Seguridad Informática

Profesor: Pedro Pinacho Davidson

ppinacho@inf.udec.cl

Conceptos básicos

Security Governance

- Colección de prácticas relacionadas con **soportar, evaluar, definir y dirigir el esfuerzo de seguridad** de una organización
- Dirigido por una junta directiva, organizaciones pequeñas pueden estar a cargo de un:
  - Chief executive officer **(CEO)**
  - O Chief information security officer **(CISO)**
- Dirección estrechamente relacionado con Gobierno TI.
- **Security es actualmente considerado un proceso de la organización.**
- Existen múltiples frameworks y guías de gobierno de la ciberseguridad NIST SP 800-53, NIST SP 800-100, enfocados en gobierno y defensa per adoptado y adaptado a otros tipos de organizaciones.

Principios de Gestión de la Seguridad de Información: *Segregación de Funciones*

- Garantizando Integridad y Evitando Conflictos de Interés
- **Definición:** Dividir responsabilidades críticas.
  - **Prevención de Fraudes**: Reducción de actos indebidos.
  - **Minimiza Errores:** Detecta y corrige rápidamente.
  - **Auditoría y Conformidad**: Sin un único punto de falla.
  - **Confianza en el Sistema**: Responsabilidades distribuidas.

Principios de Gestión de la Seguridad de Información: *Privilegios mínimos*

- **Definición: Otorgar solo los permisos necesarios.**
  - Reducción de Riesgos: Menor acceso, menor vulnerabilidad (contención).
  - Control Efectivo: Gestión simplificada de derechos.
  - Auditoría y Conformidad: Facilidad en seguimiento de permisos.
  - Optimización de la Seguridad: Asegurando acceso necesario.

Principios de Gestión de la Seguridad de Información: *Necesidad de Saber*

- **Definición: Acceso basado en la relevancia de la tarea.**
  - Protección de Datos: Limita la exposición de información.
  - Reducción de Brechas: Menos acceso, menos puntos de ataque.
  - Auditoría y Conformidad: Rastreo claro de quién accede a qué.
  - Fortalecimiento de la Confidencialidad: Solo lo esencial es visible..

Compromiso Directivo en Seguridad de la Información

LIDERAZGO: DEFINIR Y PROMOVER LA CULTURA DE SEGURIDAD.

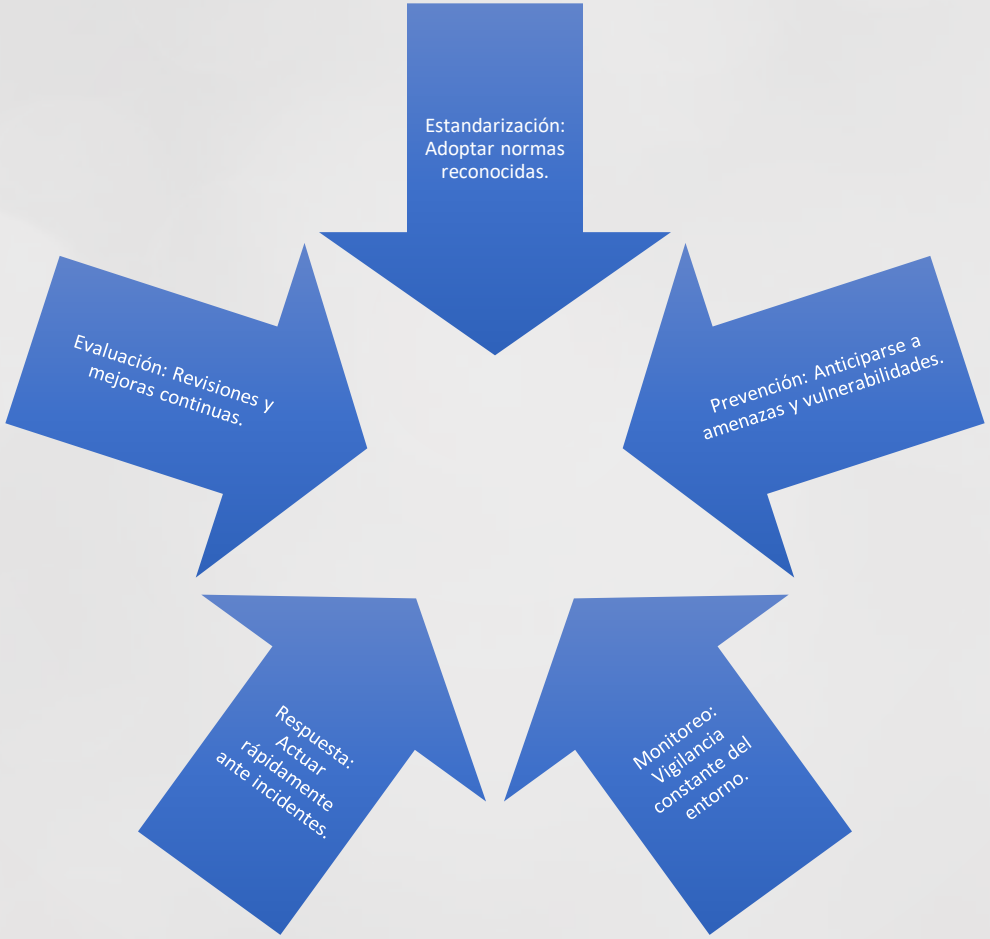
RECURSOS: ASEGURAR LA INVERSIÓN ADECUADA EN HERRAMIENTAS Y PERSONAL.

POLÍTICAS: ESTABLECER Y RESPALDAR DIRECTRICES CLARAS.

COMUNICACIÓN: FOMENTAR LA SENSIBILIZACIÓN Y FORMACIÓN.

VISIÓN INTEGRAL: ALINEAR SEGURIDAD CON OBJETIVOS EMPRESARIALES.

Buenas Prácticas y Controles



El importante rol del usuario

Primera Línea de Defensa: Usuarios alertas minimizan riesgos.

Concienciación: Formación y sensibilización constante.

Prácticas Seguras: Uso adecuado de tecnologías y recursos.

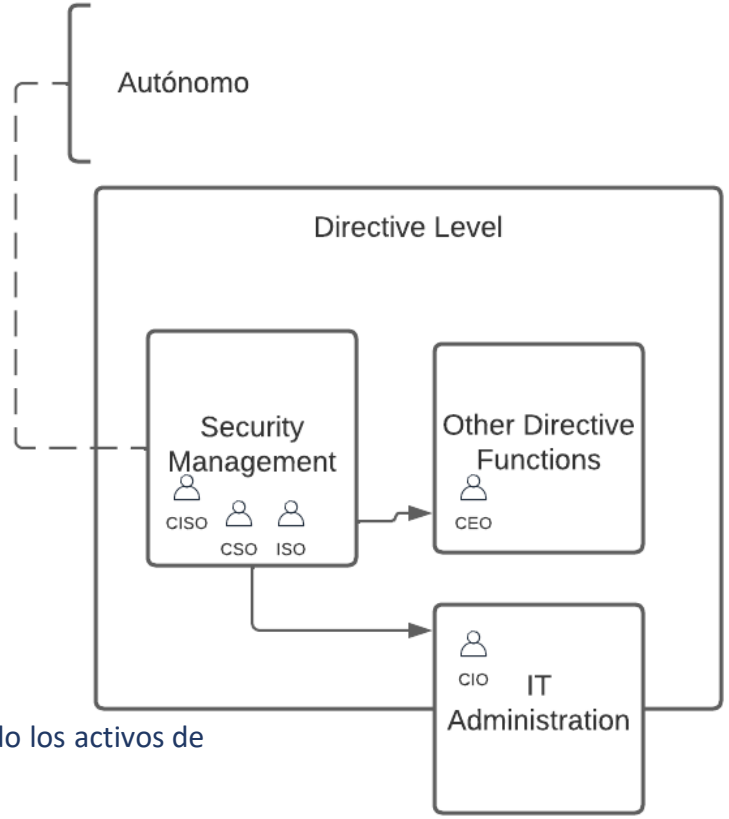
Reporte Activo: Notificar incidentes y sospechas.

Responsabilidad Compartida: Seguridad es tarea de todos.

Administrando la Función de Seguridad

- La **seguridad debe ser medible**.
  - Esto permite **evaluar la postura**
  - Evaluar el **efecto de los controles** adoptados
  - Se debe desarrollar e implementar una **estrategia**
  - Debe asegurar la apropiada creación, implementación y aplicación de una **política de seguridad**.
  - Debe de la organización.
    - **Seguridad basada en casalinearse a objetivos, misión y metas os de negocio**
  - Lo mejor es asumir un enfoque Top-Down

Organización



CISO (Chief Information Security Officer)

- **Enfoque principal:** Seguridad de la información.
- **Responsabilidades:** El CISO se encarga de la estrategia global de seguridad de la información de la empresa, protegiendo los activos de información contra amenazas internas y externas.

CSO (Chief Security Officer)

- **Enfoque principal:** Seguridad global, incluyendo seguridad física y de la información.
- **Responsabilidades:** El CSO tiene una perspectiva más amplia que el CISO, abarcando tanto la seguridad física como la cibernética. Esto puede incluir la gestión de la seguridad de las instalaciones físicas, empleados, y activos, además de las responsabilidades relacionadas con la seguridad de la información.

ISO (Information Security Officer)

- **Enfoque principal:** Implementación de la seguridad de la información.
- **Responsabilidades:** A menudo reportando al CISO o al CSO, el ISO se centra en la implementación de políticas y procedimientos de seguridad específicos dentro de la organización. Este rol implica la supervisión del día a día de las operaciones de seguridad, la formación de empleados en buenas prácticas de seguridad, y la respuesta a incidentes de seguridad.

CIO (Chief Information Officer)

- **Enfoque principal:** Estrategia y gestión de las Tecnologías de la Información (TI).
- **Responsabilidades:** El CIO se ocupa de la visión global de la tecnología dentro de la organización, asegurando que las TI soporten los objetivos empresariales.

Otros Roles para resguardar la ciberseguridad

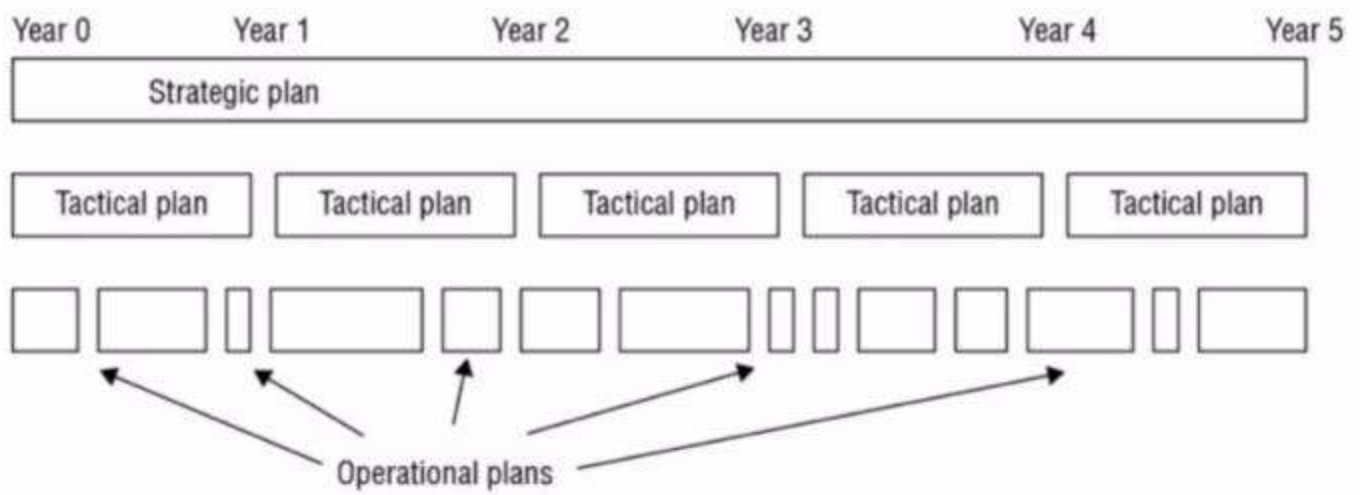
Garantizando la integridad de una organización

- Implica distintos roles:
  - **CISO** (Chief Information Security Officer): Lidera la estrategia de seguridad.
  - **Analista de seguridad**: Monitorea amenazas y alertas.
  - **Ingeniero de seguridad**: Diseña soluciones de protección.
  - **Auditor de seguridad**: Evalúa y reporta vulnerabilidades.
  - **Respuesta a incidentes:** Gestiona y mitiga los ataques.
  - **Formador de concienciación**: Entrena al personal en prácticas seguras.

Funciones de Dirección de Seguridad

- **Definir roles** de seguridad
- Establecer **cómo se administrará** la seguridad
- **Cómo se verificará** la efectividad de los controles
- **Desarrollar políticas de seguridad**
- Realizar **análisis de riesgos**
- **Educar** a los trabajadores

Strategic, tactical and operational plan timeline comparison



Roles y Responsabilidades

- Los roles más comunes en seguridad de la información son los siguientes:
  - **Senior Manager**: organizational owner, último responsable, firma todas las políticas, en la mayoría de los casos es un ente de gestión y no profesional en ciberseguridad.
  - **Security professional:** incluye a infoSec officer, Computer Incident Reponse Team (CIRT), entre otros y está asignado a personal entrenado y con experiencia en redes, sistemas y seguridad. Deben seguir las directivas del Senior Manager.
  - **Asset Owner:** Encargado de clasificar la información para su protección y acceso. Típicamente gestores de alto rango
  - **Custodian:** Encargado de implementar la protección definida por políticas de seguridad y Senior Management. Encargado de preservar la Triada CIA, y cumplir con responsabilidades delegadas de Asset Owner. Cumplen tareas como: testing backups, validar integridad de datos, implementar soluciones de seguridad, administrar data storage basados en clasificación de datos.
  - **User:** personas que operan sistemas asegurados, están limitados por el principio de mejor privilegio posible, y son responsables de conocer y observar las políticas de seguridad.
  - **Auditor:** encargados de verificar que la política de seguridad esté implementada y que las soluciones de seguridad son adecuadas, aporta al cumplimiento y reportes de efectividad revisados por Senior Management, entregan información importante para la toma de decisiones.

Security Control Frameworks

- Existen varios marcos de referencia, uno de los más conocido es *Control Objetives for Información and Related Technology* (**COBIT**), desarrollado *por Information System Audit and Control Association* (ISACA)
- Principios de COBIT:
  - Provide Stakeholder value
  - Holistic Approach
  - Dynamic Gobernance System
  - Governance distinct from Management
  - Tailored to Enterprise Needs
  - End-to-End Governance System

Otras guías disponibles

- NIST 800-53 Rev. 5 https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final Recomendaciones del Gobierno US.
- Center of Internet Security (CIS), provee información sobre configuración segura de OS, aplicaciones, y hardware en https://learn.cisecurity.org/benchmarks
- NIST Risk Management Framework (RMF) https://csrc.nist.gov/projects/risk-management/about-rmf
- NIST Cybersecurity Framwork (CSF) https://www.nist.gov/cyberframework
- Internationa Organization form Standarization (ISO) Familia 27000 https://www.itgovernanceusa.com/iso27000-family
- Information Technology Infraestructure Library (ITIL) https://www.itlibrary.org/

ISO 27002:2013

Norma internacional

Guía de **mejores prácticas** para la gestión de seguridad de la información

Proporciona **directrices y principios generales** para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización

Detalla controles y objetivos de control

ISO 27001:2013

Norma internacional

Establece los criterios para un **Sistema de Gestión de Seguridad** de la Información (SGSI)

Ayuda a las organizaciones a gestionar y proteger su información de manera efectiva

Proporciona un enfoque sistemático para proteger información sensible contra accesos no autorizados

Es certificable!

Políticas de Seguridad

- La **capa más alta de formalización** es la política de seguridad
  - Define **ámbito de seguridad y recursos a ser protegidos**
  - Determina que **tipos de soluciones de seguridad se consideran**
  - Es una **vista general de la seguridad** necesaria para la organización
  - La política define: **objetivos de seguridad estratégicos, visión, metas y alcances, define roles y responsabilidades, especifica requerimientos de auditoría, requerimientos de cumplimento y establece los niveles de riesgo aceptables**.
  - De la política **se derivan otros documentos**: estándares, baselines, guías, procedimientos.

Una Política de Seguridad no se vende ni se compra

- No existen productos que hagan todo.
- Establece lo que se puede hacer y lo que no, de forma escrita y formal.
- Demuestra que la empresa se lo quiere tomar en serio. **Implica un compromiso con los directivos.**
- Útil frente a una auditoria, sobre todo si se siguen las normalizaciones.
- Útil para demostrar casos de intrusiones o delitos contra los sistemas informáticos.
- Facilita el cumplimiento legal.

Objetivos Principales

Proteger la **integridad** de la información.

Garantizar la **confidencialidad**.

Asegurar la **disponibilidad**.

Cumplir con **normativas legales y estándares.**

Security Standards, Baselines, and Guidelines

Standards definen requerimientos a ser cumplidos, ej: homogeidad de hardware y software, tecnología y controles de seguridad.

Baselines define los niveles mínimos de seguridad que cada sistema de la organización debe poseer. Es una versión más operacional del standard., muchas veces hace referencia a estándares gubernamentales o de la industria.

Guidelines, ofrecen guías para la implementación de estándares y baselines, son guías operacionales para profesionales y usuario, pueden ser sugerencias y no necesariamente obligatorias.

Security Procedures

- Elemento final de la formalización de la seguridad también llamados *standard operating procedure* (SOP)
- Son documentos detallados paso paso que describen acciones exactas para implementar mecanismos de seguridad, controles o soluciones.
- Se actualizan regularmente con nuevo software y hardware

Nombre	Código	Descripción	Estado	Vigencia
Documentos Componentes	PSI_DC01	Declaración Oficial de Documentación las Políticas de Seguridad	Esperando Aprobación	Indefinida
Guia Elemental de Elaboración	PSI_GE01	Definición de Metodología, roles y responsabilidades como fases de generación de políticas de seguridad	Revisión	Indefinida
Política de la Seguridad de La Información (Política de Primer Nivel)	PSI_SI01	Definiciones básicas, clasificaciones de información y declaración de riesgo	Declarada	No especificado
Políticas de Seguridad del Personal	PSI_SP01	Normas de actuación como usuarios respecto a buenas prácticas, uso adecuado de recursos y seguridad de información	Declarada	No especificado
Política de Administración de Sistemas	PSI_SE_AS01	Normas y procedimientos de buenas prácticas en administración de sistemas.	Declarada	No especificado
Política de Redes	PSI_SE_PR01	Procedimientos de gestión, uso y coordinación con empresas externas	Declarada	No especificado
Estándares de Desarrollo de Software Departamental	PSI_PD01	Declaración de plataforma departamental, arquitectura de servicios y restricciones de desarrollo	Revisión	Indefinida
Plan General de Continuidad Operativa	PSI_CN01	Procedimientos para garantizar operatividad administrativa en caso de incidentes mayores	Declarada	No especificado
Declaración de faltas a las políticas de seguridad y sanciones asociadas	PSI_SA01	Definiciones basadas en estatuto administrativo y potestades departamentales	Declarada	No especificado
Control de Acceso Físico a Laboratorios y NOC Departamental	PSI_SE_AS01_01	Procedimientos de Implantación Rápida, de uso temporal	Aplicada	Temporal

Componentes de la Política

- Alcance y Aplicabilidad.
- Roles y Responsabilidades.
- Medidas de Seguridad.
- Protocolos de Respuesta a Incidentes.

Objetivos de Seguridad de Empresa Minera X

- Brindar protección a las operaciones de la organización mediante la gestión segura de:
  - Información, Redes de datos, Sistemas de procesamiento de información
  - Instalaciones de la empresa, Equipos, Servicios provistos, Software
  - Personal
- Buscando garantizar:
  - Continuidad operativa, minimizar daños ante incidentes, maximizar retorno de inversiones y desarrollar oportunidades sustentadas en tecnología.

Objetivos de Política de Minera X

- Definir Seguridad de la Información para la empresa
- Formalizar el compromiso directivo en el tiempo de forma progresiva
- Apoyar el proceso en las mejores prácticas internacionales
  - ISO (27001:2013, 27002:2013)
- Establecer cimientos para el soporte:
  - Cumplimientos organizacionales, nacionales e internacionales
  - Comunicación, Capacitación, entrenamiento
  - Continuidad del negocio
  - Orgánica adecuada