Seguridad de la Información

Introducción a la gestión de la seguridad

Federico Pacheco

 @FedeQuark

 www.federicopacheco.com.ar

 info@federicopacheco.com.ar

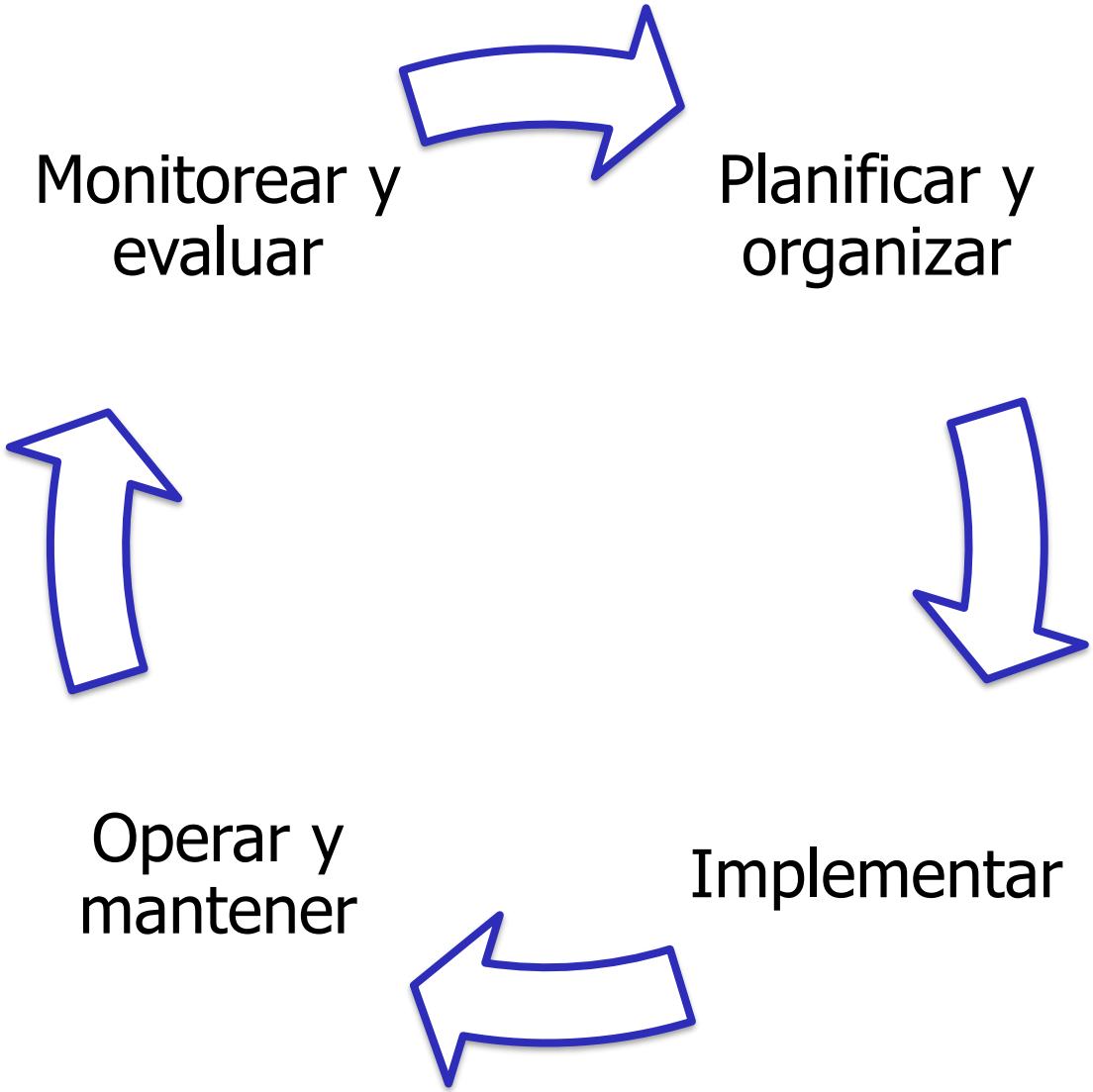
Contenidos

- Necesidad de gestión de la seguridad
- Estructura normativa
- Implementación de un sistemas de gestión de la seguridad (SGSI)
- Gestión del riesgo
- Gestión de cambios y actividades
- Gestión de incidentes
- Concientización de usuarios
- Clasificación de la información

Gestión de la seguridad

- Objetivo principal
  - Proteger los activos de información de la organización
- Necesidad fundamental
  - Alineación con el negocio
- Características
  - Proceso continuo y cíclico
  - No hay soluciones únicas ni infalibles
  - Incumbencia de la alta gerencia (Top-Down)
  - Requiere establecer un sistema de gestión (SGSI)
  - Relacionado con el gobierno de la seguridad (Security Governance)

Proceso continuo (PDCA)

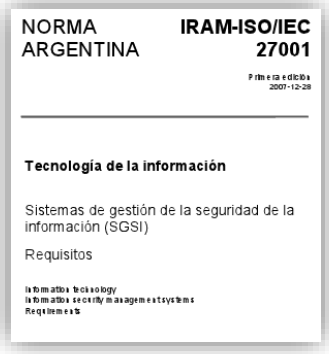


Normativas

- Definen y clasifican las metas y objetivos
- Definen roles, responsabilidades y escala de autoridad
- Establecen criterios aceptables y uniformes de conducta
- Garantizar el cumplimiento de normas externas
- Definen acciones informativas
  - Informan al personal sus obligaciones y medidas por incumplimiento
  - Informan a terceros sobre las definiciones establecidas por la organización

Estándares de SGSI

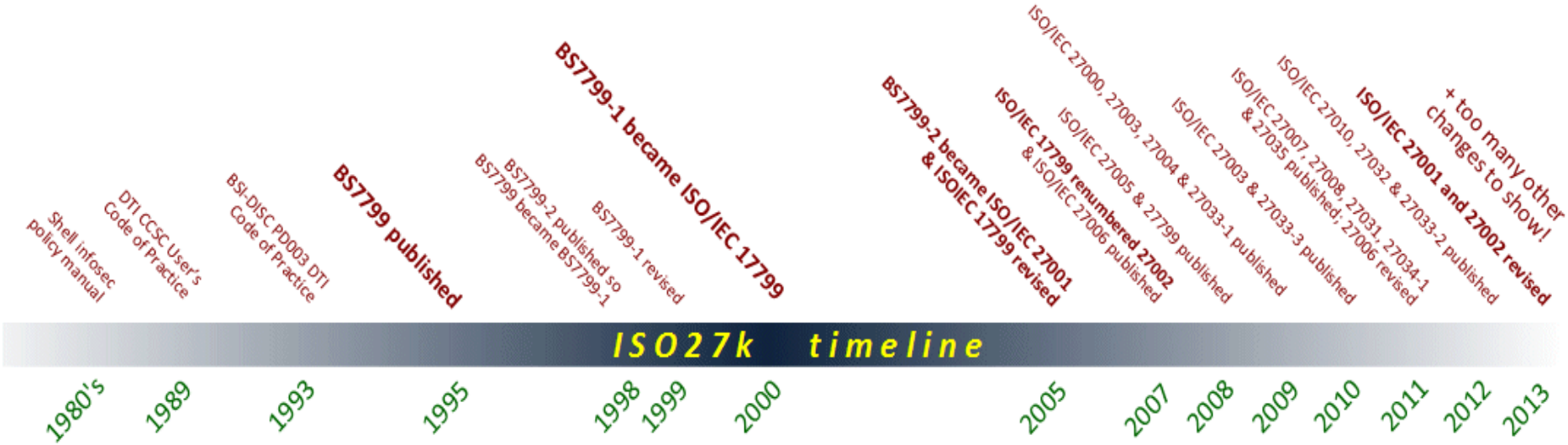
- ISO 27000
  - Familia de estándares de seguridad de la información basado en BS7799
  - Ejemplos
    - 27.001: Requisitos de los SGSI ← Certificable
    - 27.002: Objetivos de control y controles recomendables
    - 27.003: Guía de implementación del SGSI
    - 27.005: Gestión de riesgos


NORMA ARGENTINA
IRAM-ISO/IEC 27001
Primera edición
2007-12-28
Tecnología de la información
Sistemas de gestión de la seguridad de la información (SGSI)
Requisitos
Information technology
Information security management systems
Requirements

- COBIT (Control Objetives for Information and related Technologies)
  - Utilizado para implementar Gobierno de TI
  - Desarrollado por
    - ISACA – Information Systems Audit and Control Association
    - ITGI – IT Governance Institute

- Otros
  - SOGP (Standard of Good Practice for Information Security)
  - ISM3 (Information Security Management Maturity Model)

Timeline ISO 27.000



Estructura ISO 27002

- Evaluación y tratamiento de riesgos
- Política de Seguridad
- Organización de seguridad
- Gestión de Activos
- Gestión de Recursos Humanos
- Seguridad Física y Ambiental
- Gestión de Operaciones y Comunicaciones
- Control de accesos
- Adquisición, desarrollo y mantenimiento de sistemas
- Gestión de incidentes de seguridad
- Administración de la continuidad del negocio
- Cumplimiento de normativa y leyes

Gestión de riesgos

- Objetivo
  - Reducirlos hasta un nivel tolerable

- Requerimientos de su gestión
  - Dimensionamiento y alcance
  - Establecer políticas
  - Armar equipo
  - Definir metodologías y herramientas
  - Identificar y medir riesgos

- Tratamiento
  - Medidas de control
  - Transferencia
  - Aceptación
  - Eliminación del factor

Política de Seguridad

- Qué es
  - Declaración de directivas de alta gerencia sobre el compromiso con la seguridad
- Objetivo
  - Garantizar apoyo y proveer dirección de acuerdo al negocio y normativas
- Características
  - Breve y general
  - Dictada por comité de seguridad y aprobada por autoridades
  - Define el desarrollo del programa de gestión de seguridad
  - Comunicada y aceptada por todo el personal
  - Alineada con normativas legales y corporativas
  - Representada por un documento declarativo
  - Es parte de la estructura de políticas de la organización
  - Revisión con un frecuencia tal que garantice su validez

Política de Seguridad – Contenidos

- Definiciones de seguridad, objetivos y alcances, su importancia y aplicación
- Propósito de su existencia en relación a los principios de la seguridad
- Marco de establecimiento de objetivos de control y evaluación
- Definición de responsabilidades en la gestión de la seguridad
- Referencias a documentación de respaldo o ampliación
- Explicación de los principios y requerimientos a cumplir
  - Legales, regulatorios y contractuales
  - Educación, capacitación y concientización
  - Gestión de la continuidad del negocio
  - Consecuencias de su incumplimiento

Estructura normativa

← Nivel estratégico

← Nivel táctico

← Nivel táctico

← Nivel operativo

Estructura normativa

Estándares	• Especifican el uso uniforme de una tecnología
Normas	• Recomendaciones generales según objetivos
Baselines	• Parámetros mínimos para un estándar
Guidelines	• Recomendaciones y sugerencias
Procedimientos	• Descripción detallada de tareas

Organización de la seguridad

- Organización interna
  - Compromiso gerencial
  - Coordinación
  - Asignación de responsabilidades
  - Autorización para procesamiento de información
  - Acuerdos de confidencialidad
  - Contacto con autoridades y grupos de interés
  - Revisión independiente
- Terceras partes
  - Riesgos relacionados con terceros
  - Tratamiento con clientes
  - Acuerdos con terceros

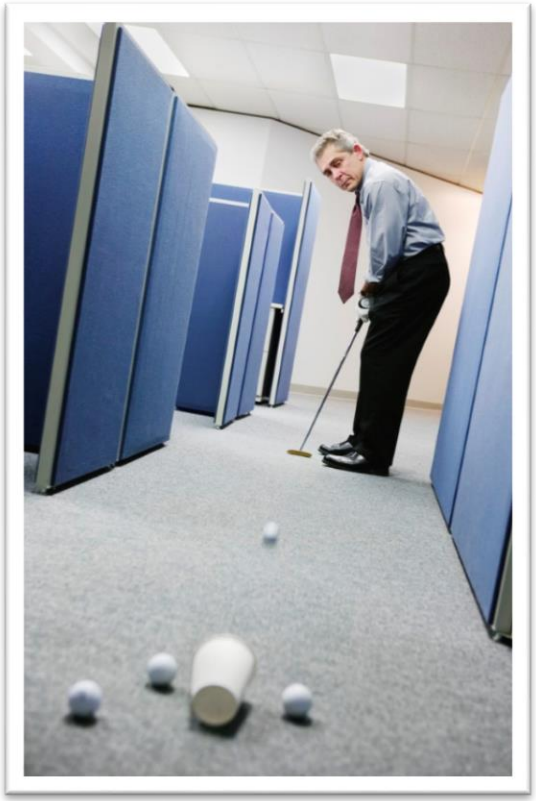
Recomendaciones de gestión

- Establecer fuente de asesoramiento interna y externa
- Promover un enfoque multidisciplinario
- Realizar revisiones de todo proceso y documento
- Documentar todo proceso y procedimiento
- Incluir revisiones independientes de seguridad

Compromiso gerencial

- Problemas de la alta gerencia
  - Falta de entendimiento sobre la necesidad de seguridad
  - Idea de la seguridad como problemática, costosa e innecesaria
  - Incapacidad de identificar los riesgos asociados
  - Creer que se interferirá con el negocio
  - Creer que la seguridad es un tema de tecnología

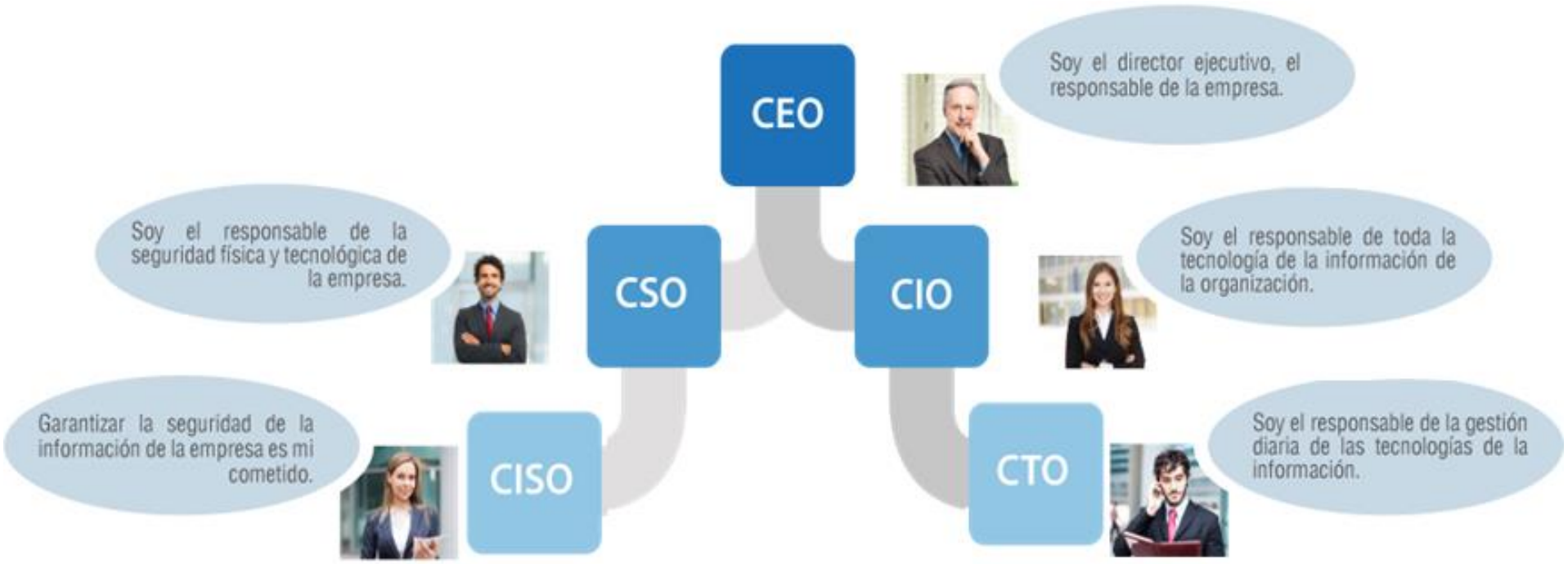
- Recomendaciones para comunicación con alta gerencia
  - Utilizar canales adecuados de comunicación
  - Aprovechar a las personas con mayor llegada
  - Hablarles en términos de riesgos y negocios



Coordinación y responsabilidad

- Máxima autoridad: Comité de seguridad
- Responsable funcional
  - CISO, ISSO, Gerente
- Objetivos
  - Establecer y mantener un SGSI
  - Comunicarse con la alta dirección
  - Conocer el negocio y los procesos

El C-Level



Dependencia del área

- Gerencia de Sistemas
- Auditoría Interna
- Area de Seguridad Informática
- Gerencia de Seguridad
- Consultoría Externa
- Recursos Humanos

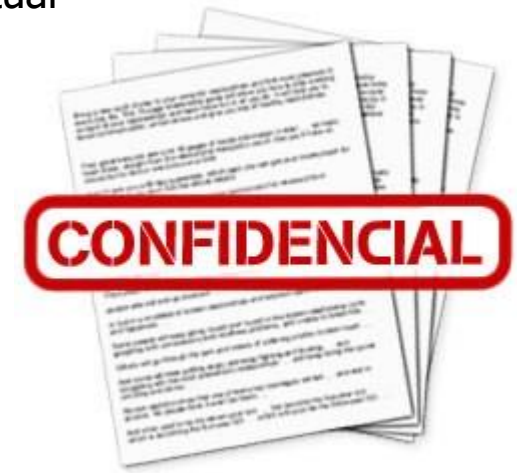
Funciones relacionadas

- Gerente o Director General
- Comité de Seguridad
- Responsable de Seguridad
- Analista de Seguridad
- Administrador de Seguridad
- Auditor de seguridad

Acuerdos de confidencialidad

- Documento que refleja las necesidades de protección de la información

- Características
  - Utilizan terminología legal
  - Consideraciones legales y regulatorias
  - Incluyen definición de información confidencial
  - Indican duración del compromiso y acciones finales
  - Responsabilidades y acciones sobre la información
  - Aclaraciones sobre secretos comerciales y propiedad intelectual
  - Usos permitidos y derechos
  - Derecho para auditar y supervisar
  - Procesos de notificación e informes ante incumplimiento
  - Términos de devolución o destrucción
  - Acciones ante incumplimiento
  - Existencia en distintas formas



Contacto con autoridades

- Definición de autoridades y formas de contacto
  - Autoridades jerárquicas, legales, policiales, servicios públicos, etc.

- Características
  - Soportan la gestión de incidentes y continuidad del negocio
  - Detallan condiciones que lo ameritan
  - Pueden incluir grupos de interés especial

Terceras partes

- Identificación y análisis de riesgos relacionados con terceros
- Mantener la seguridad de lo que es accedido, procesado o gestionado por terceros
- Evaluar riesgos asociados a la provisión o recepción de un servicio
- Determinar requerimientos de control
- Establecer acuerdos (pueden ser impuesto por la contraparte)
- Considerar seguridad respecto a clientes

Subsistemas de gestión

Activos	RRHH	Entorno físico	Comunicaciones
Operaciones	Control de accesos	Incidentes	Continuidad del negocio
	Cumplimiento	Sistemas de información	

Gestión de activos

- Tipos de activos: documentos, software, físicos, servicios, personas, intangibles
- Incluye responsabilidad por los activos
- Procesos necesarios
  - Identificación
    - Inventario y propietarios
  - Valuación
    - Subjetiva y objetiva
  - Clasificación
    - Tratamiento según nivel

Gestión de RRHH

- Incluye distintos procesos
  - Contratación
  - Tiempo de trabajo
  - Desvinculación

- Incluye distintas actividades
  - Rotación de funciones
  - Vacaciones obligatorias
  - Segregación de funciones
  - Background Checks
  - Acuerdos para personal y terceros

Gestión de la seguridad física

- Definición de un plan de seguridad física y ambiental
- Objetivo
  - Impedir accesos físicos no autorizados, daños a instalaciones e información
- Incluye seguridad en el ambiente y en el equipamiento
  - Enfoque especial en el datacenter
- Protección proporcional a los riesgos identificados

Gestión de las comunicaciones y operaciones

- Objetivo
  - Garantizar el funcionamiento de las instalaciones de procesamiento de información

- Incluye
  - Gestión de procedimientos operativos
  - Gestión de la provisión de servicios de 3ros
  - Planificación de sistemas y gestión de la capacidad
  - Protección contra código malicioso
  - Sistemas de backup
  - Seguridad de las redes
  - Manejo de medios de almacenamiento
  - Intercambio de la información
  - Servicios de comercio electrónico
  - Seguimiento y control

Gestión de los sistemas de control de accesos

- Definición de requerimientos
- Gestión de accesos de usuarios
- Responsabilidades del usuario
- Dispositivos móviles y trabajo remoto
- Acceso sistemas
  - Red
  - Sistema operativo
  - Aplicaciones
  - Información

Gestión de sistemas de información

- Incluye adquisición, desarrollo y mantenimiento

- Abarca distintos aspectos
  - Requerimientos de seguridad
  - Procesamiento adecuado
  - Controles criptográficos
  - Seguridad de los archivos de sistema
  - Seguridad en los procesos de desarrollo y soporte
  - Gestión de vulnerabilidades técnicas

Gestión de incidentes

- Informe de los eventos y fallas de seguridad
  - Es necesaria la determinación de "incidente de seguridad"
  - Los incidentes son inevitables

- Abarca distintos aspectos
  - Responsabilidades y procedimientos
  - Aprendizaje a partir de los incidentes
  - Recolección de evidencia

- Capacidad de respuesta
  - Equipo de respuesta a incidentes de seguridad (CSIRT)

Gestión de la continuidad del negocio

- Objetivo
  - Inclusión de la seguridad de la información la gestión de la continuidad del negocio

- Incluye
  - Evaluación de los riesgos
  - Elaboración e implementación de planes de continuidad
  - Marco para la planificación de la continuidad
  - Pruebas, mantenimiento y reevaluación de planes

Gestión del cumplimiento

- Objetivo
  - Poder operar bajo las condiciones establecidas interna y externamente

- Incluye el cumplimiento en diversos campos
  - Requerimientos legales
  - Políticas de seguridad
  - Normativas propias de la industria
  - Normas internacionales
  - Estándares y requerimiento técnicos
  - Auditorías de sistemas y seguridad

Gestión de la seguridad – Aspectos legales

Due Diligence (Debida Diligencia)

- Responsabilidad de entender las amenazas y los riesgos

Due Care (Debido Cuidado)

- Implementar contramedidas para protegerse de los riesgos

Si una organización no cumple con esto en relación a la protección de sus activos puede ser acusada de negligencia

Familia ISO 27.000 (I)

- ISO 27.003
  - Aspectos críticos para el diseño e implementación de un SGSI.
- ISO 27.004
  - Guía para el desarrollo y uso de métricas para determinar la eficacia de un SGSI.
- ISO 27.005
  - Directrices para la gestión del riesgo en la seguridad de la información.
- ISO 27.006
  - Requisitos para la acreditación de entidades de auditoría y certificación de SGSI.
- ISO 27.007
  - Guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19.011.

Familia ISO 27.000 (II)

- ISO 27.008
  - Guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.
- ISO 27.009
  - Guía de uso y aplicación de ISO 27.001 para sectores específicos.
- ISO 27.010
  - Guía para la gestión de seguridad cuando se comparte información entre organizaciones.
- ISO 27.011
  - Guía de implementación de SGSI para organizaciones del sector de telecomunicaciones.
- ISO 27.013
  - Guía de implementación integrada de ISO 27001 e ISO 20.000 (gestión de servicios TI).

Familia ISO 27.000 (III)

- ISO 27.014
  - Guía de gobierno corporativo de la seguridad de la información.
- ISO 27.015
  - Guía de SGSI orientada a organizaciones del sector financiero y de seguros.
- ISO 27.016
  - Guía de valoración de los aspectos financieros de la seguridad de la información.
- ISO 27.017
  - Guía de seguridad para Cloud Computing (ISO 27.002 + controles adicionales)
- ISO 27.018
  - Buenas prácticas en controles de protección de datos para servicios de cloud computing.

Familia ISO 27.000 (IV)

- ISO 27.019
  - Guía de SGSI para sistemas relacionados con el sector de la industria de la energía.
- ISO 27.023
  - Guía de correspondencias entre versiones 2005 y 2013 de ISO 27001/2.
- ISO 27.031
  - Guía de apoyo para adecuación de TICs para la continuidad del negocio.
- ISO 27.032
  - Guía para seguridad cibernética y protección de infraestructuras críticas.

ISO 27.033: Seguridad en redes

- 27033-1: conceptos generales
- 27033-2: directrices de diseño e implementación de seguridad en redes
- 27033-3: escenarios de referencia de redes
- 27033-4: comunicaciones entre redes mediante gateways de seguridad
- 27033-5: aseguramiento de comunicaciones mediante VPNs
- 27033-6: convergencia IP
- 27033-7: redes inalámbricas

ISO 27.034: Seguridad en aplicaciones

- 27034-1: conceptos generales
- 27034-2: marco normativo de la organización
- 27034-3: proceso de gestión de seguridad en aplicaciones
- 27034-4: validación de la seguridad en aplicaciones
- 27034-5: estructura de datos y protocolos y controles de seguridad de aplicaciones
- 27034-6: guía de seguridad para aplicaciones de uso específico

Familia ISO 27.000 (V)

- ISO 27.035
  - Guía sobre la gestión de incidentes de seguridad en la información.
- ISO 27.036
  - Guía de seguridad en las relaciones con proveedores.
  - 4 secciones
    - 27036-1: visión general y conceptos
    - 27036-2: requisitos comunes
    - 27036-3: seguridad en la cadena de suministro TIC
    - 27036-4: seguridad en entornos de servicios Cloud
- ISO 27.037
  - Guía de directrices para actividades relacionadas con la evidencia digital.

Familia ISO 27.000 (VI)

- ISO 27.038
  - Guía de especificación para seguridad en la redacción digital.
- ISO 27.039
  - Guía para selección, despliege y operación de IDS/IPS.
- ISO 27.040
  - Guía para la seguridad en medios de almacenamiento.
- ISO 27.041
  - Guía para la garantizar la idoneidad y adecuación de los métodos de investigación.

Familia ISO 27.000 (VII)

- ISO 27.042
  - Guía con directrices para el análisis e interpretación de las evidencias digitales.
- ISO 27.043
  - Principios y procesos de investigación de incidentes.
- ISO 27.044
  - Gestión de eventos y de la seguridad de la información.
- ISO 27.050
  - Tratamiento de la información almacenada en medios electrónicos.
- ISO 27.799
  - Directrices para el sector sanitario y de datos de salud de pacientes.

¿Preguntas?

Federico Pacheco

 @FedeQuark

 www.federicopacheco.com.ar

 info@federicopacheco.com.ar