
- Presentación Digital

Reporte a la Gerencia: Cómo Hacerlo

- Preparar un Presentación de 60 minutos
- Agendar una reunión de 2 horas
- Llamado a la reunión por el Ejecutivo de más alto nivel

Reporte a la Gerencia: Cómo Hacerlo (2)

- El Ejecutivo inicia la reunión
- Presentar por 30 - 45 minutos
- Descanso

Reporte a la Gerencia: Cómo Hacerlo (3)

- Finalizar la Presentación
- Convocatoria de Análisis/Preguntas
- Cierre

Síntesis

- Proceso Esencial de 6 Pasos
- Usar los 6 Pasos cuando sea posible
  1. Planificación de la Auditoría
  2. Conferencia de Entrada
  3. Trabajo de Campo
  4. Preparación del Reporte
  5. Conferencia de Salida
  6. Reporte a la Gerencia

¿Preguntas?

¡Muchas Gracias!