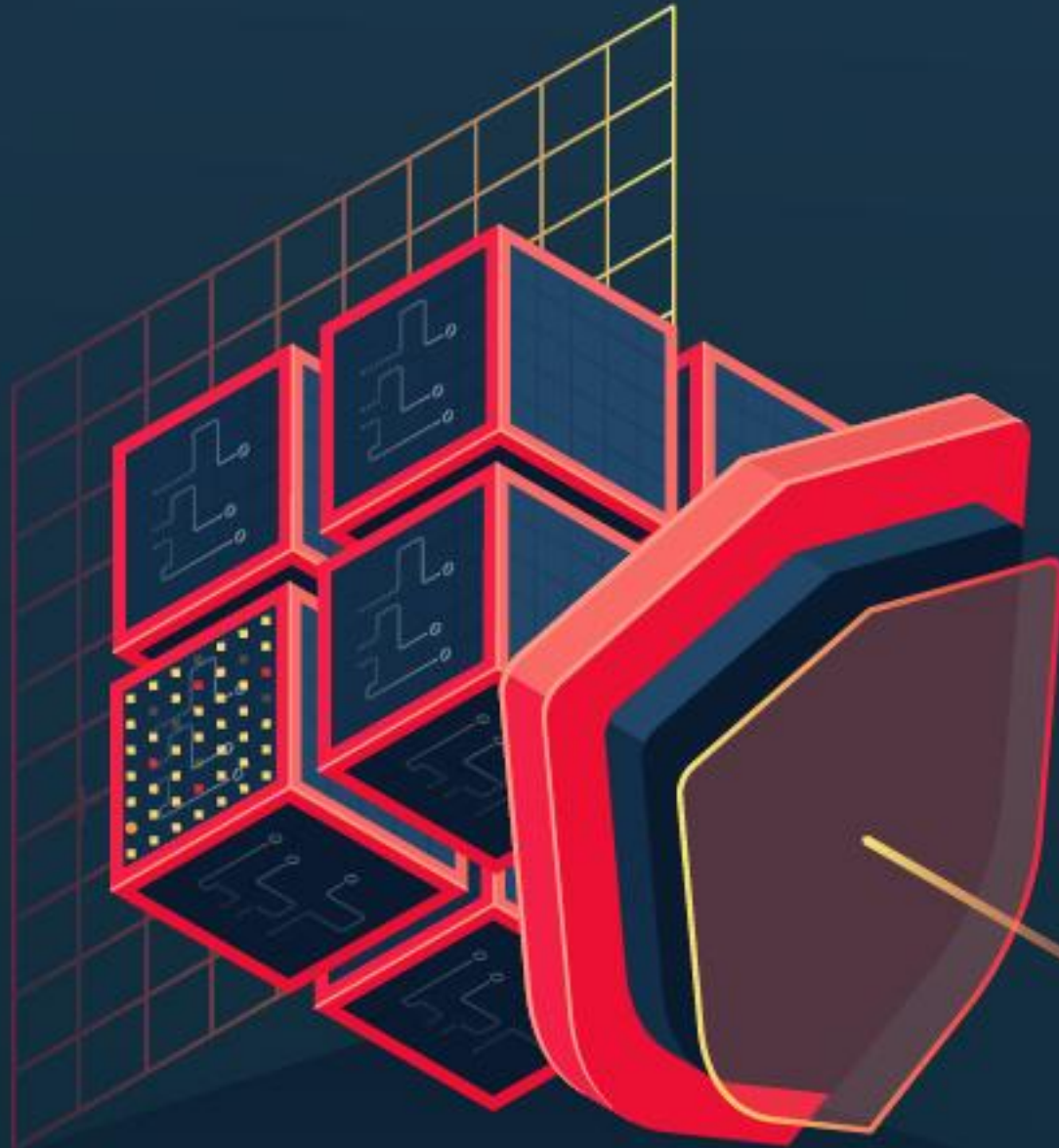




ECUADOR
UNIVERSIDAD
INTERNACIONAL
SEK



FUNDAMENTOS DE CIBERSEGURIDAD

Ing. José Luis Medina

Definición de Políticas

Políticas de Seguridad

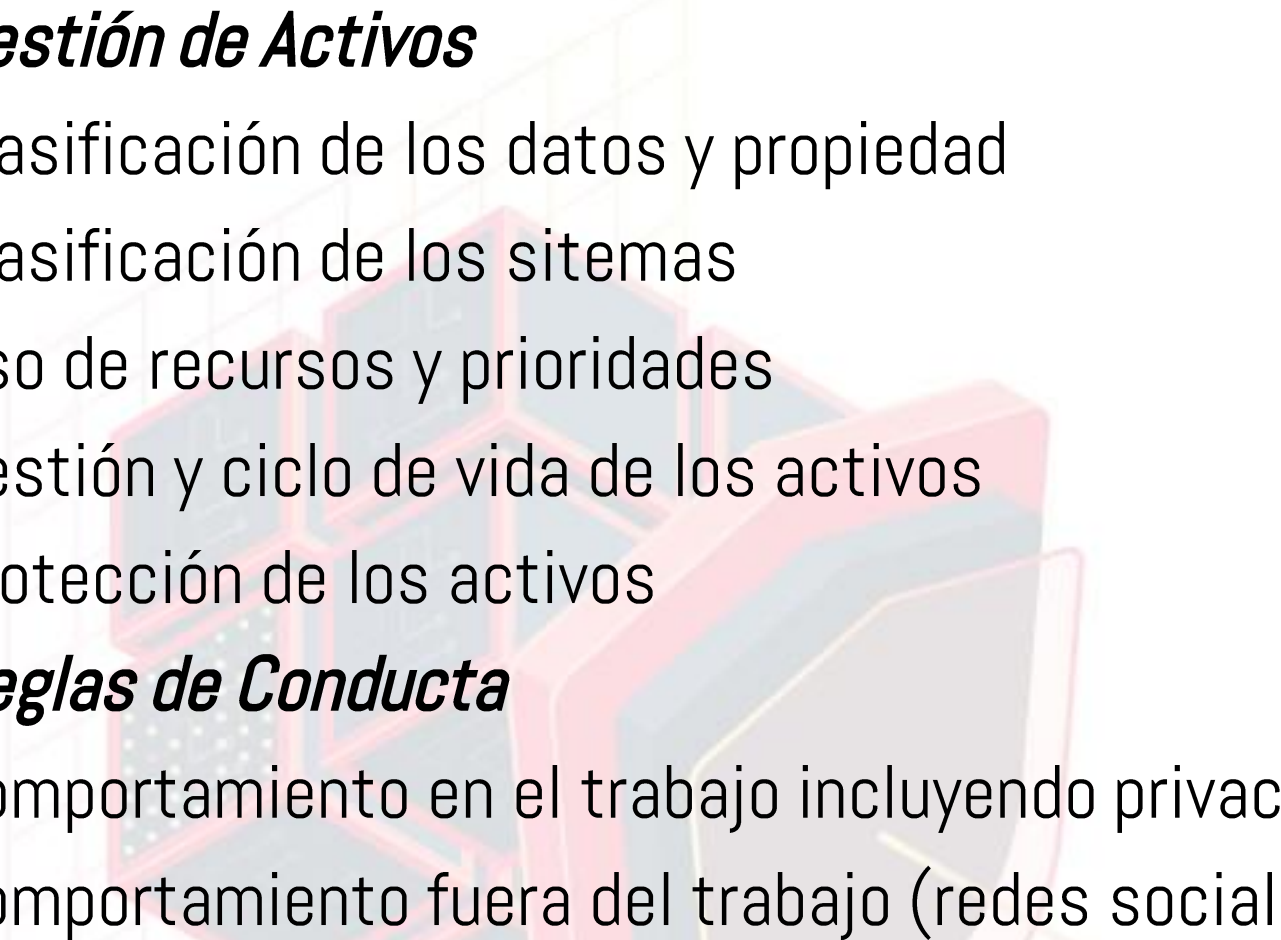
- Son un elemento muy importante dentro de la ciberseguridad
- **Son documentos** que establecen las reglas del juego en seguridad informática, estas cubren toda la organización
- Las políticas deben **crearse** correctamente, **validarse** y estas deben ser **aprobadas** por el **consejo directivo**
- El **ciclo de vida** de las políticas de seguridad definen un proceso formal de **creación** para cada documento, **revisado**, **aprobado** y **actualizado** por lo menos una vez al año
- Deben ser **claras** y **concisas**



Conjunto de políticas propuesta por
COBIT5

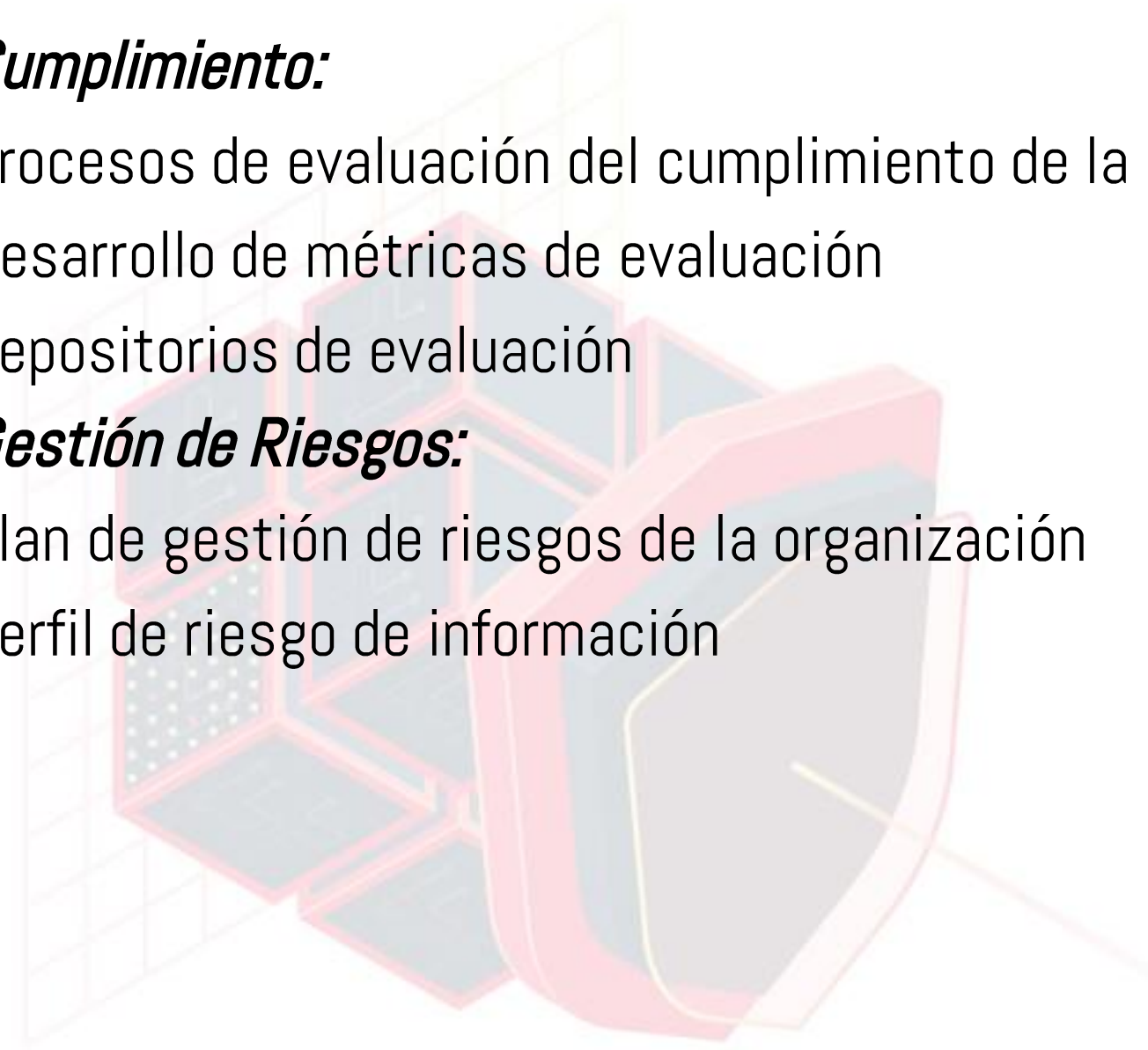
- ***Continuidad del negocio y recuperación de desastres***
- Análisis del impacto en el negocio (BIA)
- BCPs (Plan de Continuidad del negocio)
- DRP (Plan de recuperación ante desastres)
- Umbrales definidos para las contingencias



- 
- ***Gestión de Activos***
 - Clasificación de los datos y propiedad
 - Clasificación de los sistemas
 - Uso de recursos y prioridades
 - Gestión y ciclo de vida de los activos
 - Protección de los activos
 - ***Reglas de Conducta***
 - Comportamiento en el trabajo incluyendo privacidad (internet/mail, uso de activos)
 - Comportamiento fuera del trabajo (redes sociales)

- ***Gestión de Proveedores***
- Gestión de contratos con proveedores
- ***Adquisición, Desarrollo, Mantenimiento***
- Gestión de compras
- Políticas de codificación
- Integración, gestión de cambios y gestión de la configuración
- ***Comunicaciones y Operaciones***
- Arquitectura de Seguridad de la información y diseño de aplicaciones
- Acuerdos de Nivel de Servicio

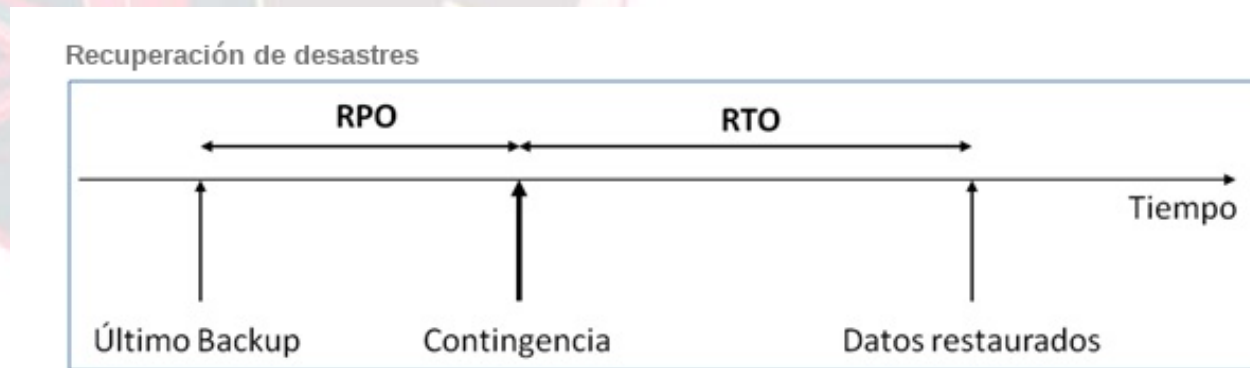
- ***Cumplimiento:***
- Procesos de evaluación del cumplimiento de la seguridad de la información TI
- Desarrollo de métricas de evaluación
- Repositorios de evaluación
- ***Gestión de Riesgos:***
- Plan de gestión de riesgos de la organización
- Perfil de riesgo de información



Política de respuesta ante incidentes

- Esta política se encarga de la necesidad de **responder** ante los **incidentes** de seguridad informática (ciberseguridad) reportados a fin de recuperar la actividad empresarial
- La política debe incluir una definición de incidentes de seguridad informática (Ciberseguridad) además de una política que indique como tratar estos incidentes
- La política debe tener un factor de criticidad según el incidente, además el equipo de TI (personas) con cada una de sus responsabilidades para responder al incidente

- ***RPO (Recovery Point Objective)***
- Se refiere al tiempo que transcurre entre el momento del desastre de TI y el último punto de restauración de los datos, es decir la tolerancia por parte de la organización en referencia a la cantidad de datos que está dispuesta a perder ante un fallo de seguridad o caso fortuito
- ***RTO (Recovery Time Objective)***
- Se refiere al 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 la continuidad del negocio



Controles de Ciberseguridad

- Los controles de seguridad son fundamentales para mantener la seguridad dentro de la infraestructura de TI de cualquier organización
- Un recurso excelente para la aplicación de estos controles lo provee el Centro para la Seguridad de Internet (**Center for Internet Security, CIS**), el cual propone la aplicación de 20 controles críticos de seguridad.



Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

CIS Control 1: Inventario de Dispositivos autorizados y no autorizados

Gestione activamente todo dispositivo hardware en la red (inventario, seguimiento y corrección), de tal manera que solo los dispositivos autorizados obtengan acceso y que los dispositivos no autorizados y no gestionados sean detectados y se prevenga que obtengan acceso.

CIS Control 2: Inventario de Software autorizados y no autorizados

Gestione activamente todo software en la red (inventario, seguimiento y corrección), de tal manera que solo software autorizado esté instalado y pueda ejecutarse, y que el software no autorizado y no gestionado sea encontrado y se prevenga su instalación y ejecución.

CIS Control 3: Gestión continua de vulnerabilidades

Adquirir, evaluar y tomar medidas continuamente sobre nueva información para identificar vulnerabilidades, remediar y minimizar la ventana de oportunidad para los atacantes.



CIS Control 4: Uso controlado de privilegios administrativos

Los procesos y herramientas utilizados para rastrear, controlar, prevenir y corregir el uso, la asignación y la configuración de privilegios administrativos en computadoras, redes y aplicaciones.



CIS Control 5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores

Establezca, implemente y gestione activamente (rastree, informe, corrija) la configuración de seguridad de dispositivos móviles, computadoras portátiles, servidores y estaciones de trabajo utilizando una rigurosa gestión de configuraciones y un proceso de control de cambios para evitar que los atacantes exploten servicios y configuraciones vulnerables.



CIS Control 6: Mantenimiento, monitoreo y análisis de logs de auditoría

Reúna, administre y analice registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.



CIS Control 7: Protección de correo electrónico y navegador web

Minimizar la superficie de ataque y la oportunidad para atacantes de manipular el comportamiento humano a través de su interacción con navegadores web y sistemas de correo electrónico.



CIS Control 8: Defensa contra malware

Controlar la instalación, propagación y ejecución de código malicioso en múltiples puntos de la organización, al mismo tiempo que optimizar el uso de automatización para permitir la actualización rápida de la defensa, la recopilación de datos y la acción correctiva.



CIS Control 9: Limitación y control de puertos de red, protocolos y servicios

Administrar (rastrear/controlar/corregir) el uso operacional continuo de puertos, protocolos y servicios en dispositivos en red para minimizar las ventanas de vulnerabilidad disponibles para los atacantes.



CIS Control 10: Capacidad de recuperación de datos

Los procesos y herramientas utilizadas para respaldar adecuadamente la información crítica con una metodología comprobada para la recuperación oportuna de la misma.



CIS Control 11: Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores

Establecer, implementar y gestionar activamente (rastrear, reportar, corregir) la configuración de seguridad de la infraestructura de red utilizando un proceso de gestión de configuración y control de cambios riguroso para prevenir que los atacantes exploten servicios y configuraciones vulnerables.



CIS Control 12: Defensa de borde

Detectar/prevenir/corregir el flujo de información que transfieren redes de diferentes niveles de confianza con un enfoque en datos que dañan la seguridad.





CIS Control 13: Protección de datos

Los procesos y herramientas utilizadas para prevenir la exfiltración de datos, mitigar el efecto de la exfiltración de datos y asegurar la privacidad e integridad de la información sensible.



CIS Control 14: Control de acceso basado en la necesidad de conocer

Los procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el acceso seguro a activos críticos (por ejemplo, información, recursos, sistemas) de acuerdo con la determinación formal de qué personas, computadoras y aplicaciones tienen una necesidad y derecho a acceder a estos activos críticos basado en una clasificación aprobada.



CIS Control 15: Control de acceso inalámbrico

Los procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el uso seguro de las redes de área local inalámbricas (WLAN), puntos de acceso y sistemas de clientes inalámbricos.



CIS Control 16: Monitoreo y control de cuentas

Gestione activamente el ciclo de vida de las cuentas del sistema y de aplicaciones (su creación, uso, latencia, eliminación) con el fin de minimizar las oportunidades para que los atacantes las aprovechen.

CIS Control 17: Implementar un programa de concienciación y entrenamiento de seguridad

Para todos los roles funcionales en la organización (priorizando aquellos que son misionales para la organización y su seguridad), identificar los conocimientos, habilidades y capacidades específicos necesarios para soportar la defensa de la empresa; desarrollar y ejecutar un plan integral para evaluar, identificar brechas y remediar a través de políticas, planificación organizacional, capacitación y programas de concienciación.

CIS Control 18: Seguridad del software de aplicación

Gestione el ciclo de vida de seguridad de todo el software interno desarrollado y adquirido para prevenir, detectar y corregir las debilidades de seguridad.

CIS Control 19: Respuesta y manejo de incidentes

Proteger la información de la organización, así como su reputación, desarrollando e implementando una infraestructura de respuesta a incidentes (por ejemplo, planes, funciones definidas, capacitación, comunicaciones, supervisión de la gestión) para descubrir rápidamente un ataque y luego contener de manera efectiva el daño, erradicando la presencia del atacante y restaurando la integridad de la red y los sistemas.

CIS Control 20: Pruebas de penetración y ejercicios de equipo rojo

Probar la fortaleza general de la defensa de una organización (la tecnología, los procesos y las personas) simulando los objetivos y las acciones de un atacante.

Bibliografía

- ISACA, Fundamentos de Ciberseguridad, Segunda Edición, 2017
- ESTRADA Corletti Alejandro, Ciberseguridad una estrategia informático / militar, Nov. 2017
- CIS, 20 controles críticos

