Infraestructura Computacional

Análisis de Riesgos y Endurecimiento de Máquinas

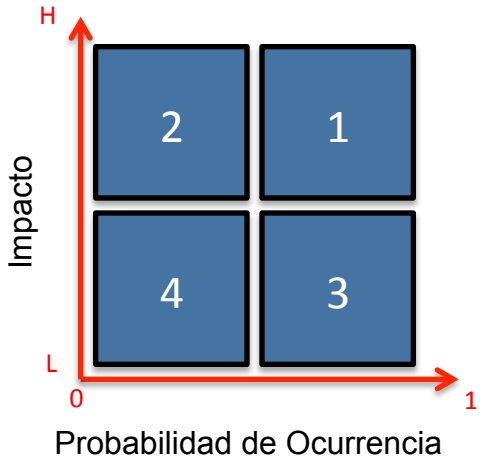
Francisco Rueda

Sandra Rueda

Análisis de Riesgos

- ¿Cómo organizar la búsqueda y eliminación de los problemas de seguridad?

Análisis de Riesgos



Análisis de Riesgos

- La administración de riesgos es el proceso de identificar los riesgos y tomar medidas para eliminarlos o reducirlos a un nivel aceptable

Análisis de Riesgos

- Vulnerabilidad
  - Imperfección o debilidad en los procedimientos de seguridad de un sistema, en su diseño, su implementación o en los controles internos
- Riesgo
  - Impacto negativo de la explotación de una vulnerabilidad
- Amenaza
  - Posibilidad de que una vulnerabilidad sea explotada

Análisis de Riesgos

- Fuentes de amenazas
  - Naturales
    - inundaciones, terremotos, avalanchas, tormentas
  - Ambientales
    - corte de luz, polución, derrames de químicos
  - Humanas
    - errores o acciones deliberadas

Amenazas

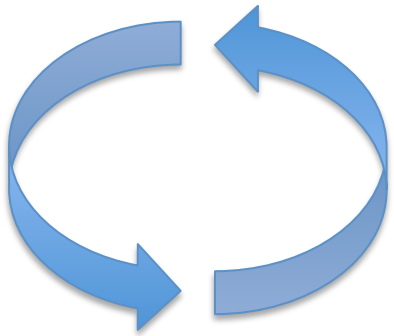
- Humanas
  - Acceso no autorizado al sistema
  - Spoofing (suplantación)
  - Modificación no autorizada de datos
  - Fraude
  - Robo de información
  - Instalación de software malicioso
  - Acceso no autorizado a datos
  - Espionaje en los medios de transmisión

Vulnerabilidades

- Buffer overflow
- Error de configuración
- Esquema de manejo que permite claves débiles
- Almacenar información confidencial sin cifrar
- Errores de implementación

Administración de Riesgos

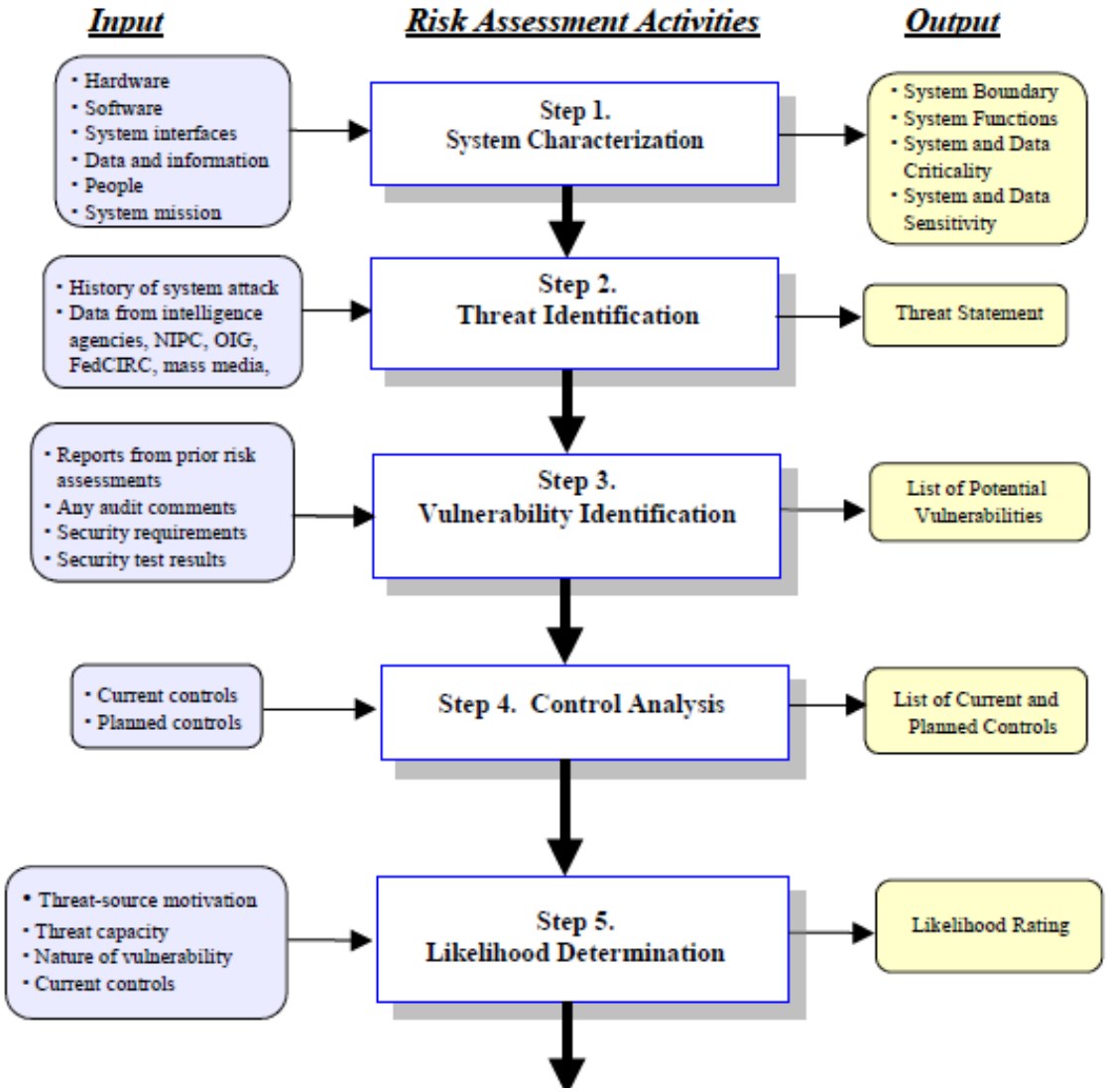
- Identificación
- Valoración
- Mitigación
- Evaluación permanente



Identificación y Valoración del Riesgo

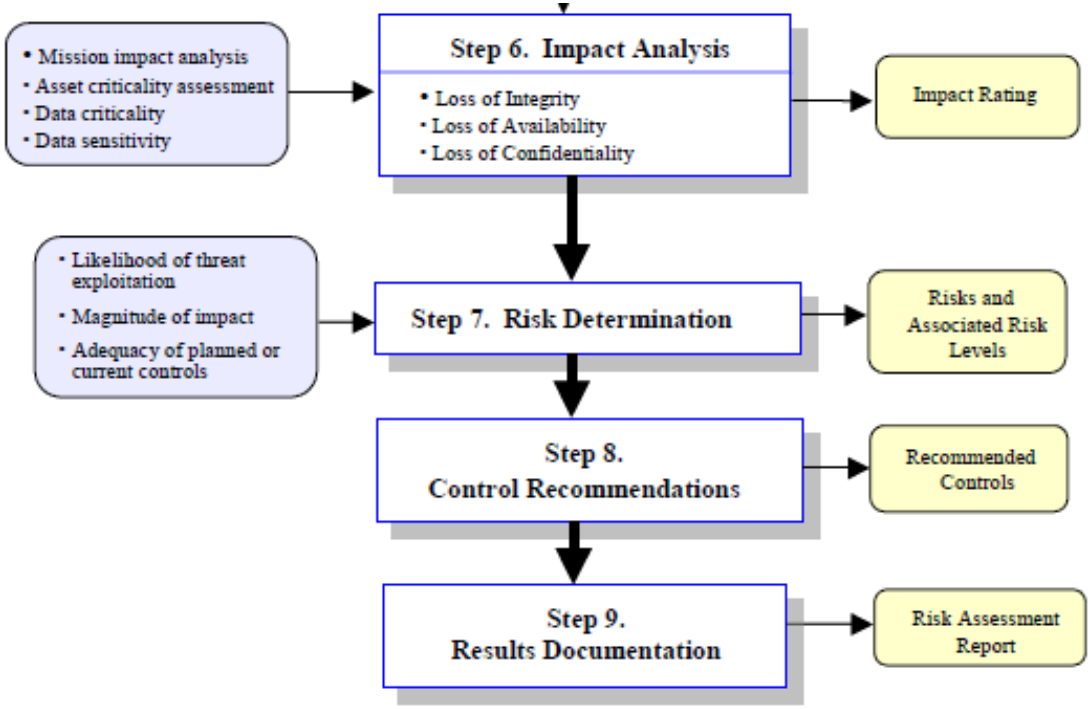
- Caracterización del sistema
- Identificación de amenazas
- Identificación de vulnerabilidades
- Análisis de control
- Determinación de probabilidades
- Análisis de impacto
- Determinación de riesgo
- Recomendaciones de control
- Documentación de resultados

Identificación y Valoración del Riesgo



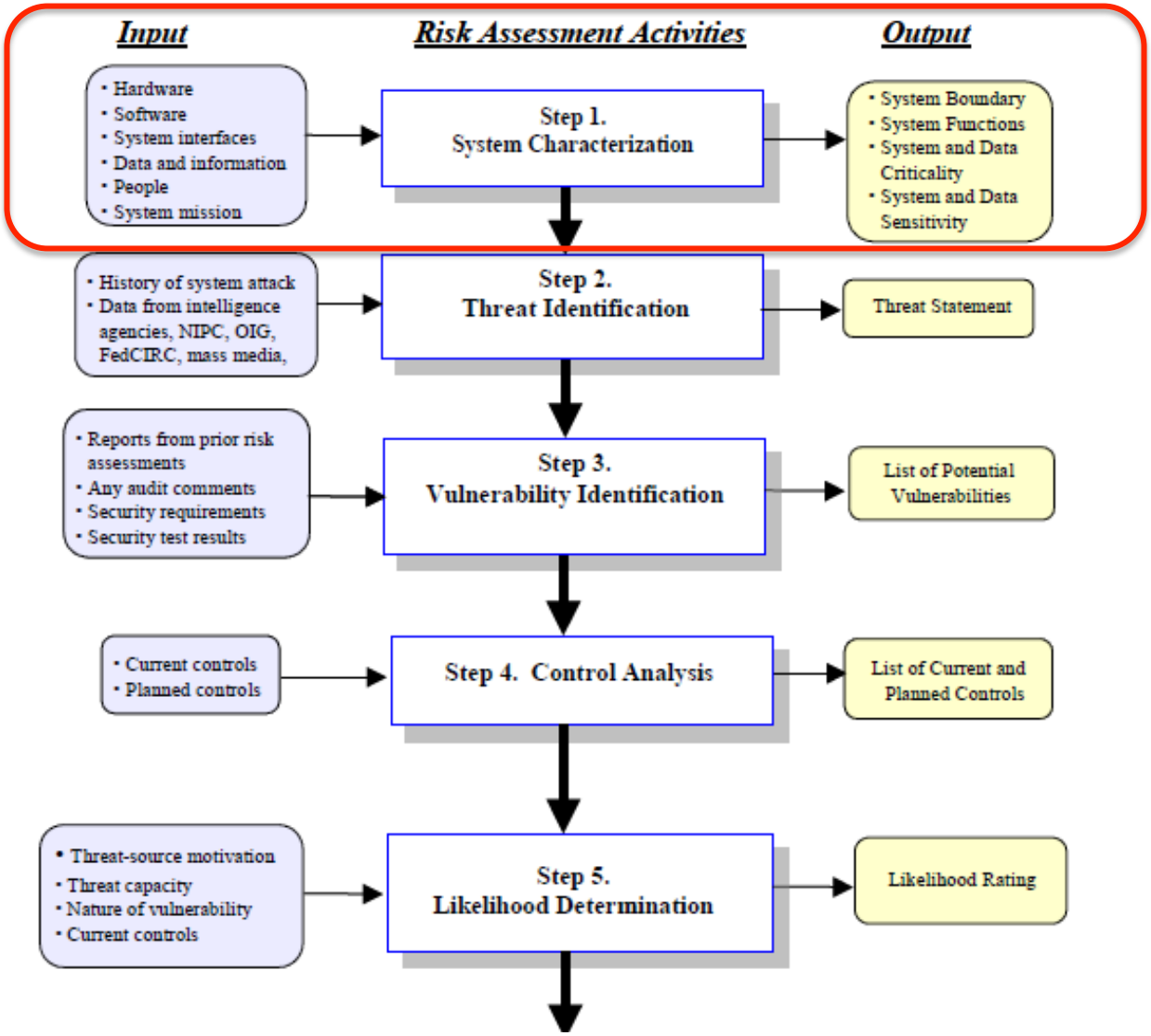
Tomado de [Nist2002]

Identificación y Valoración del Riesgo



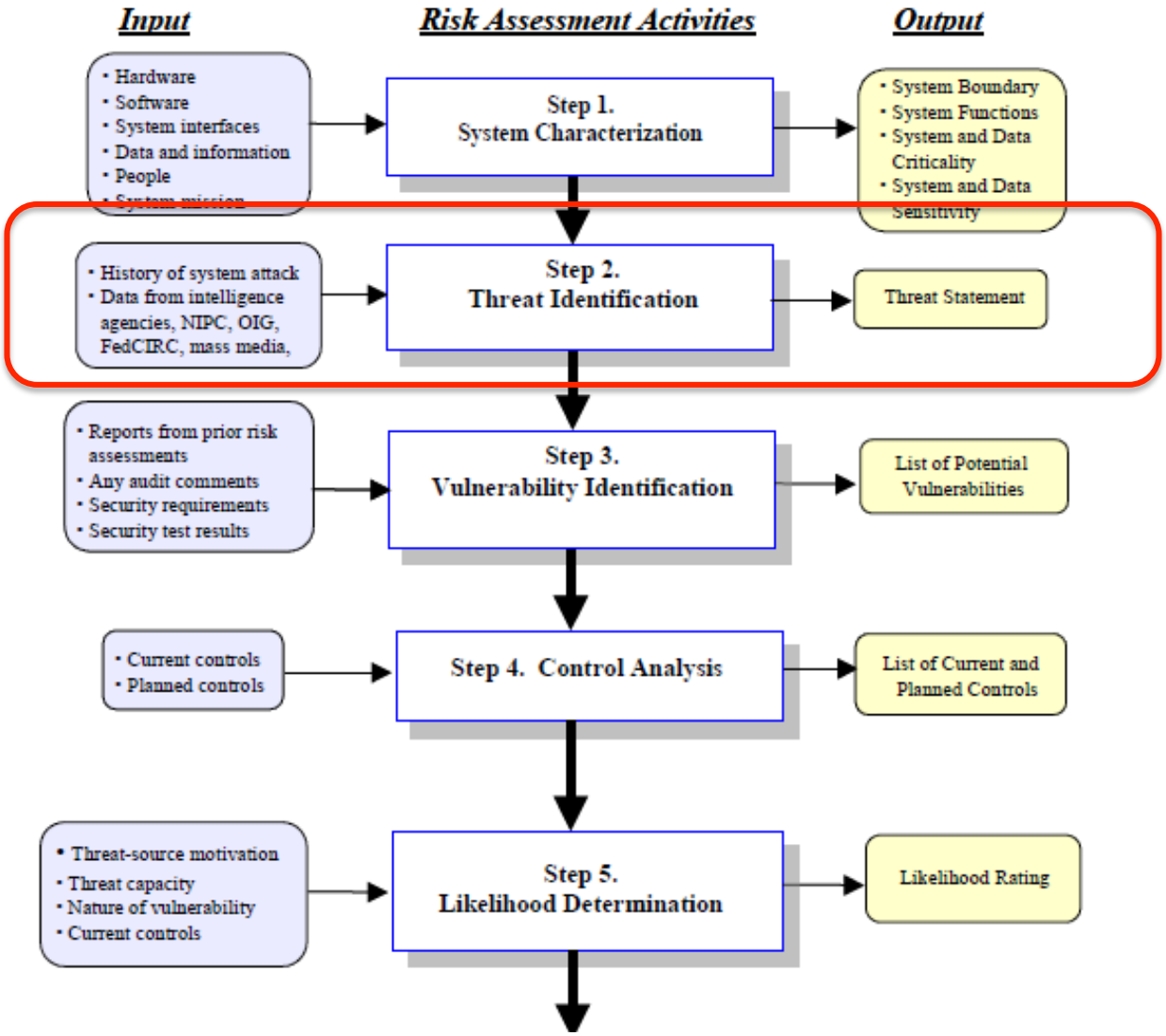
Tomado de [Nist2002]

Identificación y Valoración del Riesgo



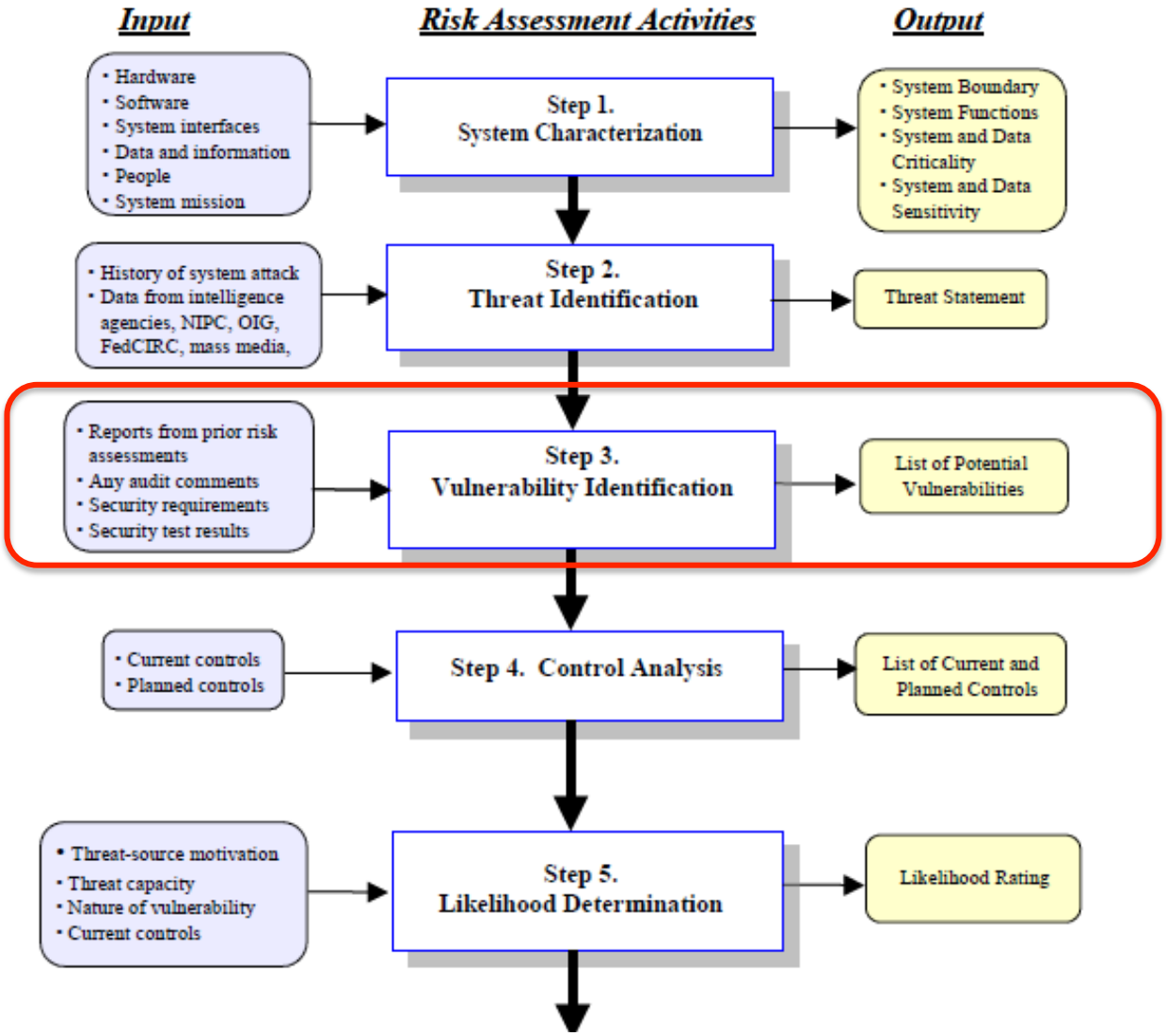
Tomado de [Nist2002]

Identificación y Valoración del Riesgo



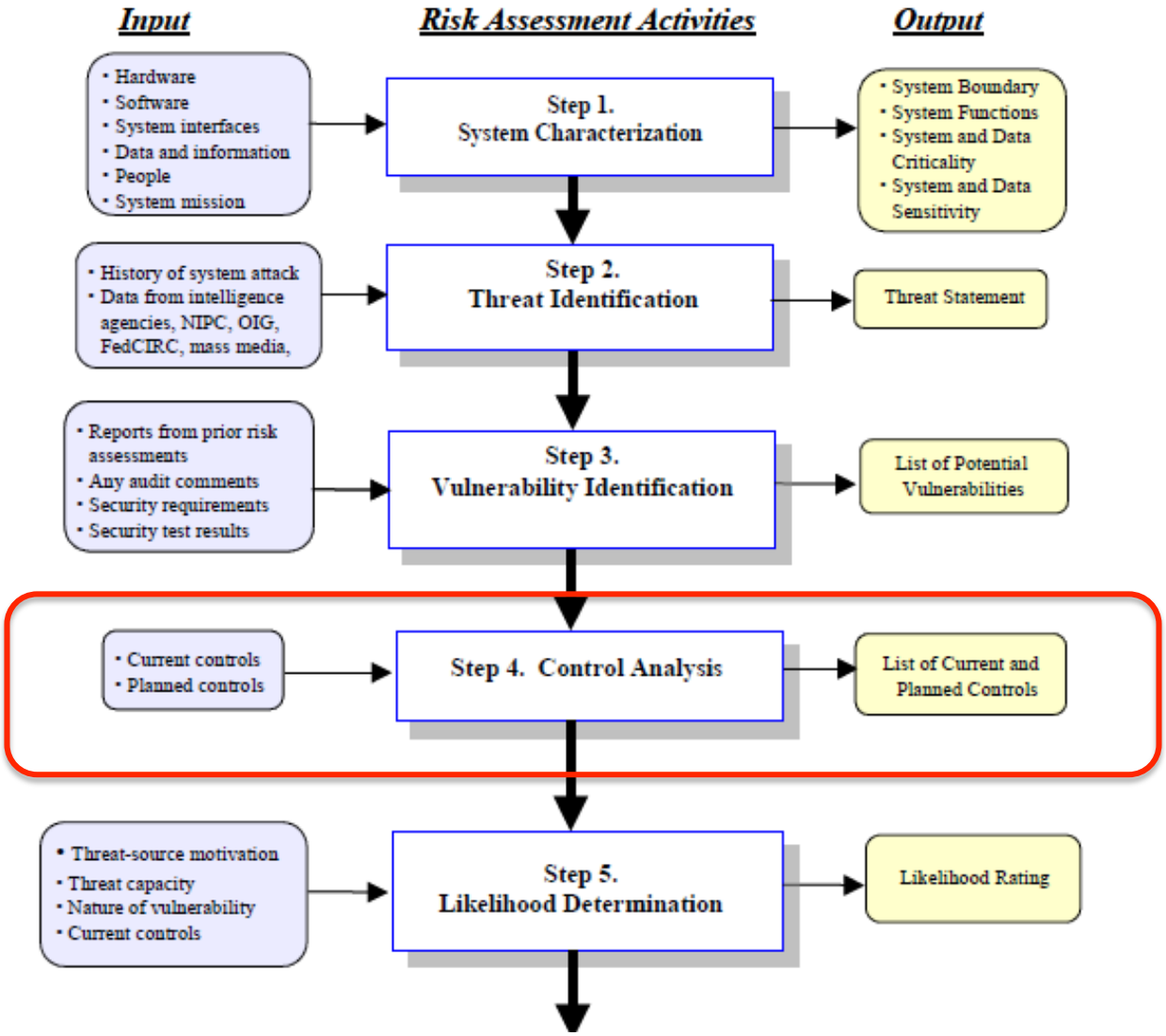
Tomado de [Nist2002]

Identificación y Valoración del Riesgo



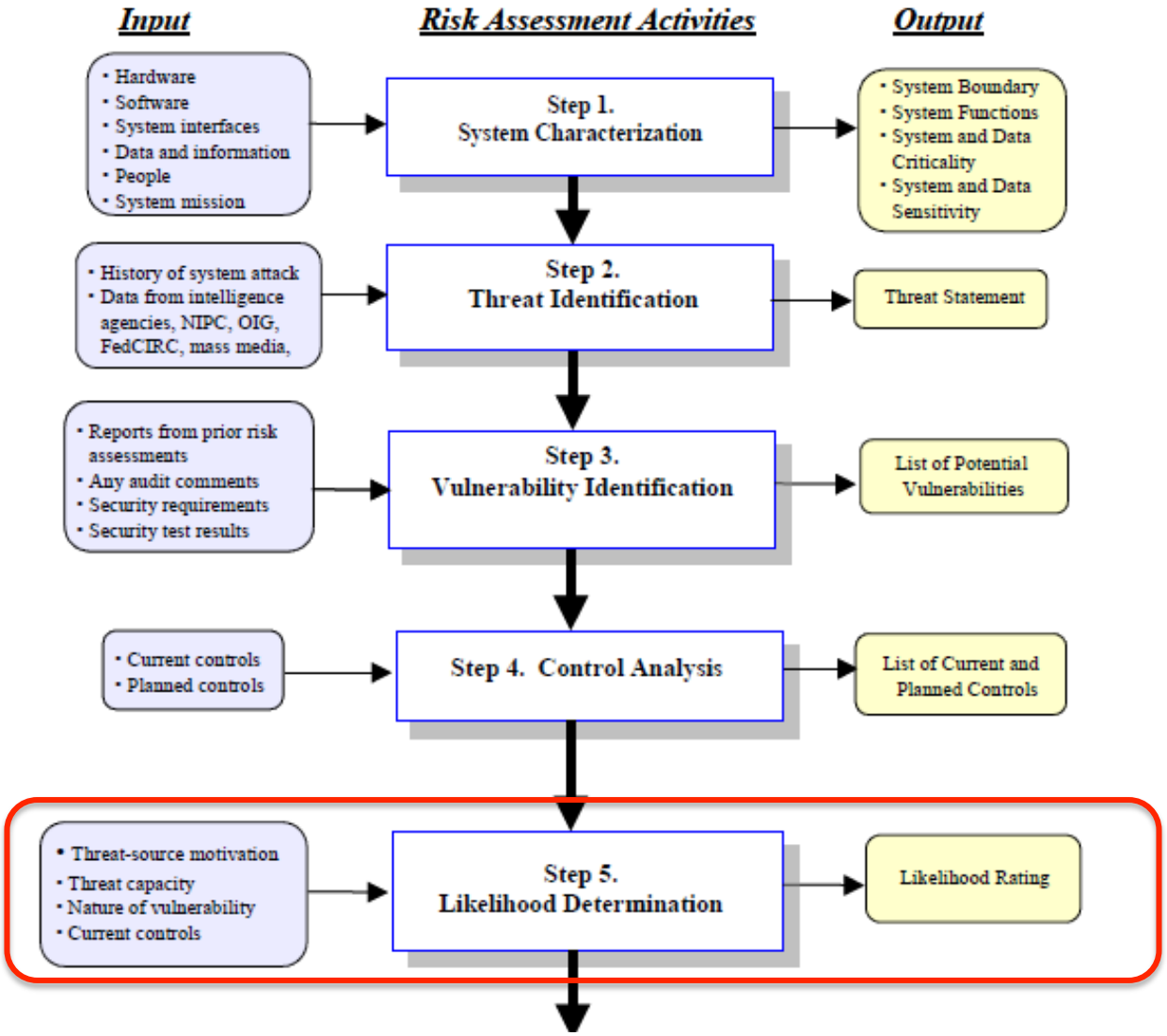
Tomado de [Nist2002]

Identificación y Valoración del Riesgo



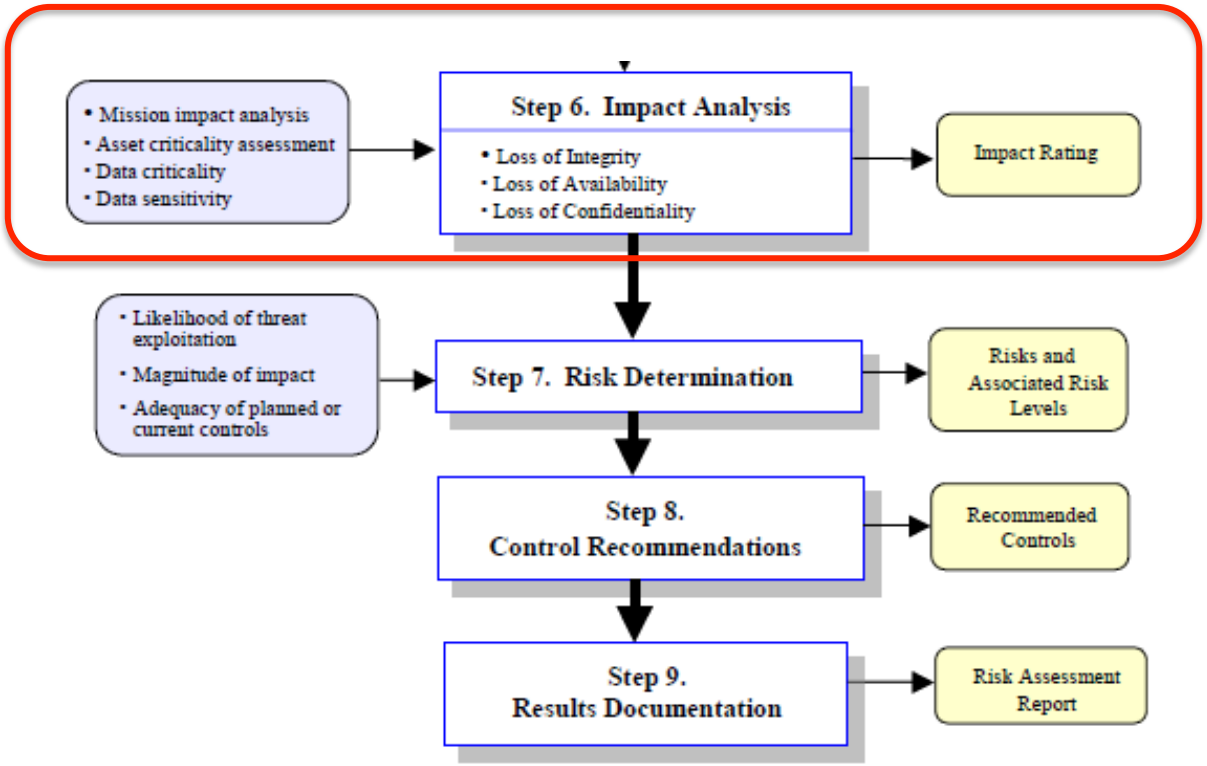
Tomado de [Nist2002]

Identificación y Valoración del Riesgo



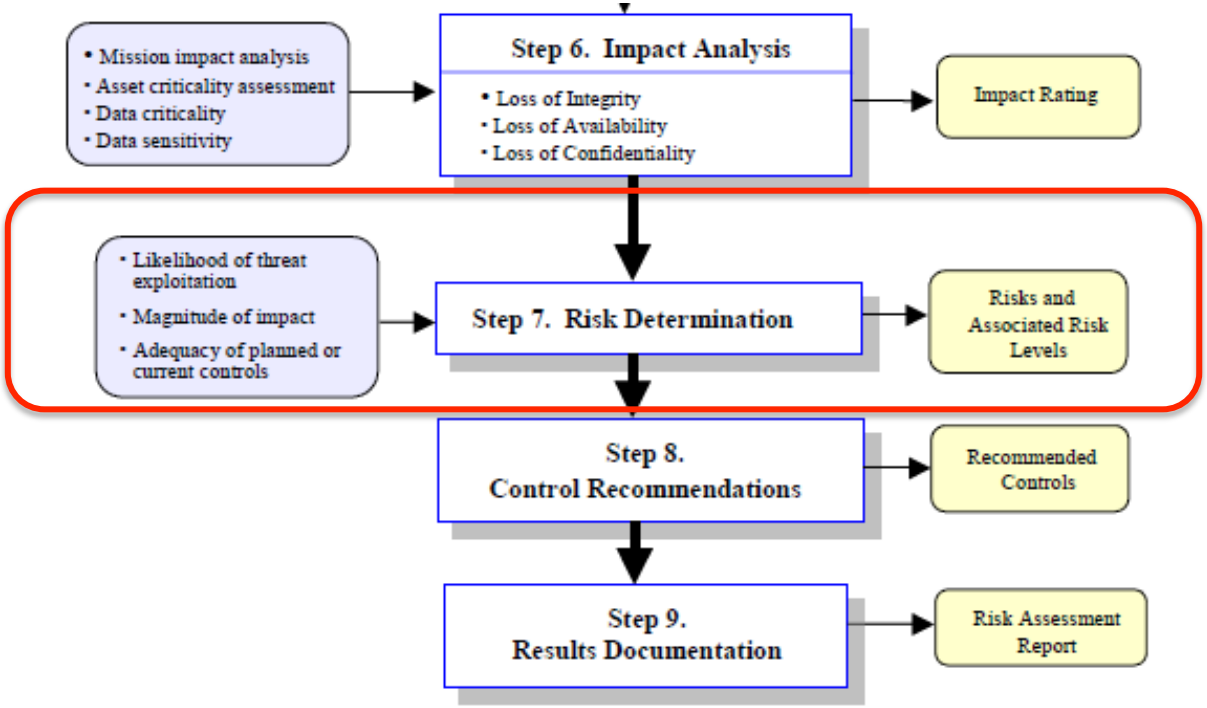
Tomado de [Nist2002]

Identificación y Valoración del Riesgo



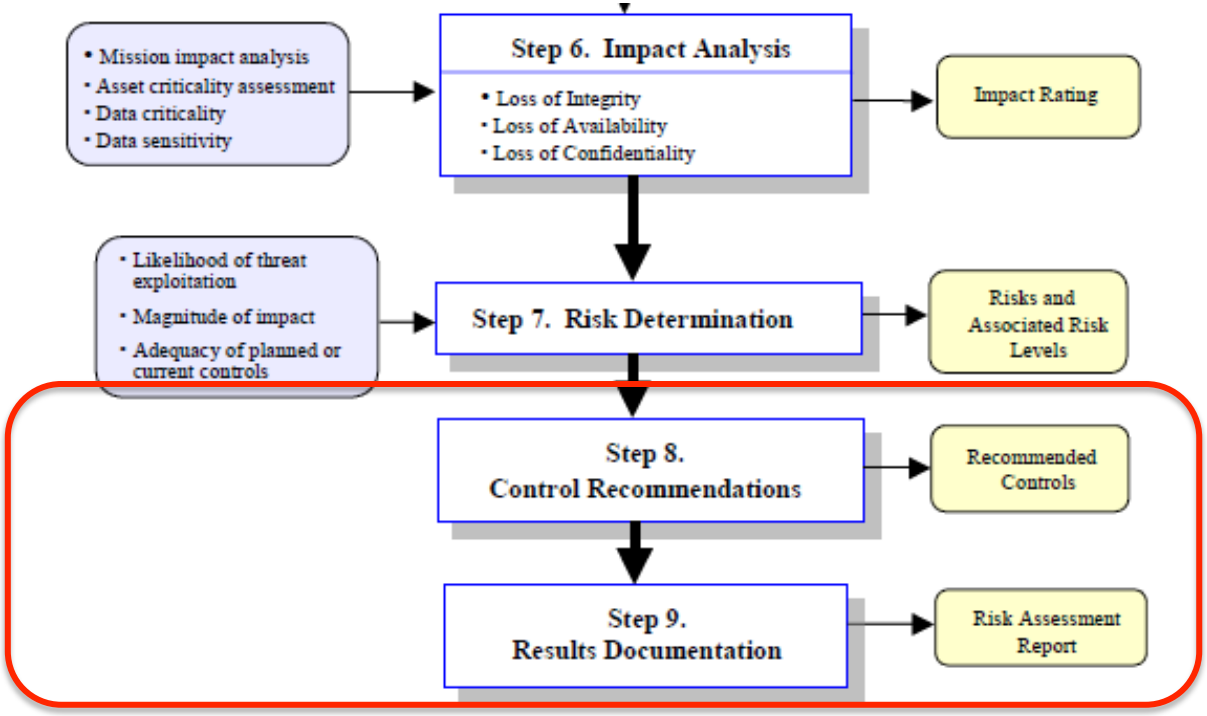
Tomado de [Nist2002]

Identificación y Valoración del Riesgo



Tomado de [Nist2002]

Identificación y Valoración del Riesgo



Tomado de [Nist2002]

Problemática

- Los recursos de una empresa pueden ser atacados
  - Acceso indebido
  - Problemas de configuración
  - Denegación de servicio

Principios de Diseño

- *El diseño y la construcción de técnicas que excluyan sistemáticamente todos los errores son temas constantes de investigación, pero hasta la fecha no existe un método completo y realizable para la construcción de sistemas grandes de propósito general.*

Principios de Diseño

- Simplicidad
- Valores seguros por defecto
- Mediación completa
- Diseño abierto
- Separación de privilegios
- Privilegios mínimos

Principios de Diseño

- Aceptación sicológica
- Tener presente el costo de romper la seguridad
- Mantener registros de las tareas realizadas en el sistema

Endurecimiento

- Principios generales para el endurecimiento de máquinas
  - Minimizar
  - Actualizar
  - Mantener múltiples niveles de defensa
  - Aislar
  - Configurar
  - Monitorear

Minimizar

- Servicios
- Cuentas de administradores
- Cuentas de usuario
- Permisos de ejecución de aplicaciones

Actualizar

- Sistema operacional
- Parches
- Aplicaciones

Mantener Niveles de Defensa

- Firewall
- IDS
  - host
  - red
- Antivirus
- Antispam

Defensa in depth

Aislar

- Servicios
- Unidades organizacionales
- Intranet e Internet

Configurar

- Sistemas operativos y servicios
  - Cambiar opciones por defecto
  - Autenticación y control de acceso
    - Cuentas por usuario (eliminar cuentas compartidas)
    - Eliminar cuentas anónimas
    - Privilegios mínimos

Monitorear

- Actividades ejecutadas
  - Administradores
  - Usuarios regulares
  - Programas
- Tráfico de red
- Mantener logs

Asignar Responsabilidad

- Políticas y mecanismos para registro de actividades y asignación de responsabilidades

Evaluar

- Pruebas de penetración
  - Password cracker
  - Port scanner
  - Problemas típicos de implementación

Endurecimiento

- Seguridad física
- Redundancia de servicios críticos
- Políticas de respaldo
- Políticas de recuperación y continuidad

Referencias

- Advanced information security for technical staff. CERT, 2003-2008
- Guide to General Server Security. NIST, 2008
- Guidelines on Securing Public Web Servers. NIST, 2007
- Preparing to Detect Signs of Intrusion. CMU/SEI-SIM-005, 1998.