Norma ISO 27001:2013 para la validación de la seguridad informática

Nombre del Ponente: Pablo Corona Fraga

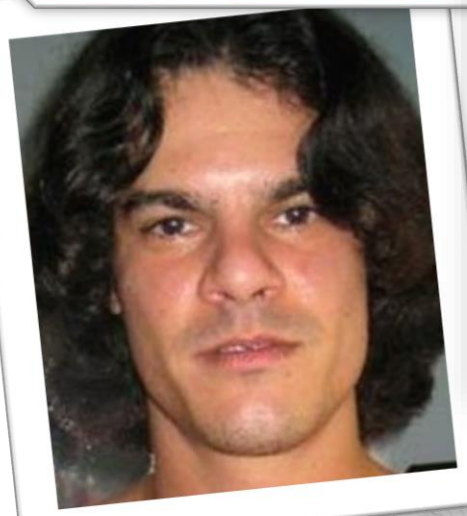
Robo físico

Robo digital

US largest card incident hacker has track record says Miami Herald

21 August 2009

As the fall-out in the Albert Gonzalez credit card hacking case - in which the card hacker was charged earlier this week with gaining unauthorized access to 130 million people's card details from major merchants - continues, the Miami Herald

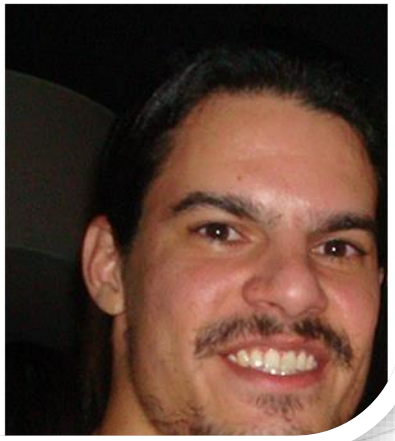


posts tagged 'Albert Gonzalez'

In Surprise Appeal, TJX Hacker Claims U.S. Authorized His Crimes

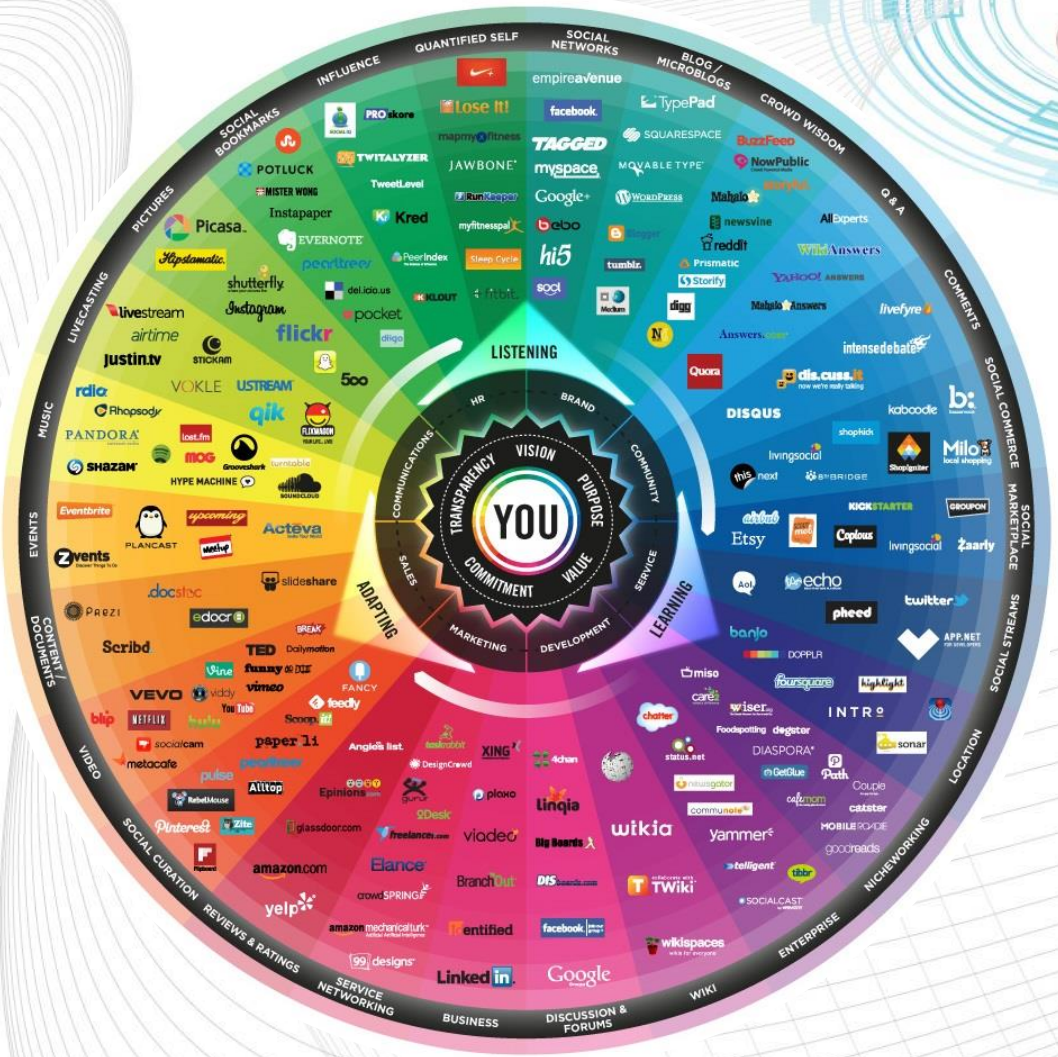
By Kim Zetter ✉ April 7, 2011 | 4:07 pm | Categories: Breaches, Hacks and Cracks, The Courts

Albert Gonzalez, the hacker who masterminded the largest credit card heists in U.S. history, is asking a federal judge to throw out his earlier guilty pleas and lift his record-breaking 20-year prison sentence, on allegations that the government authorized his years-long crime spree.



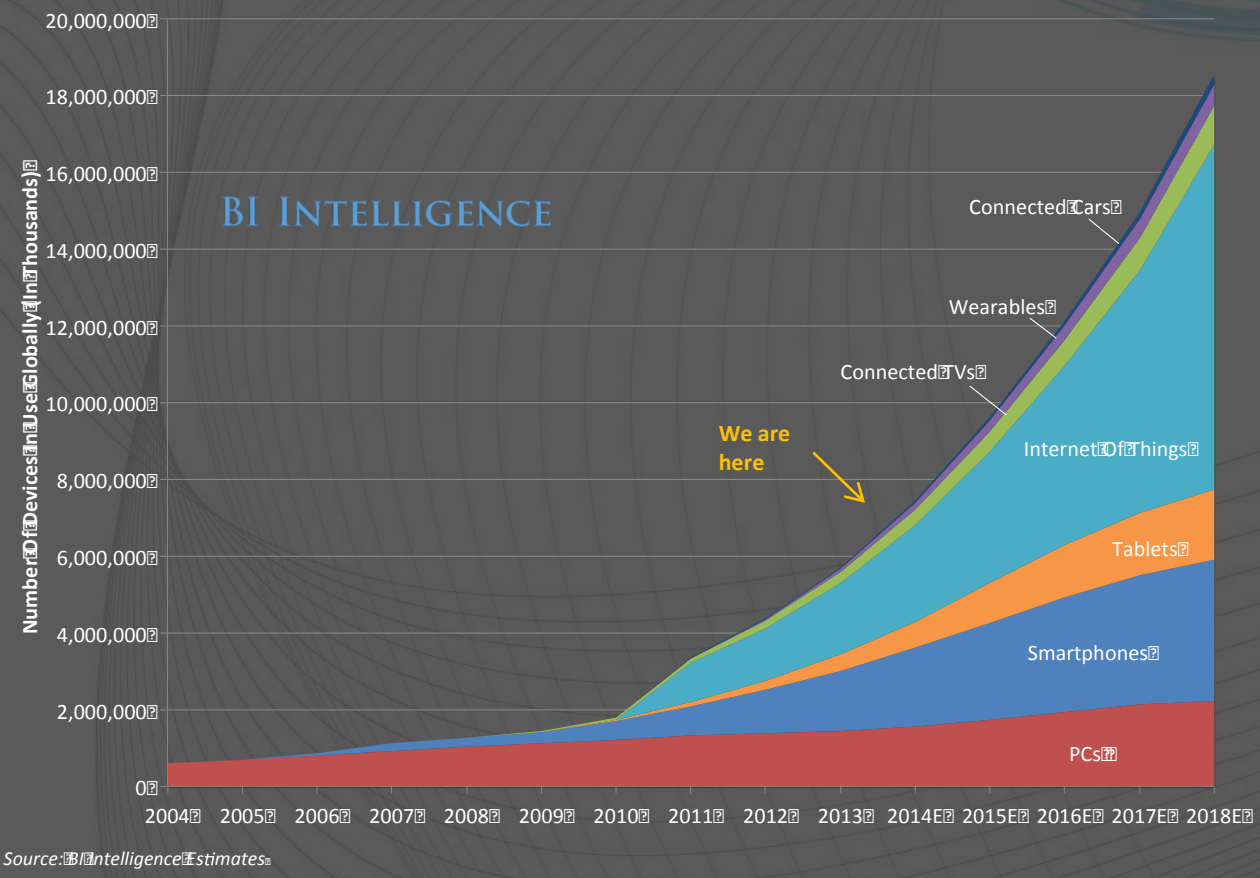
Gonzalez, 29, admitted last year that he and accomplices hacked into TJX, Office Max, Dave & Busters, Heartland Payment Systems and other companies to steal more than 130 million credit and debit card numbers, in what the government deemed the biggest computer crime case ever prosecuted in the United States. He's currently serving time at the Milan low-security federal prison in southeastern Michigan, with a release date in the year 2025.

ema®
entidad mexicana
de acreditación a.c.



2do. Congreso Internacional para la Acreditación en el Sector Salud

Everything!



Source: BI Intelligence Estimates

ema®
entidad mexicana
de acreditación a.c.

Cloud

entidad mexicana de acreditación a.c.

¿En quién confiamos?

¿Qué quieren?

La pregunta no es si habrá un ciberincidente, Sino cuándo y qué impacto tendrá

¿Qué saben hacer?

Seguridad de la información

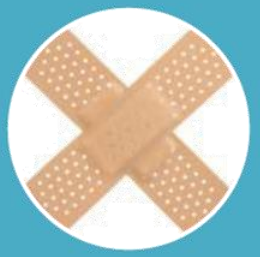
3 tipos de riesgos

Intencional

Anonimicidad

Oportunista

Complejidad



Accidental

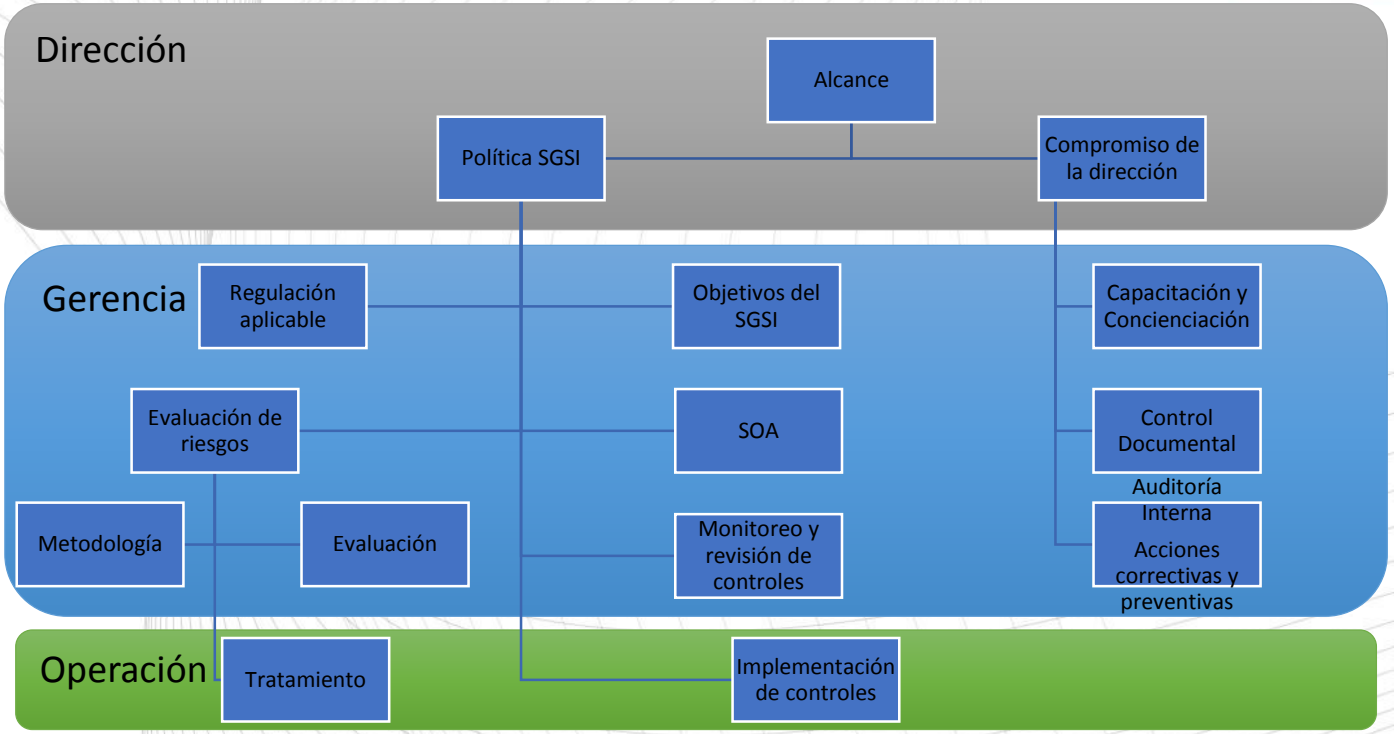
RIESGO

Serie ISO 27000

La familia 27000 cuenta con muchas norma, entre ellas:

- ISO/IEC 27000 Vocabulario e introducción
- **ISO/IEC 27001 Especificación**
- **ISO/IEC 27002 Guía de Controles**
- ISO/IEC 27003 Guía de Implementación
- ISO/IEC 27004 Métricas
- ISO/IEC 27005 Gestión de Riesgos
- ISO/IEC 27006 Guía de certificación para SGSI
- **ISO/IEC 27008 Lineamientos para evaluación de controles**
- ISO/IEC 27011 ISO27k para telecoms
- ISO/IEC 27017 ISO27k para cómputo en la nube
- ISO/IEC 27018 ISO27k PDP para proveedores de nube
- ISO 27799 ISO27k para sector salud

Sistema de Gestión de Seguridad de la Información




Indicadores de desempeño
Leyes
Regulaciones
Estandares
Autoridades
Intereses Generales
Beneficios comunes
Intereses políticos
Contratos
SLA
NDA
Clientes
Cumplimiento del contrato
Seguridad / Confidenciaidad
Propiedad intelectual
Objetivos Estrategicos
Presupuesto
Socios / Inversionistas
Ingresos / Ganancias / ROI
Reputación
Sanciones/ Multas/ Penas
Objetivos de Negocio
Políticas
Dirección / C-Level
Ingresos / Ganancias
Bonos / Opciones
Uso de recursos y optimización
Empleo
Objetivos de Operación
Procesos
Procedimientos
Administración
Bonos
Promociones
Salario
Actividades diarias
Indicadores de operación
Operación
Promociones
Crecimiento personal/ Reconocimiento
Salario
Objetivos

Política de seguridad de la información

Protegemos la integridad, confidencialidad y disponibilidad de la información que manejamos y los activos relacionados.

CIO

Información Documentada

La documentación debe:

Ser solo la que necesaria

La que será leida

La que será seguida

Cuidar que la documentación no sea solo para la auditoría

¿el eslabón más débil?

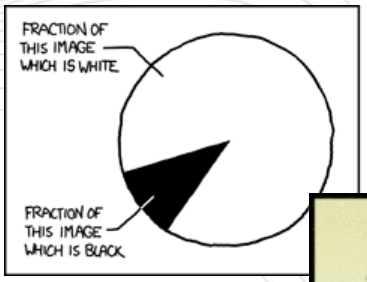
Lenguaje adecuado

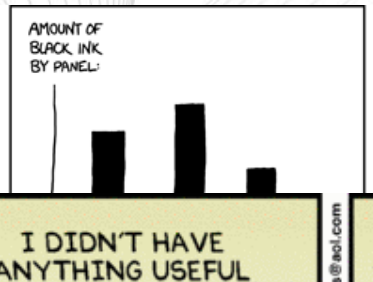
Monitoreo

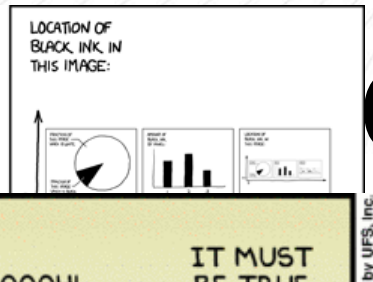
Análisis

Automatización

entidad mexicana de acreditación a.c.



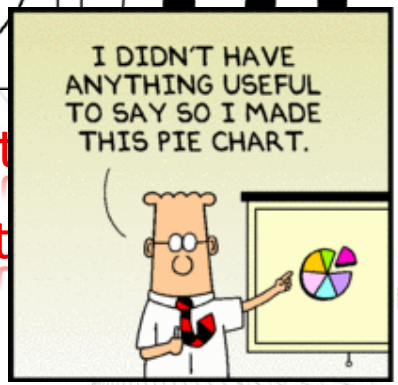


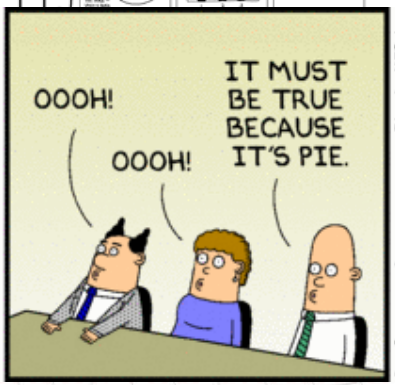


d

Número de t

Cant





Bitácoras llenas

Equipos con antivirus

Monitoreo

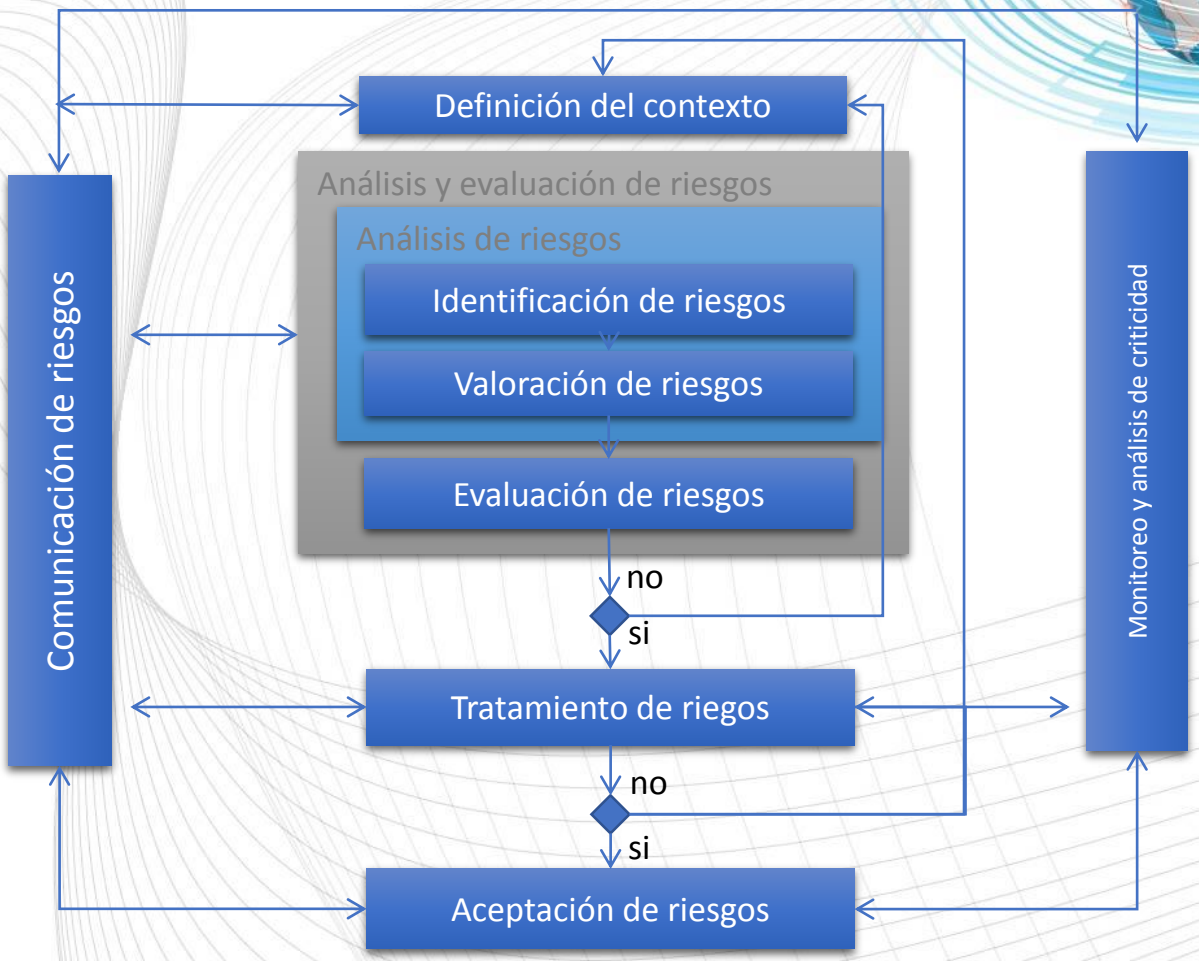
- Establecer Entradas y salidas
- Establecer métricas
- Establecer mecanismos de medición
- Establecer KPI’s
- Establecer metas con respecto a KPI´s


Indicadores de desempeño
Cumplimiento de leyes, Declaraciones de impuestos, ...
Ahorro, beneficios, calidad, tiempos de respuesta, riesgos de negocio, ...
Retorno de inversión, EBITDA, P&L, Multas Sanciones, ...
COBIT, TOGAF, BSC, Eficiencia, ...
ITIL, ISO/IEC 20000-1, ISO/IEC 27001, ...
Actividades diarias, beneficios, metas, hitos, milestones, ...
Objetivos

Puntos clave

- Concienciación del empleado en materia de seguridad.
- Realización de comités a distintos niveles (operativos, de dirección, etc.) con gestión continua de no conformidades, incidentes de seguridad, acciones de mejora, tratamiento de riesgos.
- Creación de un sistema de gestión de incidentes que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).
- La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.
- La seguridad no es un producto, es un proceso.
- La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.
- La seguridad debe ser inherente a los procesos de información y del negocio.

Análisis de riesgos



Controles Administrativos, Físicos y Tecnológicos

entidad mexicana de acreditación a.c.

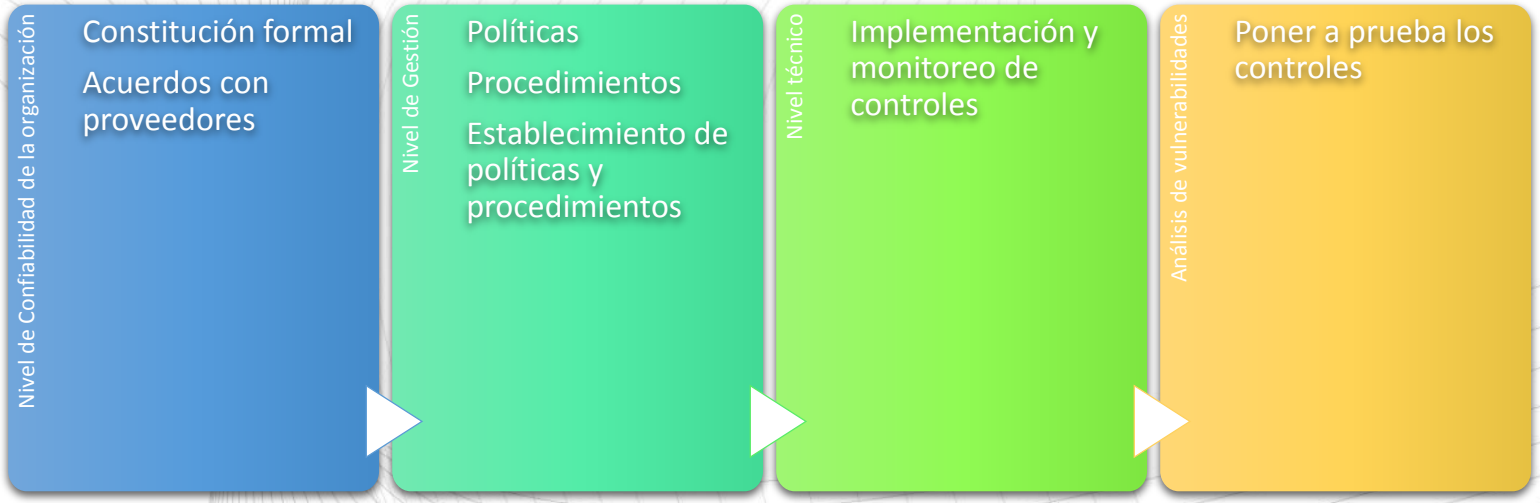
A.5 Políticas de seguridad de la información
A.5.1 Gestión de la dirección para la seguridad de la información
A.5.1.1 Políticas de seguridad de la información
A.5.1.2 Revisión de las políticas de seguridad de la información
A.6 Organización de la seguridad de la información
A.6.1 Organización interna
A.6.1.1 Roles y responsabilidades de seguridad de la información
A.6.1.2 Segregación de tareas
A.6.1.3 Contacto con autoridades
A.6.1.4 Contacto con grupos de especial interés
A.6.1.5 Seguridad de la información en la administración de proyectos
A.6.2 Los dispositivos móviles y teletrabajo
A.6.2.1 Política de dispositivos móvil
A.6.2.2 El teletrabajo
A.7 Seguridad ligada a los recursos humanos
A.7.1 Previo al empleo
A.7.1.1 Investigación
A.7.1.2 Términos y Condiciones de empleo
A.7.2 Durante el empleo
A.7.2.1 Responsabilidades de la Dirección
A.7.2.2 Concientización, educación y capacitación en seguridad de la información
A.7.2.3 Proceso disciplinario
A.7.3 Terminación o cambio de empleo
A.7.3.1 Responsabilidades en la terminación o cambio de empleo

A.8 Gestión de activos
A.8.1 Responsabilidad sobre los activos
A.8.1.1 Inventario de los activos
A.8.1.2 Propiedad de los activos
A.8.1.3 Uso aceptable de los activos
A.8.1.4 Devolución de los activos
A.8.2 Clasificación de la información
A.8.2.1 Clasificación de la Información
A.8.2.2 Etiquetado de la información
A.8.2.3 Manejo de los activos
A.8.3 Manejo de medios
A.8.3.1 Gestión de medios removibles
A.8.3.2 Disposición medios
A.8.3.3 Transferencia de medios físicos
A.9 Control de acceso
A.9.1 Requisitos del negocio para el control de acceso
A.9.1.1 Política de control de acceso
A.9.1.2 Acceso a las redes y servicios de la red
A.9.2 Gestión de acceso de usuarios
A.9.2.1 Registro y cancelación de usuarios
A.9.2.2 Provisión de acceso de usuarios
A.9.2.3 Gestión de derechos de acceso privilegiado
A.9.2.4 Gestión de la información secreta de autenticación de los usuarios
A.9.2.5 Revisión de los derechos de acceso de usuario
A.9.2.6 Eliminación o ajuste de los derechos de acceso
A.9.3 Responsabilidades del usuario
A.9.3.1 Uso de información secreta de autenticación
A. 9.4 Control de acceso a sistemas y aplicaciones
A.9.4.1 Restricción de acceso a la información
A.9.4.2 Procedimientos de inicio de sesión seguros
A.9.4.3 Sistema de administración de contraseñas
A.9.4.4. Uso de privilegios de los programas de utilidades
A.9.4.5 Control de acceso a código fuente del programa.

A.10 Criptografía
A.10.1 Controles criptográficos
A.10.1.1 Política sobre el uso de controles criptográficos
A.10.1.2 Gestión de llaves
A.11 Seguridad física y ambiental
A.11.1 Áreas seguras
A.11.1.1 Perímetro de seguridad física
A.11.1.2 Controles físicos de entrada
A.11.1.3 Aseguramiento de oficinas, salas e instalaciones
A.11.1.4 Protección contra amenazas externas y ambientales
A.11.1.5 Trabajo en áreas seguras
A.11.1.6 áreas de entrega y carga
A.11.2 Equipo
A.11.2.1 Ubicación y protección de equipo Control
A.11.2.2 Servicios públicos
A.11.2.3 Seguridad del cableado
A.11.2.4 Mantenimiento de equipos
A.11.2.5 Retiro de activos
A.11.2.6 Seguridad de los equipos y activos fuera de las instalaciones
A.11.2.7 Disposición o reutilización segura del equipo
A.11.2.8 Equipo de usuario desatendido
A.11.2.9 Política de pantalla y escritorio limpio
A.12 Seguridad de las operaciones
A.12.1 Procedimientos y responsabilidades operativas
A.12.1.1 Procedimientos operativos documentados
A.12.1.2 Gestión de cambios
A.12.1.3 Gestión de capacidad
A.12.1.4 Separación de entornos de desarrollo, pruebas y operación
A12.2 Protección contra malware
A.12.2.1 Controles contra el malware
A.12.3 Respaldos
A.12.3.1 Respaldo de la información
A.12.4 Registro y monitoreo
A.12.4.1 Registro de eventos
A.12.4.2 Protección de la información del registro
A.12.4.3 Registros del administrador y operador
A.12.4.4 Sincronización del reloj
A.12.5 Control del software operacional
A.12.5.1 Instalación de software en sistemas operacionales
A.12.6 Gestión de Vulnerabilidades Técnicas
A.12.6.1 Gestión de las vulnerabilidades técnicas
A.12.6.2 Restricciones en la instalación de software
A.12.7 Consideraciones de auditoría a sistemas de información
A.12.7.1 Controles de auditoria a los sistemas de información
A.13 Seguridad en las comunicaciones
A.13 1 Gestión de la seguridad en la red
A.13.1.1 Controles de red
A.13.1.2 Seguridad en los servicios de red
A.13.1.3 Segregación en redes
A.13.2 Transferencia de información
A.13.2.1 Políticas y procedimientos de transferencia de información
A.13.2.2 Acuerdos de transferencia de información
A.13.2.3 Mensajería electrónica
A.13.2.4 Acuerdos de confidencialidad o no divulgación

A.14 Adquisición, desarrollo y mantenimiento de sistemas
A.14.1 Requisitos de seguridad para los sistemas de información
A.14.1.1 Análisis y especificación de requisitos de seguridad
A.14.1.2 Servicios de aplicaciones seguras en redes públicas
A.14.1.3 Protección de aplicaciones de servicios de transacciones
A.14.2 Seguridad en desarrollo y procesos de soporte
A.14.2.1 Política de desarrollo seguro
A.14.2.2 Procedimientos de control de cambios a sistemas
A.14.2.3 Revisión técnica de aplicaciones después de cambios en la plataforma de operación
A.14.2.4 Restricciones a los cambios en los paquetes de software
A.14.2.5 Principios de ingeniería en sistemas seguros
A.14.2.6. Entorno de desarrollo seguro
A.14.2.7 Desarrollo de sistemas subcontratado (outsourcing)
A.14.2.8 Pruebas de seguridad a los sistemas
A,14.2.9 Pruebas de aceptación a los sistemas
A.14.3 Datos de prueba
A.14.3.1 Protección de datos de prueba
A.15 Relaciones con los proveedores
A.15.1 Seguridad de la información en relación con proveedores
A.15.1.1 Política de seguridad de la información para la relación con proveedores
A.15.1.2 Abordar la seguridad dentro de acuerdos con proveedores
A.15.1.3 Cadena de suministro en Tecnologías de la información y comunicaciones
A.15.2 Gestión de entrega de servicios de proveedores
A.15.2.1 Monitoreo y revisión de los servicios de proveedores
A.15.2.2 Gestión de cambios en los servicios de proveedores
A.16 Gestión de incidentes de seguridad de la información
A.16.1 Gestión de incidentes de seguridad de la información y mejoras
A.16.1.1 Responsabilidades y procedimientos
A.16.1.2 Notificación de los eventos de seguridad de la información
A.16.1.3 Notificación de los puntos débiles de la seguridad
A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información
A.16.1.5 Respuesta a incidentes de seguridad de la información
A.16.1.6 Aprendizaje de los incidentes de seguridad de la información
A.16.1.7 Recopilación de evidencias
A.17 Aspecto de seguridad de la información en la Gestión de la continuidad del negocio
A.17.1 Continuidad de la seguridad de la información
A.17.1.1 Planificación de la continuidad de la información de seguridad
A.17.1.2 Implementación de continuidad de seguridad de la información
A.17.1.3 Verificar, revisar y evaluar la continuidad de seguridad de la información
A.17.2 Redundancias
A.17.2.1 Disponibilidad de instalaciones de procesamiento de información
A.18 Cumplimiento
A.18.1 Cumplimiento con requisitos legales y contractuales
A.18.1.1 Identificación de la legislación aplicable y requisitos contractuales
A.18.1.2 Derechos de propiedad intelectual
A.18.1.3 Protección de registros
A.18.1.4 Protección de datos y privacidad de la información personal
A.18.1.6 Regulación de los controles criptográficos
A.18.2 Revisiones a la seguridad de la información
A.18.2.1 Revisión independiente de la seguridad de la información
A.18.2.2 Cumplimiento de las políticas y normas de seguridad
A.18.2.3 Revisión de cumplimiento técnico

Nivel de profundidad para la evaluación



Los niveles pueden sumar las condiciones de cada uno de los niveles anteriores.

Pruebas de seguridad

Físico	Personas	Sistemas / Redes	Aplicaciones
Acceso a edificios y cerraduras	Ingeniería social	Sistemas operativos	Web (.net, php, xml, http/s)
CCTV y sistemas de identificación	Concientización de seguridad	Bases de datos	Java, C++ y revisión de código
Auditorías fuera de horas de trabajo	Simulaciones de Phishing	Routers, Switches, Firewalls y VPN	Pruebas con y sin credenciales de acceso reales
Intervención de comunicaciones y redes inalámbricas	Redes sociales y políticas de publicación	VoIP / telefonía	Asegurar aplicaciones de terceros
		Equipo portátil /móvil	
		Denegación de Servicio	

entidad mexicana de acreditación a.c.

INTERNATIONAL STANDARD

ISO/IEC 27002

Second edition
2013-10-01

Information technology — Security techniques — Code of practice for information security controls

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information

Reference number
ISO/IEC 27002:2013(E)

TECHNICAL SPECIFICATION

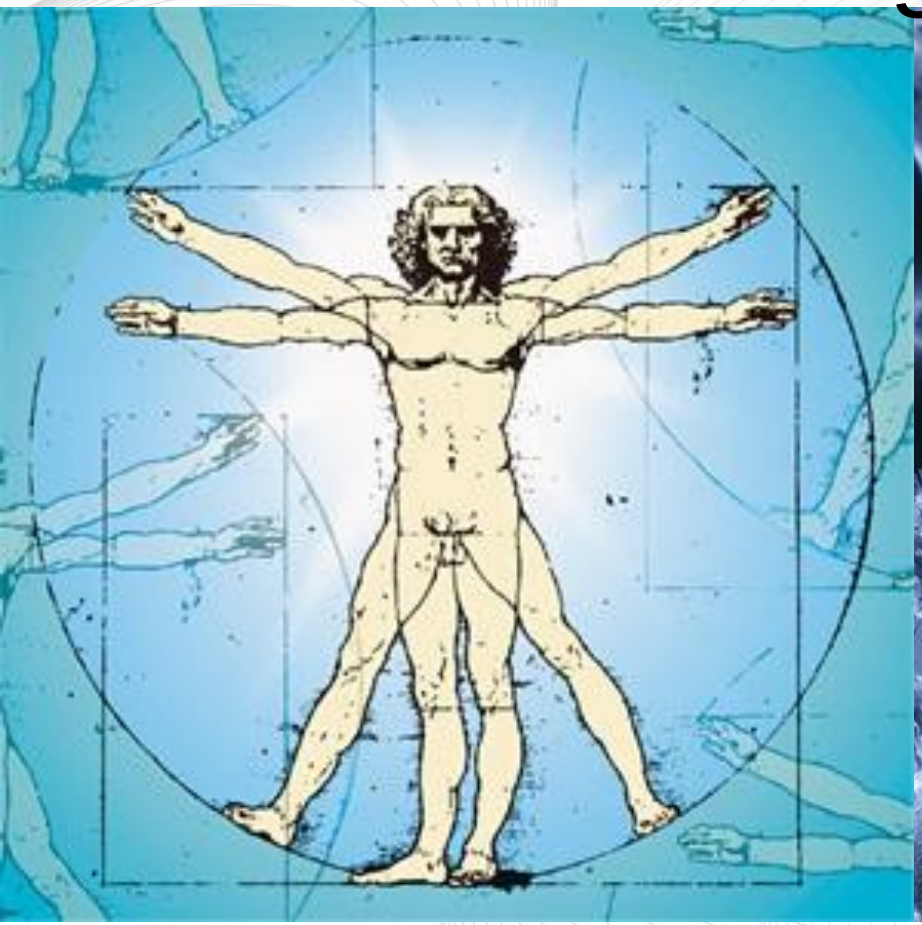
ISO/IEC TS 27008
X (first revision)
2016-05-09

Information technology — Security techniques — Guidelines for the assessment of information security controls

Technologies de l'information — Techniques de sécurité — Lignes directrices pour les auditeurs des contrôles de sécurité de l'information

Reference number
ISO/IEC TR 27008:2011(E)

El cuerpo humano es el sistema más antiguo que hemos asegurado



Comprender los signos vitales y seguir las mejores practicas

entidad mexicana de acreditación a.c.

Introduce solo elementos saludables

Complementar con parches y actualizaciones

El aislamiento de las amenazas externas

Atención a las alertas

Trazabilidad

¿Qué?

¿Quién?

¿Dónde?

GRACIAS

Pablo Corona Fraga

Gerente de Certificación de Sistemas de Gestión de TI
Normalización y Certificación Electrónica S.C.
1204 5191 ext. 427
pcoronaf@nyce.org.mx

Twitter: @pcoronaf