technologyINT
Ciberseguridad & Computo Forense

Curso de Preparación para el CISSP

Dominio 1 – Seguridad y Gestión de Riesgo

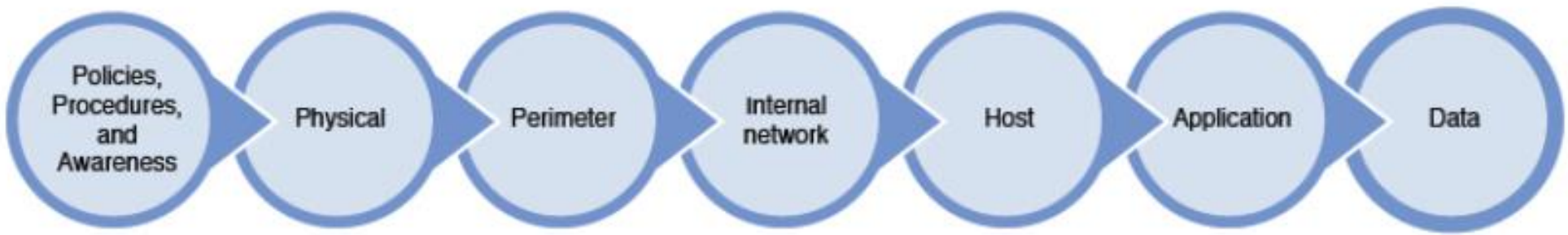
Seo Rodríguez, MBA
CISSP, CRISC, CISM, CISA, Security+, MCSE, MCT, VCP, ITIL, Cisco CCNA, Network+ & A+

Términos Básicos de Seguridad

Términos de seguridad

- CIA
  - Confidencialidad
  - Integridad
  - Disponibilidad
- Auditoría y Cotabilidad
- No repudio
- Postura de seguridad predeterminada
- Defensa en profundidad

La figura 1-1 muestra un ejemplo del concepto de defensa en profundidad.



Otros Terminos de Seguridad

- Abstración
- Ocultacion de datos
- Cifrado

Principios de gobernanza de seguridad

Principios de gobernanza de la seguridad

- Determinar y articular el estado de seguridad deseado de la organización.
- Proporcionar la dirección estratégica, los recursos, la financiación y el apoyo para garantizar que se pueda lograr y mantener el estado de seguridad deseado.
- Mantener la responsabilidad y la rendición de cuentas a través de la supervisión.

Principios de Gobernanza de Seguridad

- Alineación de funciones de seguridad
- Estrategias y metas organizacionales
- Misión y objetivos organizacionales
- Caso de negocio
- Presupuesto de seguridad, métricas y efectividad
- Recursos
- Procesos organizacionales
- Adquisiciones y desinversiones
- Comités de gobierno
- Funciones y responsabilidades organizativas
- Junta Directiva
- Gestión
- Comité de Auditoría
- Propietario de los datos
- Custodio de datos

Principios de Gobernanza de Seguridad

Propietario del Sistema	Administrador de sistema	Administrador de seguridad	Analista de seguridad
Propietario de la aplicación	Supervisor	**Usuario**	**Auditor**

Marcos de control de Seguridad

- ISO/IEC 27000 Series
- Zachman Framework
- TOGAF
- DoDAF
- MODAF
- SABSA
- COBIT
- NIST 800 Series
- HITRUST CSF
- CIS Critical Security Controls
- COSO
- OCTAVE
- ITIL
- Six Sigma
- CMMI
- CRAMM
- Top-down versus bottom-up approach
- Security program life cycle

Objetivos de control para tecnologías de la información y afines (COBIT)

COBIT 5 es un marco de desarrollo de controles de seguridad que documenta cinco principios:

- Satisfacer las necesidades de las partes interesadas
- Cubriendo la empresa de un extremo a otro
- Aplicar un único marco integrado
- Permitiendo un enfoque holístico
- Separar la gobernanza de la gestión

Estos cinco principios impulsan los objetivos de control categorizados en siete habilitadores:

- Principios, políticas y marcos
- Procesos
- Estructuras organizacionales
- Cultura, ética y comportamiento
- Información
- Servicios, infraestructura y aplicaciones
- Personas, habilidades y competencias

Publicación especial (SP) del Instituto Nacional de Estándares y Tecnología (NIST) Serie 800

- **SP 800-12 Rev. 1:** Presenta los principios de seguridad de la información.
- **SP 800-16 Rev. 1:** Describe la capacitación basada en **funciones de** tecnología de la información / ciberseguridad para departamentos, agencias y organizaciones federales.
- **SP 800-18 Rev. 1:** Proporciona pautas para desarrollar planes de seguridad para sistemas de información federales.
- **SP 800-30 Rev. 1:** Proporciona orientación para realizar evaluaciones de riesgo de organizaciones y sistemas de información federales, ampliando la orientación en SP 800-39.
- **SP 800-34 Rev. 1:** Proporciona pautas sobre el propósito, proceso y formato del desarrollo de planes de contingencia del sistema de información.

- **SP 800-53 Rev. 4:** Proporciona un catálogo de controles de seguridad y privacidad para los sistemas de información federales y un proceso para seleccionar controles (Rev. 5 pendiente).
- **SP 800-53A Rev. 4:** Proporciona un conjunto de procedimientos para realizar evaluaciones de controles de seguridad y controles de privacidad empleados dentro de los sistemas de información federales.
- **SP 800-55 Rev. 1:** Proporciona orientación sobre cómo utilizar métricas para determinar la idoneidad de los controles, políticas y procedimientos de seguridad en el lugar.
- **SP 800-60 Vol. 1 Rev. 1:** Proporciona pautas para mapear tipos de información y sistemas de información a categorías de seguridad.
- **SP 800-61 Rev. 2:** proporciona pautas para el manejo de incidentes.

Controles de seguridad críticos de CIS

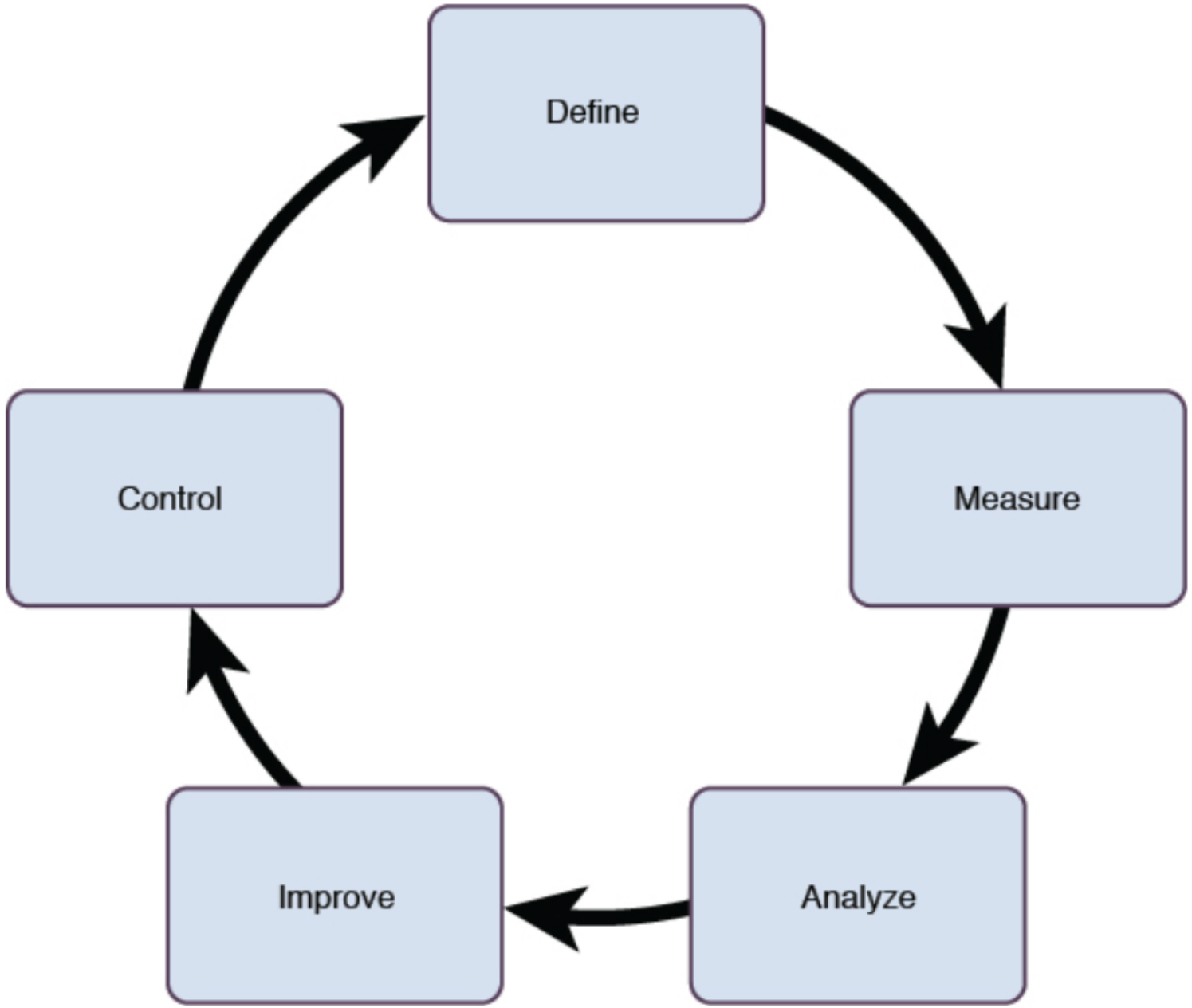
1. Inventario y control de activos de hardware
2. Inventario y control de activos de software
3. Gestión continua de vulnerabilidades
4. Uso controlado de privilegios administrativos
5. Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores
6. Mantenimiento, seguimiento y análisis de registros de auditoría
7. Protecciones de correo electrónico y navegador web
8. Defensas de malware
9. Limitación y control de puertos, protocolos y servicios de red
10. Capacidades de recuperación de datos

11. Configuraciones seguras para dispositivos de red, como firewalls, enrutadores y conmutadores
12. Defensa de límites
13. Protección de Datos
14. Acceso controlado basado en la necesidad de saber
15. Control de acceso inalámbrico
16. Seguimiento y control de cuentas
17. Implementar un programa de capacitación en concientización sobre seguridad.
18. Seguridad del software de aplicación
19. Respuesta y gestión de incidentes
20. Pruebas de penetración y ejercicios del equipo rojo

Tabla 1-2 Procesos y publicaciones principales de ITIL v3

Estrategia de servicio ITIL	Diseño de servicios ITIL	Transición del servicio ITIL	Operación del servicio ITIL	Mejora continua del servicio de ITIL

Las figuras 1-3 y 1-4 muestran ambas metodologías Six Sigma.



Integración del modelo de madurez de capacidad (CMMI)

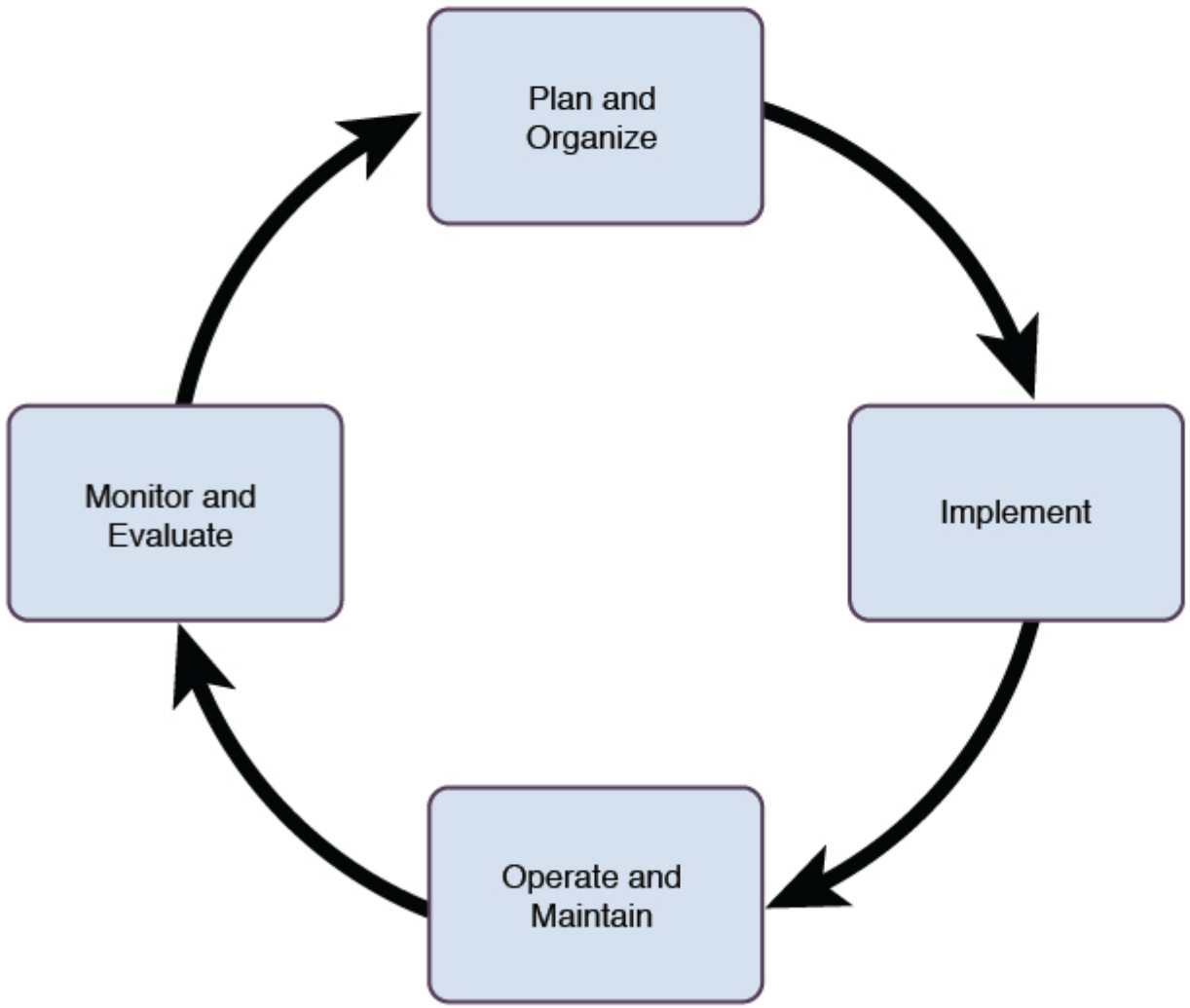
Enfoque de arriba hacia abajo versus de abajo hacia arriba

Ciclo de vida del programa de seguridad

- Planificar y organizer
- Implementar
- Operar y manatener
- Supervisar y evaluar

La Figura 1-5 muestra un diagrama del ciclo de vida del programa de seguridad.

Key Topic



El debido cuidado y la debida diligencia son dos términos relacionados que las organizaciones deben entender, ya que se relacionan con la seguridad de la organización y sus activos y datos.

Due Care **Debido Cuidado**	**estándar de cuidado que una persona prudente habría ejercido en las mismas condiciones o en similares. En el contexto de la seguridad, el debido cuidado significa que una organización toma medidas razonables para proteger sus activos de información, sistemas e infraestructura de soporte.**
Due Diligence **Debida Diligencia**	La debida diligencia es el acto de investigación y evaluación Las organizaciones deben instituir los procedimientos adecuados para determinar cualquier riesgo para los activos de la organización.

Cumplimiento

Cumplimiento

Cumplimiento contractual, legal, de estándares industriales y regulatorio

Cumplimiento de requisitos de privacidad

Asuntos legales y regulatorios

Conceptos de Delitos Informáticos

Crimen asistido por computadora

Crimen dirigido por computadora

Delito informático incidental

Delito de prevalencia informática

Hackers versus crackers

Principales Sistemas Legales

Key Topic

Estos sistemas incluyen lo siguiente:

- Ley del código civil
- Ley común
- Derecho penal
- Derecho civil / extracontractual
- Derecho administrativo / regulatorio
- Derecho consuetudinario
- Ley religiosa
- Ley mixta

Licencias y propiedad intelectual

La propiedad intelectual amparada por este tipo de ley incluye lo siguiente:

- Patentar
- Secreto comercial
- Marca comercial
- Derechos de autor
- Problemas de licencias y piratería de software
- Gestión de derechos digitales (DRM)

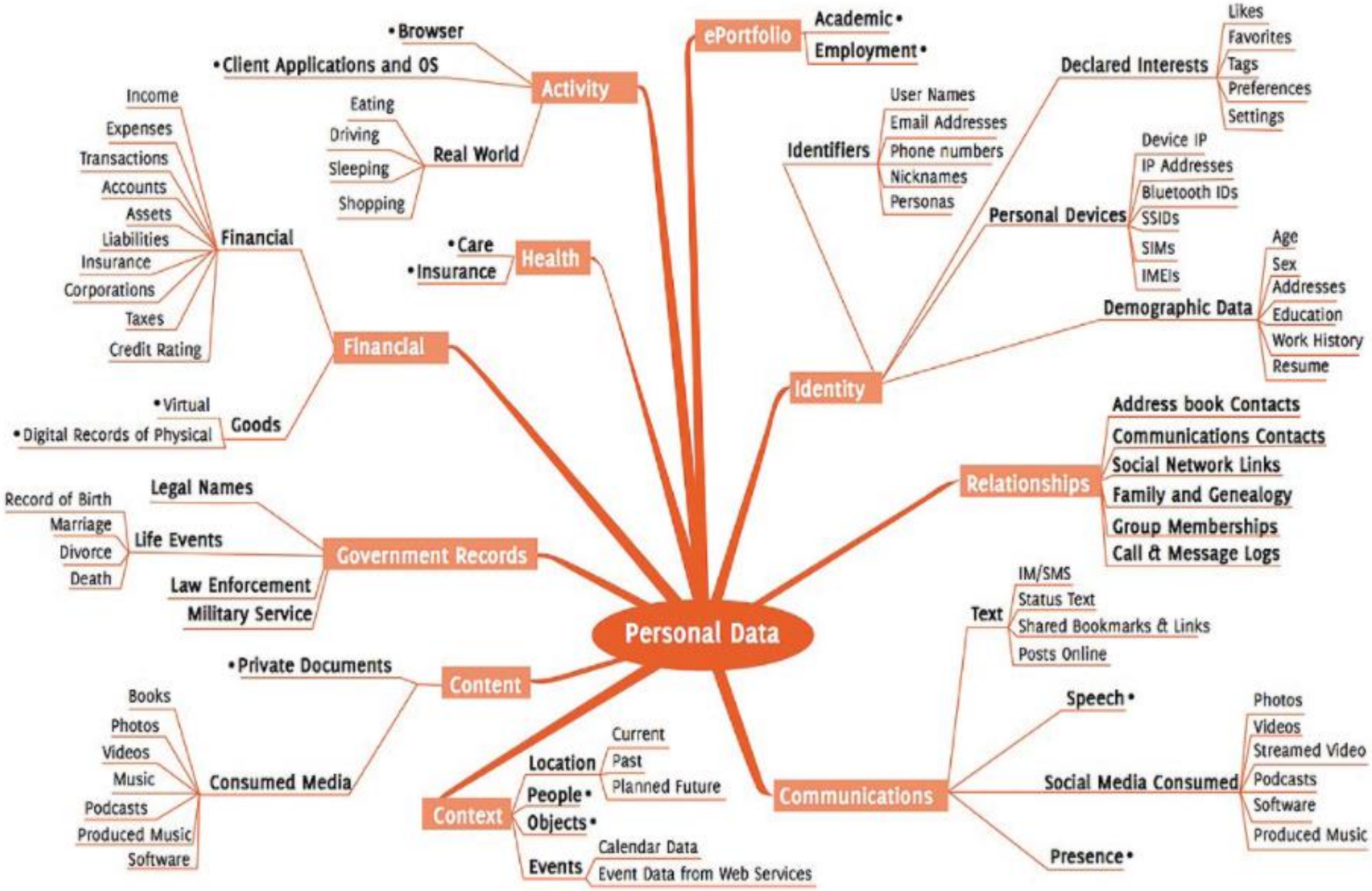
Problemas de licencias y piratería de software

- **Freeware:** Software disponible de forma gratuita, incluidos todos los derechos para copiar, distribuir y modificar el software.
- **Shareware:** software que se comparte durante un tiempo limitado. Después de una cierta cantidad de tiempo (el período de prueba), el software requiere que el usuario compre el software para acceder a todas las funciones del software. Esto también se conoce como software de prueba.
- **Software comercial:** software con licencia de una entidad comercial para su compra en un mercado mayorista o minorista.

Otros Conceptos Legales y Regulatorios

- Protección interna
- Gestión de derechos digitales (DRM)
- Delitos cibernéticos y violaciones de datos
- Controles de importación / exportación
- Flujo de datos transfronterizo
- Privacidad
- Información de identificación personal (PII)

En la Figura 1-10 se muestra una lista compleja de PII .



Leyes y Regulaciones

- Ley Sarbanes-Oxley (SOX)
- Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA)
- Ley Gramm-Leach-Bliley (GLBA) de 1999
- Ley de abuso y fraude informático (CFAA) de 1986
- Ley Federal de Privacidad de 1974
- Ley Federal de Vigilancia de Inteligencia (FISA) de 1978
- Ley de privacidad de comunicaciones electrónicas (ECPA) de 1986
- Ley de seguridad informática de 1987
- Directrices Federales de Sentencia de los Estados Unidos de 1991
- Ley Federal de Gestión de la Seguridad de la Información (FISMA) de 2002
- Ley USA PATRIOT de 2001

Etica Profesional

(ISC) 2 Código de Ética

Los cuatro cánones obligatorios del Código de Ética son los siguientes:

- Proteger la sociedad, el bien común, la necesaria confianza pública y la infraestructura.
- Actuar de manera honorable, honesta, justa, responsable y legal.
- Brindar un servicio diligente y competente a los directores.
- Avanzar y proteger la profesión.

Instituto de Ética Informática

- No use una computadora para hacer daño.
- No interfiera con el trabajo informático de otras personas.
- No fisgonee en los archivos informáticos de otras personas.
- No uses una computadora para robar.
- No use una computadora para mentir.
- No instale ni utilice software con licencia a menos que lo haya pagado.
- No use la computadora de otra persona a menos que tenga permiso o haya pagado la compensación apropiada por dicho uso.
- No se apropie de la producción intelectual de otra persona.
- Considere las consecuencias del programa que está escribiendo o del sistema que está diseñando.
- Utilice siempre una computadora de manera que garantice la consideración y el respeto de otras personas y su propiedad.

Junta de Arquitectura de Internet

Código de ética organizacional

Documentación de Seguridad

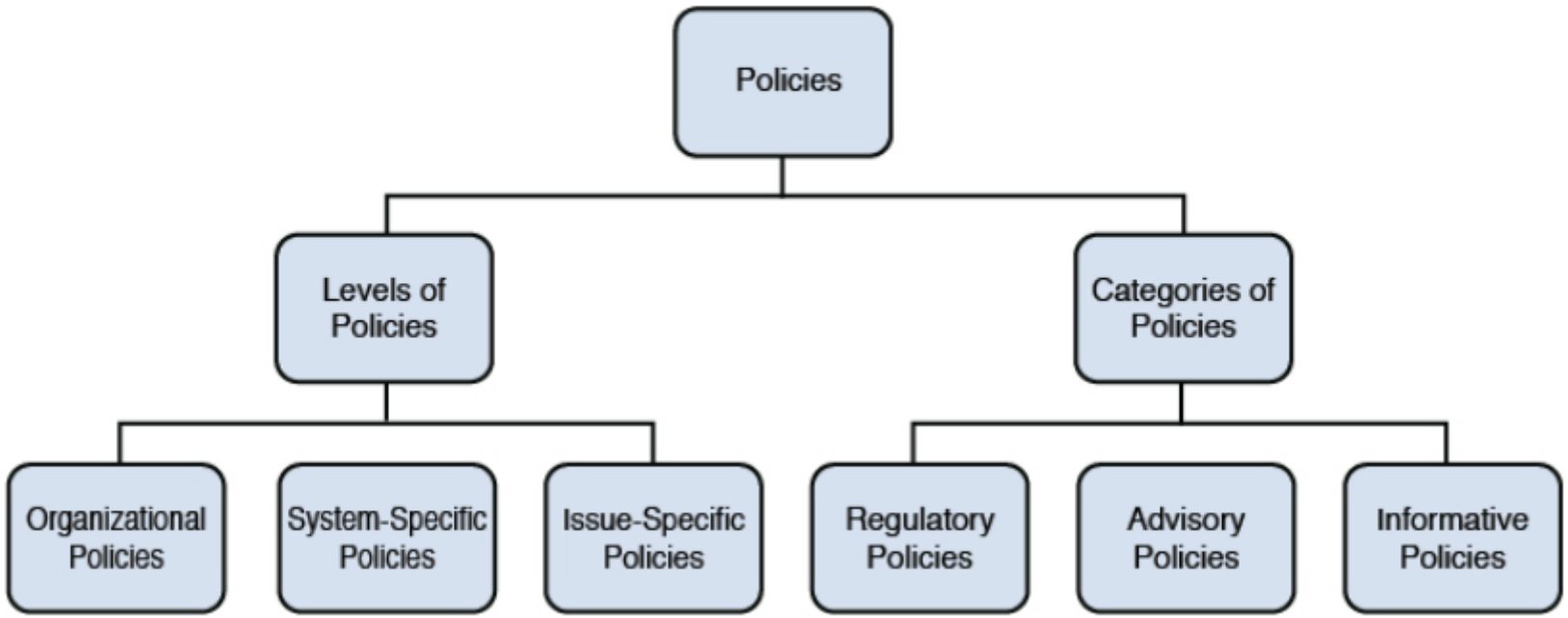
Documentación de seguridad

- Defina el alcance del programa de seguridad.
- Identifique todos los activos que necesitan protección.
- Determine el nivel de protección que necesita cada activo.
- Determine las responsabilidades del personal.
- Desarrollar consecuencias por incumplimiento de la política de seguridad.

Los documentos de gobierno de seguridad de la información incluyen:

- Políticas
- Procesos
- Procedimientos
- Estándares
- Pautas
- Líneas de base

Key Topic


Policies
Levels of Policies
Categories of Policies
Organizational Policies
System-Specific Policies
Issue-Specific Policies
Regulatory Policies
Advisory Policies
Informative Policies

Directiva de seguridad de la organización

Una directiva de seguridad de la organización es la directiva de seguridad de nivel superior adoptada por una organización. Los objetivos de negocio dirigen la política de seguridad de la organización. Una directiva de seguridad de la organización contiene instrucciones generales y debe tener los siguientes componentes:

- Definir los objetivos generales de la directiva de seguridad.
- Defina los pasos generales y la importancia de la seguridad.
- Definir el marco de seguridad para cumplir los objetivos empresariales.
- Aprobación de la política por parte de la administración estatal, incluido el apoyo a los objetivos y principios de seguridad.
- Defina todos los términos relevantes.
- Definir roles y responsabilidades de seguridad.
- Abordar todas las leyes y regulaciones relevantes.
- Identificar las principales áreas funcionales.
- Definir los requisitos de cumplimiento y las consecuencias de incumplimiento.

Directiva de seguridad específica del sistema	Directiva de seguridad específica del problema	Categorías de políticas
		• Procesos • Procedimientos • Estandares • Directrices • Linea de Base

Continuidad del negocio

Conceptos de Continuidad del Negocio y Recuperación ante Desastres

- Interrupciones
- desastres
  - tecnológico
  - Causado por el ser humano
  - natural
- Recuperación ante desastres y el plan de recuperación ante desastres (DRP)
- Planificación de la continuidad y el plan de continuidad del negocio (BCP)
- Análisis de impacto en el negocio (BIA)
- Plan de contingencia
- disponibilidad
- fiabilidad

Las causas de los desastres se clasifican en tres áreas principales según el origen:

- Desastres tecnológicos
- Desastres causados por el hombre y
- Desastres naturales

Continuidad del Negocio

- Recuperación ante desastres y el plan de recuperación ante desastres (DRP)
- Planificación de la continuidad y el Plan de continuidad del negocio (BCP)
- Análisis de impacto en el negocio (BIA)

Continuidad del Negocio

- Plan de contingencia
- Disponibilidad
- Fiabilidad (Reliability)
- Alcance y plan
- Componentes de personal

Planificación de Contingencias Comerciales

Key Topic

La siguiente lista resume los pasos de SP 800-34 Rev.1:

1. Desarrollar una política de planificación de contingencias.
2. Realizar análisis de impacto empresarial (BIA).
3. Identificar controles preventivos.
4. Crea estrategias de contingencia.
5. Desarrolle un plan de contingencia.
6. Realice pruebas, capacitación y ejercicios del plan de contingencia.
7. Mantén el plan.

Figura 1-12 Publicación especial del NIST 800-34 Rev.1

Plan de continuidad del negocio (BCP)	Plan de continuidad de operaciones (COOP)	Plan de comunicaciones de crisis	Plan de protección de infraestructura crítica (CIP)
Plan de respuesta a incidentes cibernéticos	Plan de recuperación ante desastres (DRP)	Plan de contingencia del sistema de información (ISCP)	Plan de emergencia para ocupantes (OEP)

Desarrollar una política de planificación de contingencias

- Funciones y responsabilidades
- Alcance que se aplica a los tipos de plataforma comunes y funciones de organización
- Necesidades de recursos

Desarrollar una política de planificación de contingencias

- Requisitos de formación
- Programas de ejercicios y pruebas
- Planeación de la programación de mantenimiento
- Frecuencia mínima de copias de seguridad y almacenamiento de medios de copia de seguridad

Los cuatro pasos principales del BIA son los siguientes:

1. Identificar procesos y recursos críticos.
2. Identifique los impactos de las interrupciones y calcule el tiempo de inactividad.
3. Identifique los requisitos de recursos.
4. Identifique las prioridades de recuperación.

Identificar los impactos de las interrupciones y estimar el tiempo de inactividad

Tiempo de inactividad máximo tolerable (MTD)

Tiempo medio de reparación (MTTR)

Tiempo medio entre fallos (MTBF)

Objetivo de tiempo de recuperación (RTO)

Tiempo de recuperación del trabajo (WRT)

Objetivo de punto de recuperación (RPO)

Políticas y procedimientos de seguridad del personal

Políticas y procedimientos de seguridad del personal

- Selección y contratación de candidatos
- Acuerdos y políticas de empleo
- Políticas de incorporación y baja de empleados

Políticas de incorporación y baja de empleados

- Documentar los detalles de la separación
- Tareas y responsabilidades antes de la partida
- Transferencia de conocimientos
- Entrevista de salida

Conceptos sobre políticas y procedimientos de Seguridad del personal

- Acuerdos y controles de proveedores, consultores y contratistas
- Requisitos de la política de cumplimiento de normas
- Requisitos de la política de privacidad
- Rotación de trabajos
- Separación de funciones

Conceptos de gestión de riesgos

Conceptos de gestión de riesgos

Directiva de gestión de riesgos

equipo de gestión de riesgos

equipo de análisis de riesgos

Evaluación de riesgos

Aplicación

Categorías de control

Tipos de control

Evaluación

Monitoreo y medición del control

Presentación de informes y mejora continua

Marcos de riesgo.

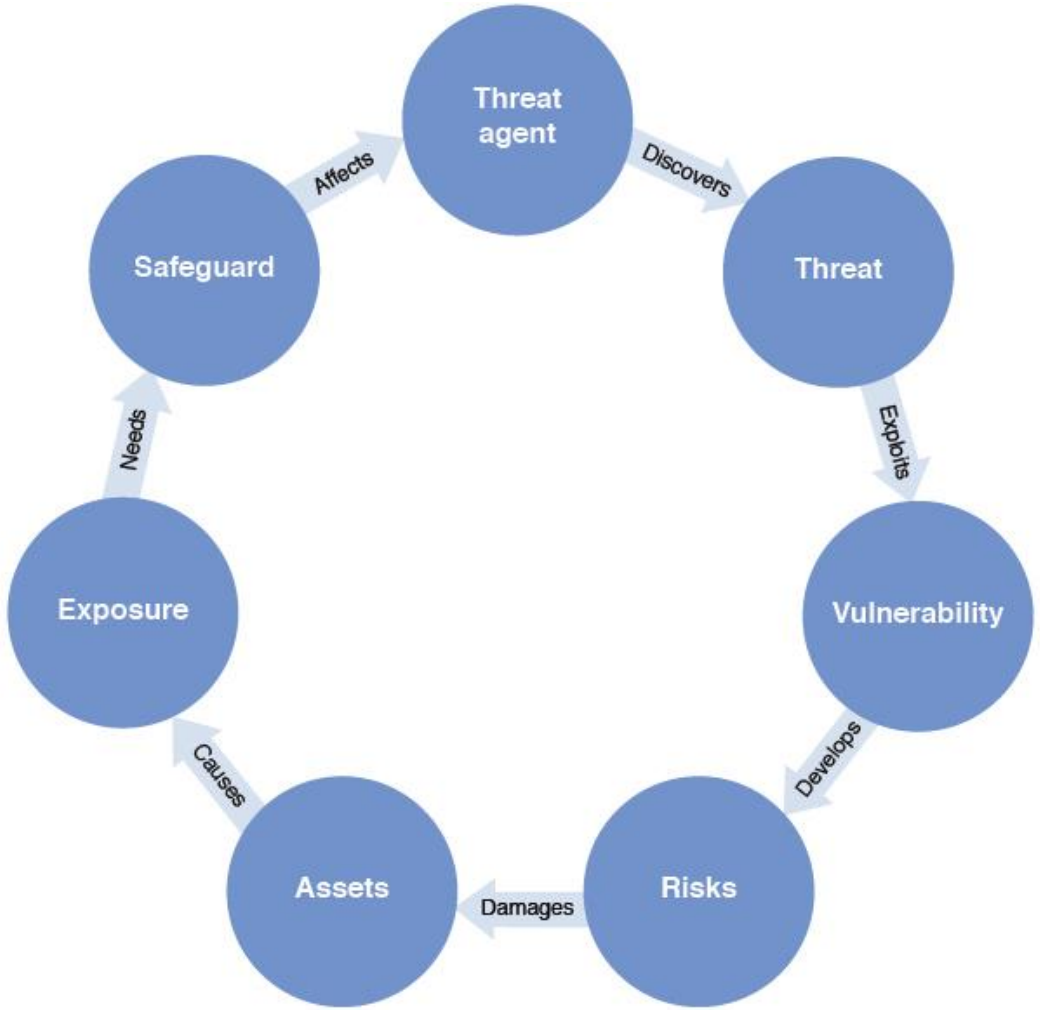
Hay tres elementos básicos utilizados para determiner el valor de un activo

- El costo inicial y continuo de compra, licencia, desarrollo y mantenimiento del activo físico o de información
- El valor del activo para las operaciones de la empresa
- El valor del activo establecido en el mercado externo y el valor estimado de la propiedad intelectual

Elementos adicionales, incluidos los siguientes:

- Valor del activo para los adversarios
- Costo para reemplazar el activo si se pierde
- Costos operativos y de productividad incurridos si el activo no está disponible
- Problemas de pasivo si el activo está comprometido

Todos los conceptos de seguridad trabajan juntos en una relación que se muestra en la figura 1-13.



Gestion de Riesgos

- Apetito de riesgo
- Política de gestión de riesgos
- Equipo de Gestión de Riesgos
- Equipo de análisis de riesgos

Evaluación de riesgos

- Identificar los activos y el valor de los activos.
- Identificar vulnerabilidades y amenazas.
- Calcule la probabilidad de amenaza y el impacto en el negocio.
- Equilibre el impacto de la amenaza con el costo de la contramedida.

Valor y costo de la información y los activos (tangibles/intangibles)

- Valor para el propietario
- Trabajo necesario para desarrollar u obtener el activo
- Costes de mantenimiento del activo
- Daños que resultarían si el activo se perdiera
- Costo que los competidores pagarían por el activo
- Sanciones que resultarían si el activo se perdiera

Después de determinar el valor de los activos, debe determinar las vulnerabilidades y amenazas a cada activo.

Identificar amenazas y vulnerabilidades

Humano: Incluye tanto a los insiders maliciosos como a los no maliciosos, terroristas, espías y personal despedido

Natural: Incluye inundaciones, incendios, tornados, huracanes, terremotos u otros desastres naturales o eventos climáticos

Aspectos técnicos: Incluye errores de hardware y software, código malintencionado y nuevas tecnologías

Físico: Incluye problemas de CCTV, fallas en las medidas perimetrales y fallas biométricas

Medio ambiente: Incluye fallas de energía y otros servicios públicos, problemas de tráfico, guerra biológica y problemas de materiales peligrosos (como derrames)

Operativo: Incluye cualquier proceso o procedimiento que pueda afectar a la CIA

Evaluación/análisis de riesgos

Análisis cuantitativo de riesgos

$$SLE = AV \times EF$$

$$ALE = SLE \times ARO$$

Análisis cualitativo de riesgos

- Alto
- Moderado
- Bajo

Conceptos de gestión de riesgos

Evaluación de riesgos

- Identificar los activos y el valor de los activos.
- Identificar vulnerabilidades y amenazas.
- Calcule la probabilidad de amenaza y el impacto en el negocio.
- Equilibre el impacto de la amenaza con el costo de la contramedida.

Selección de contramedidas (salvaguardia)

Los criterios para elegir una salvaguardia es la rentabilidad de la salvaguardia o el control, por razones de cumplimiento o para cumplir obligaciones contractuales.

Los costos de planificación, diseño, implementación y mantenimiento deben incluirse en la determinación del costo total de una salvaguardia.

Riesgo inherente vs. a riesgo residual

Manejo de riesgos y respuesta a riesgos

- Evitación de riesgos
- Transferencia de riesgos
- Mitigación de riesgos
- Aceptación del riesgo

Categorías de control

- Compensativo
- Correctivo
- Detective
- Disuasivo
- Directiva
- Preventivo
- Recuperación

Tipos de control

- Controles administrativos (de gestión)
- Controles lógicos (técnicos)
- Controles físicos

El marco de gestión de riesgos del NIST incluye los siguientes pasos:

- Categorizar los sistemas de información.
- Seleccione los controles de seguridad.
- Implementar controles de seguridad.
- Evaluar los controles de seguridad.
- Autorizar sistemas de información.
- Supervisar los controles de seguridad.

FIPS 199 proporciona un gráfico útil que clasifica los niveles de CIA para los activos de información, como se muestra en la Tabla 1-6.

Principio de la CIA	Bajo	moderado	Alto
confidencialidad	La divulgación no autorizada tendrá un efecto adverso limitado en la organización.	La divulgación no autorizada tendrá graves efectos adversos en la organización.	La divulgación no autorizada tendrá graves efectos adversos en la organización.
integridad	La modificación no autorizada tendrá un efecto adverso limitado en la organización.	La modificación no autorizada tendrá graves efectos adversos en la organización.	La modificación no autorizada tendrá graves efectos adversos en la organización.
disponibilidad	La falta de disponibilidad tendrá un efecto adverso limitado en la organización.	La falta de disponibilidad tendrá graves efectos adversos en la organización.	La falta de disponibilidad tendrá graves efectos adversos en la organización.

En la Tabla 1-7 se enumeran las familias de control NIST SP 800-53

- Control de acceso (CA)
- Sensibilización y formación (AT)
- Auditoría y rendición de cuentas (AU)
- Evaluación y autorización de seguridad (CA)
- Administración de configuración (CM)
- Planificación de contingencia (CP)
- Identificación y autenticación (IA)
- Respuesta a incidentes (IR)
- Mantenimiento (MA)
- Protección de medios (MP)
- Protección física y ambiental (PE)
- Planificación (PL)
- Administración de programas (PM)
- Seguridad del personal (PS)
- Evaluación de riesgos (AR)
- Adquisición de Sistemas y Servicios (SA)
- Protección del sistema y las comunicaciones (SC)
- Integridad del sistema y de la información (SI)

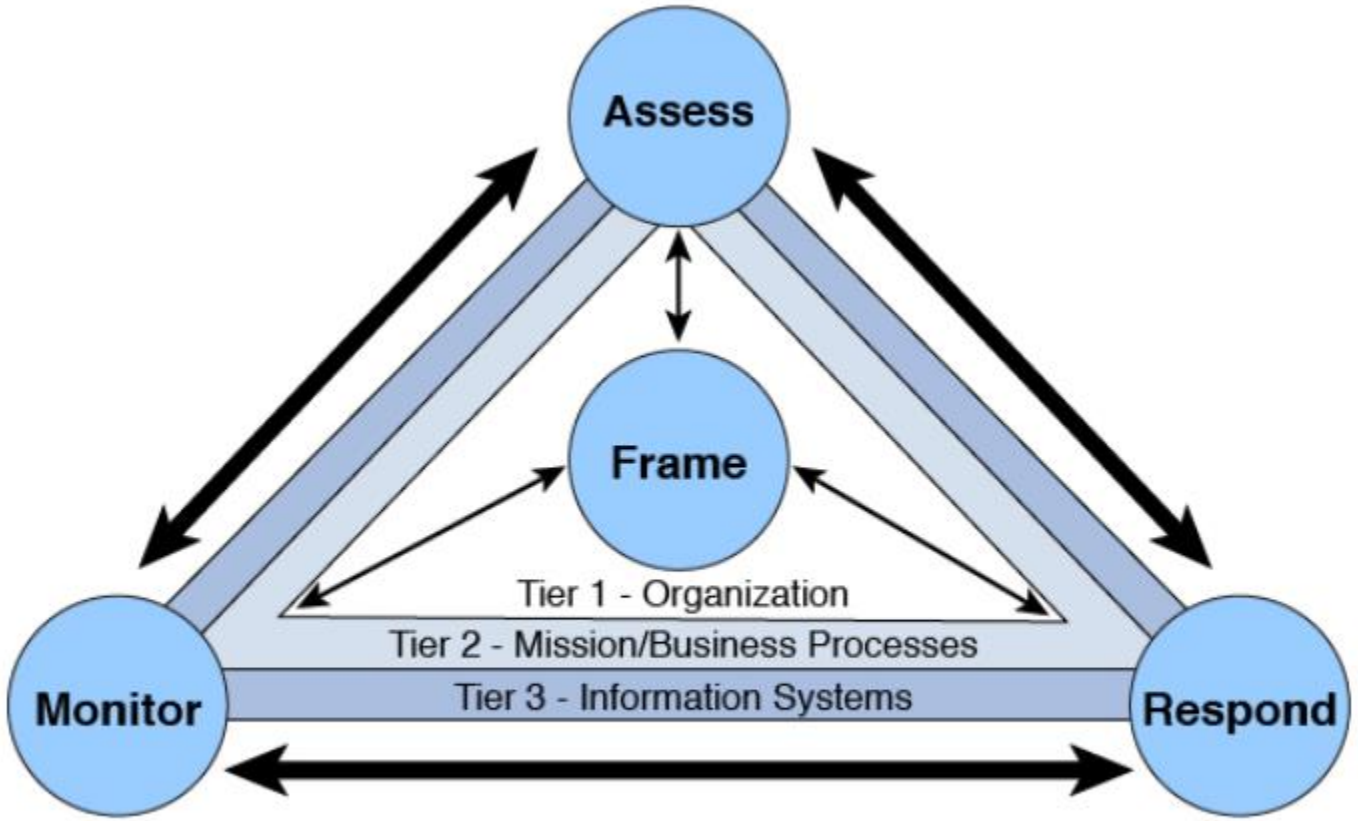
El proceso de esta publicación del NIST incluye los siguientes pasos:

1. Seleccione las líneas base de control de seguridad.
2. Adapte los controles de seguridad de línea base.
3. Documente el proceso de selección del control.
4. Aplicar el proceso de selección de control a nuevos sistemas de desarrollo y heredados.

NIST SP 800-30 identifica los siguientes pasos en el proceso de evaluación de riesgos:

1. Prepárese para la evaluación.
2. Realizar la evaluación.
    1. Identificar orígenes y eventos de amenazas.
    2. Identificar vulnerabilidades y condiciones predisponentes.
    3. Determinar la probabilidad de ocurrencia.
    4. Determinar la magnitud del impacto.
    5. Determinar el riesgo como una combinación de probabilidad e impacto.
3. Comunicar resultados.
4. Mantener la evaluación.

La Figura 1-19 muestra el proceso de gestión de riesgos aplicado en los tres niveles identificados en NIST SP 800-39.



El proceso de gestión de riesgos implica los siguientes pasos:

- Planear Riesgo.
- Evaluar el riesgo.
- Responder al riesgo.
- Monitorear el riesgo.

Marco del NIST para mejorar la ciberseguridad de infraestructuras críticas

1. **Identificar (ID):** Desarrollar la comprensión organizacional para administrar el riesgo de ciberseguridad para los sistemas, activos, datos y capacidades.
2. **Proteger (PR):** Desarrollar e implementar las salvaguardias apropiadas para garantizar la prestación de servicios de infraestructura crítica.
3. **Detectar (DE):** Desarrollar e implementar las actividades adecuadas para identificar la ocurrencia de un evento de ciberseguridad.
4. **Responder (RS):** Desarrollar e implementar las actividades adecuadas para tomar medidas con respecto a un evento de ciberseguridad detectado.
5. **Recuperar (RC):** Desarrollar e implementar las actividades apropiadas para mantener planes de resiliencia y restaurar cualquier capacidad o servicio que se haya visto afectado debido a un evento de ciberseguridad.

Marco del NIST para mejorar la ciberseguridad de infraestructura crítica

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Los pasos siguientes ilustran cómo una organización podría usar el marco para crear un nuevo programa de ciberseguridad o mejorar un programa existente. Estos pasos deben repetirse según sea necesario para mejorar continuamente la ciberseguridad.

- Priorizar y alcance.
- Orientar.
- Crear un perfil actual.
- Realizar una evaluación de riesgos.
- Cree un perfil de destino.
- Determine, analice, y dé prioridad a boquetes.
- Implementar el plan de acción.

Según ISO/IEC 27005:2011, el proceso de gestión de riesgos consta de los siguientes pasos:

1. **Establecimiento de contexto:** Define el límite de la gestión de riesgos.
2. **Análisis de Riesgos (Fases de Identificación de Riesgos y Estimación):** Evalúa el nivel de riesgo.
3. **Evaluación de riesgos (fases de análisis y evaluación de riesgos):** Analiza los riesgos identificados y tiene en cuenta los objetivos de la organización.
4. **Tratamiento de riesgos (fases de tratamiento de riesgos y aceptación de riesgos):** Determina cómo controlar los riesgos identificados.
5. **Comunicación de riesgos:** Comparte información sobre el riesgo entre los responsables de la toma de decisiones y otras partes interesadas.
6. **Monitoreo y revisión de riesgos:** Detecta cualquier riesgo nuevo y mantiene el plan de gestión de riesgos.

Amenazas Geográficas

Cuadro 1-9 Clases de extintores de incendios

clase	Tipo de fuego
Clase A	Combustibles ordinarios
Clase B	Líquidos inflamables, gases inflamables
Clase C	Equipo eléctrico
Clase D	Metales combustibles
Clase K	Aceite de cocina o grasa

Modelado de amenazas

- Modelado de amenazas centrado en la aplicación
- Modelado de amenazas centrado en activos
- Modelado de amenazas centrado en el atacante

Independientemente del método de modelado de amenazas que decida usar, los pasos básicos del proceso de modelado de amenazas son los siguientes:

- Identificar activos.
- Identificar agentes de amenazas y posibles ataques.
- Investigar las contramedidas existentes en uso por la organización.
- Identifique las vulnerabilidades que se pueden aprovechar.
- Priorizar los riesgos identificados.
- Identificar contramedidas para reducir el riesgo de la organización.

Modelo STRIDE

- Suplantación de identidad de usuario
- Manipulación
- Repudio
- Divulgación de información
- Denegación de servicio (DoS)
- Elevación de privilegios

NIST SP 800-154

- Identificar y caracterizar el sistema y los datos de interés.
- Identifique y seleccione los vectores de ataque que se incluirán en el modelo.
- Caracterizar los controles de seguridad para mitigar los vectores de ataque.
- Analizar el modelo de amenazas.

Algunos ejemplos de actores de la amenaza

Actores internos

- Empleado imprudente
- Empleado no capacitado
- Socio
- Empleado descontento
- Espía interno
- Espía del gobierno
- Vendedor
- Ladrón

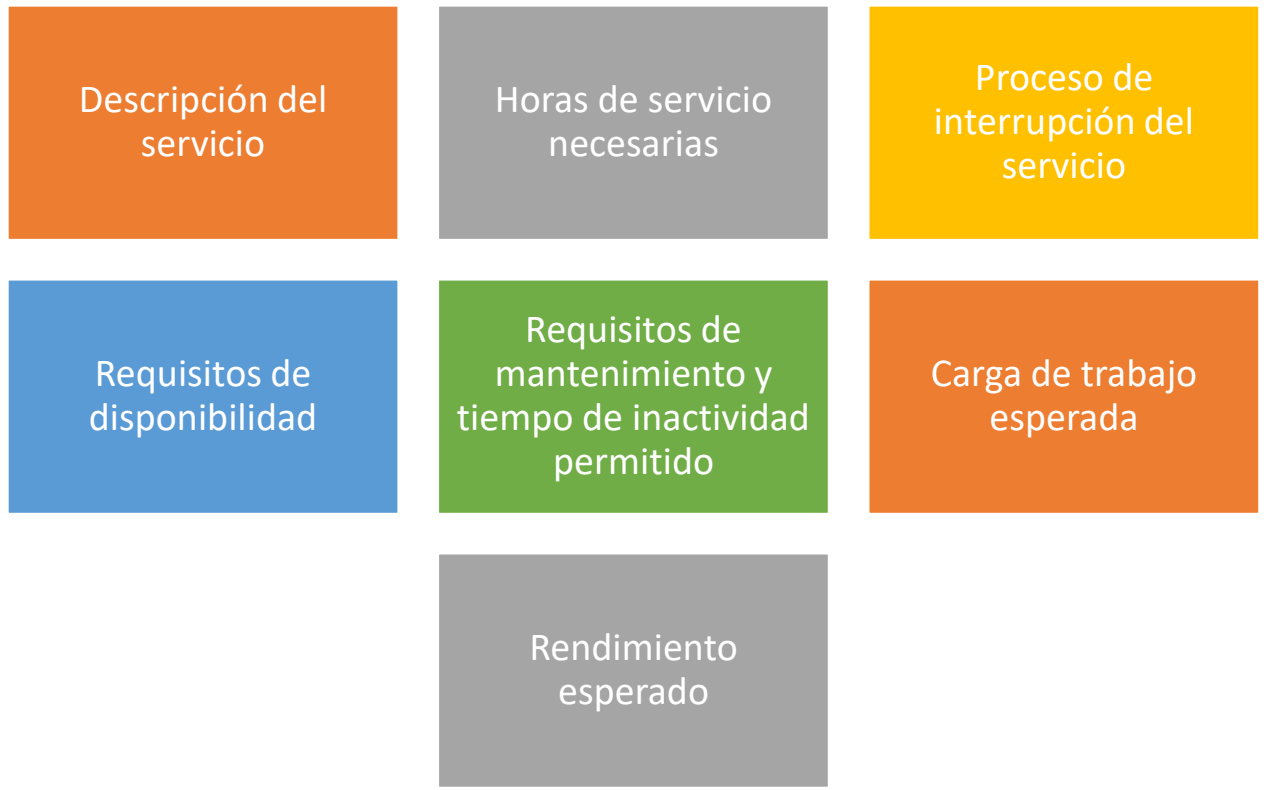
Actores externos

- Anarquista
- Competidor
- Funcionario corrupto del gobierno
- Minero de datos
- Guerrero cibernético del gobierno
- Individuo irracional
- Adversario legal
- Mafioso
- Activista
- Terrorista
- Vándalo

Una organización necesita analizar cada uno de estos actores de amenaza de acuerdo con los criterios establecidos. La organización debe dar a cada actor de amenaza una clasificación para ayudar a determinar cuáles deben analizarse. Algunos ejemplos de algunos de los criterios más utilizados son los siguientes:

- **Nivel de habilidad:** Ninguno, mínimo, operativo, adepto
- **Recursos:** Individual, equipo, organización, gobierno
- **Visibilidad:** De forma intachual, encubierta, clandestina, no importa
- **Objetivo:** Copiar, destruir, lesionar, tomar, no importa
- **Resultado:** Adquisición/robo, ventaja comercial, daño, vergüenza, ventaja técnica

Antes de que se pueda escribir y firmar un SLA



Referencias