Un Panorama Completo de la Seguridad de Información en el Mundo Digital

Carlos Gonzales Fung

Julio 2017

Presentación del Expositor

CARLOS GONZALES FUNG

- Ingeniero de Sistemas de la FIA – USMP
- Más de 19 años de experiencia en Tecnologías de Información
  - Coordinador de Proyectos en GMD
  - Gestor de Proyectos en Osinergmin
  - Oficial de Seguridad de Información en Osinergmin
  - Director de INTELITECH PERU
- Especialista en Gestión y Planeamiento TIC, Gestión de Proyectos, Seguridad de Información y Continuidad de Negocios
- Certificaciones: PMP, CISSP, CISM, CISA, ITIL-F, TOGAF-F, Cobit-F, Auditor Líder ISO 27001, Implementador Líder ISO 22301, CEH

Agenda

1. La evolución de las TICs
2. Componentes de los TICs y sus riesgos
3. Amenazas a la seguridad de información
4. Especialidades en seguridad
5. Marcos de referencia y organizaciones

1. La evolución de las TICs

¿Cómo llegamos a nuestro mundo digital de

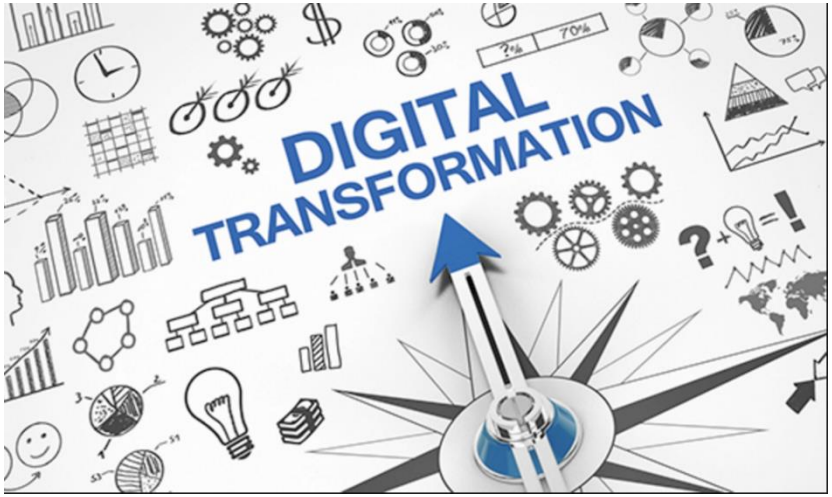
1.1. Incipiente (1960-1980)

- Poco impacto en la sociedad.
- Reservado para algunas organizaciones.
- El usuario o cliente tienes pocas opciones para escoger.
- Poca capacidad de procesamiento.

1.2. Evolutiva (1980-2000)

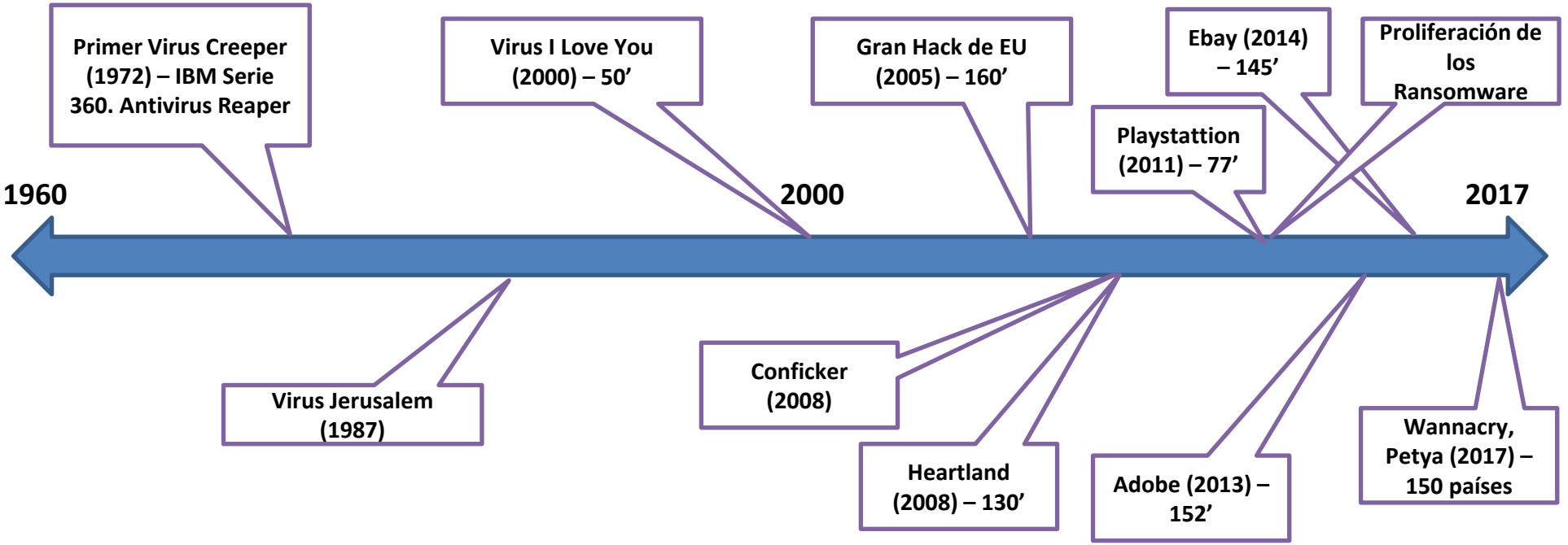
- La tecnología llega a casa y comienza a cambiar comportamientos.
- Comienza a ser accesible.
- Comienza a conectarnos globalmente. E-Commerce.
- El usuario o cliente tiene mejores opciones para escoger o tomar decisiones.
- Moderada capacidad de procesamiento.

1.3. Mundo Digital (2000-2017)



- La tecnología es nuestro día a día. Es integrada.
- Crecimiento explosivo.
- Accesible para todos.
- Redes sociales.
- Las empresas se centran en lo que el cliente quiere y en cómo entregarle un producto o servicio.
- Alta capacidad de procesamiento.

1.4. Evolución de la Seguridad de Información



2. Componentes de las TICs y sus Riesgos

- Organizaciones
- Aplicaciones
- Infraestructura Tecnológica
- Cloud
- Móviles
- SCADA
- Internet de las Cosas

2.1. Organizaciones

MALWARE

FRAUDE

CIBERTERRORISMO

INGENIERÍA SOCIAL

NATURALES

AMENAZAS

DEFENSAS

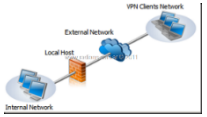
SEGURIDAD DE INFORMACIÓN

SISTEMAS DE GESTIÓN

CONTINUIDAD DE NEGOCIOS

ETHICAL HACKING

SEGURIDAD PERIMETRAL

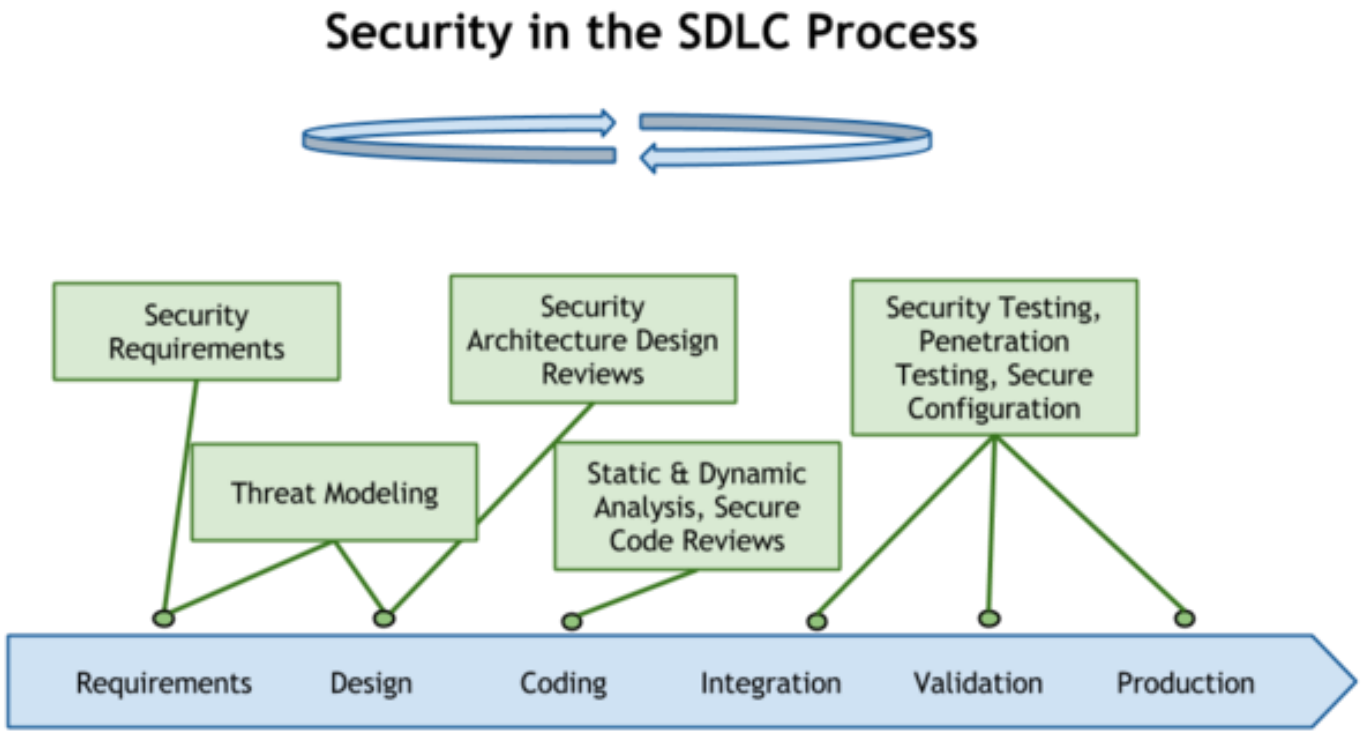


CAPACITACIÓN ENTRENAMIENTO

ORGANIZACIÓN

2.1. Organizaciones (Gobierno de la Seguridad de Información)

2.2. Aplicaciones (Ciclo de Desarrollo Seguro)



2.3. Infraestructura Tecnológica

- CAPACITACIÓN
- REQUISITOS DE SEGURIDAD
- ANÁLISIS DE VULNERABILIDAD
- “PARCHES”
- LINEA BASE DE SEGURIDAD

2.4. Cloud Computing (Riesgos)

- Se pierde el control físico de los datos. Es posible que una empresa no sepa donde está almacenada su información.
- Empleados del centro de datos Cloud pueden robar información. Asimismo accidentalmente se puede brindar accesos a personal no autorizado.
- Caso: **Dropbox (2011)**. 25 millones de usuarios. Una actualización a su site permitía acceder a una cuenta con cualquier contraseña.

2.4. Cloud Computing (Clasificación de Información)

"Apetito" por uso de Cloud Público

Clasificación de Información	Impactos Potenciales
Muy Confidencial	Impacto severo al negocio
Restringida	Impacto moderado
Uso Interno	Bajo impacto
Pública	Muy bajo o casi ningún impacto

2.4. Cloud Computing (Protección)

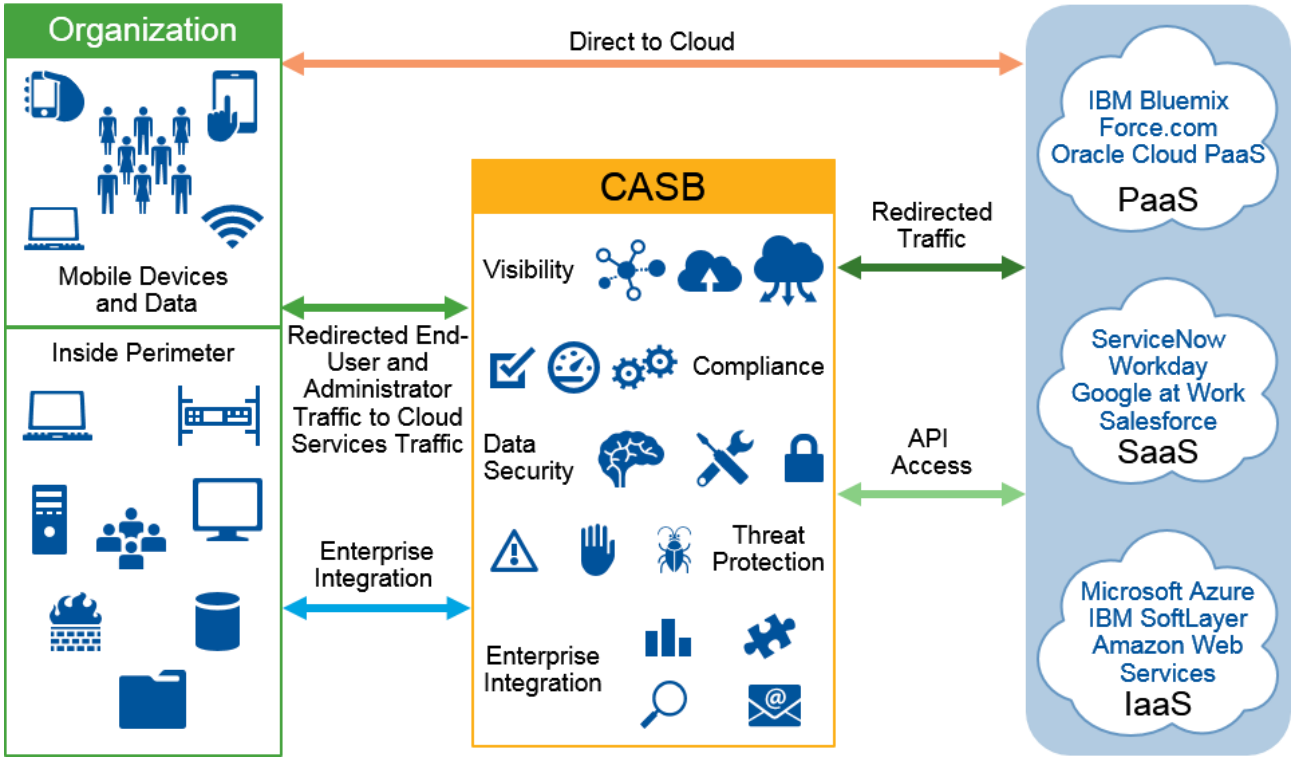
Protección de Información de Alto Valor

- Identificar Activos de Información de Alto Valor.
- Aislar los Activos de Información de Alto Valor.
- Encriptar información sensible.
- Implementar controles robustos para los accesos de Altos Privilegios.

Con los proveedores

- Revisar los planes de continuidad y recuperación de desastres.
- Utilizar múltiples proveedores de servicio cloud.
- Implementar una arquitectura cloud de alta disponibilidad para minimizar interrupciones.
- Procedimientos de Backup y Restore. Backups fuera de las instalaciones.
- Actualizar y probar el plan de gestión de crisis de la organización.
- Simular distintos escenarios de desastre.

2.4. Cloud Computing (CASB)



2.4. Cloud Computing (CASB)

CASB (Cloud Access Security Broker)

- Buscan proteger de ataques orientados a la información y los usuarios.
- Operan como intermediarios entre las aplicaciones de la nube y los usuarios.

Proveen:

- Visibilidad
- Conformidad
- Prevención de amenazas
- Seguridad de datos

2.5. Dispositivos Móviles (Riesgos y Controles)

Riesgos:

- Malware
- Robo
- Acceso a información no autorizada (personal, organizacional)
- Daño del dispositivo.

Métodos para reducir riesgos:

- Seguridad del dispositivo.
- Seguridad de las aplicaciones.
- Seguridad de las redes.

Controles de Seguridad:

- Encriptación
- Autenticación y control de accesos seguro.
- Control de acceso al dispositivo.

2.5. Dispositivos Móviles (BYOD)

BYOD (Bring your own device) permite a los usuarios conectar sus propios equipos (tablets, smartphones) a la red de la empresa.

Aspectos a considerar:

- Política de uso aceptable
- Cumplimiento de las políticas de la organización
- Privacidad
- Propiedad de los datos
- Soporte
- Infraestructura / Arquitectura tecnológica. Segmentación (VLANs).
- Análisis Forense
- Consideraciones Legales

2.6. Internet de las Cosas (Principales Riesgos)

Seguridad:

- Acceso a información personal trasmitida entre dispositivos.
- Ataques a la rede en la que están conectados los dispositivos.
- Personas no autorizadas pueden explotar vulnerabilidades para crear riesgos físicos (ejemplo: acceso a la computadora de un carro).

Privacidad:

- Acceso no autorizado a información personal sensible, por ejemplo: Geolocalización precisa
- Cuentas financieras/bancarias
- Información de salud.
- Hábitos.
- Condiciones físicas.

2.6 Internet de las Cosas (Medidas de Seguridad)

1. Las empresas deben implementar seguridad en sus dispositivos desde el comienzo de su desarrollo.
2. En el diseño:
   - Evaluaciones de riesgos de seguridad o privacidad.
   - Minimizar la cantidad de datos que obtienen.
   - Realizar pruebas de seguridad antes de lanzar sus productos.
3. Proveedores que hagan mantenimiento a la seguridad.
4. Cuando hay riesgos: defensa multicapas.
5. Control de accesos
6. Monitoreo de productos a lo largo del ciclo de vida y “parchar” vulnerabilidades.

2.7. SCADA

Sistemas que permiten controlar y supervisar los procesos industriales a distancia.

Ejemplos:

- Generadores de Energía
- Alarmas de defensa civil
- Plantas de tratamiento de agua

Sujeto a ataques de **Ciberterrorismo**.

¿Por qué es importante?

- Impacto masivo.
- Pérdida de vidas humanas.

Casos:

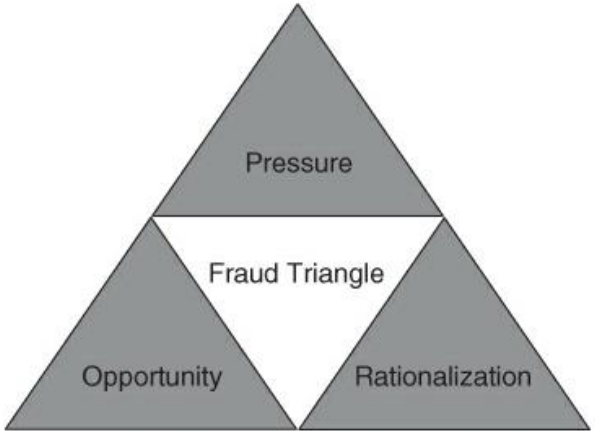
- **Stutnex** infectó las instalaciones nucleares de Iran explotando vulnerabilidades de sus sistemas SCADA.

3. Amenazas a la Seguridad de Información

- Fraude
- Espionaje Industrial
- Ciberterrorismo
- Malware
- Ingeniería Social

3.1. Fraude

- *"Engaño ilícito o criminal con la finalidad de lograr un beneficio personal"*
- *"Crimen imperceptiblemente oculto que evoluciona en el tiempo y cuidadosamente organizado que aparece en muchas formas"*



3.1. Fraude (Tipos)

- *Fraude de Tarjeta de Crédito.*
- *Fraude en seguros.*
- *Corrupción.*
- *Falsificación.*
- *Fraude de garantía de producto.*
- *Fraude en atención de salud.*
- *Fraude en telecomunicaciones.*
- *Lavado de dinero.*
- *Fraude del Click.*
- *Robo de identidad.*
- *Evasión de impuestos.*
- *Plagio.*

3.1. Fraude (Prevención y Detección)

Prevención:

- *Concientización.*
- *Rotación de personal.*
- *Segregación de funciones.*
- *Controles de la Norma ISO 27001.*
- *Específicos, de acuerdo al giro de la organización.*

Detección:

- *Sistemas de detección basados en juicio experto.*
- *Reglas SI-ENTONCES.*
- *Big Data.*
- *Basadas en Datos.*
- *Basadas en Estadísticas.*

3.2. Espionaje Industrial

El uso de técnicas de espionaje para obtener información clave.

- *Detalles de un nuevo proyecto de la competencia.*
- *Una lista de clientes de la competencia.*

Casos:

- *VIA Technology (2003).*
- *General Motors (1993).*
- *Bloomberg (2003).*

Crecimiento:

- *53% (2015) según CNN*

3.2. Espionaje Industrial (Medidas)

¿Cómo ocurre?

- *Spyware (tipo de malware).*
- *Esteganografía.*
- *Spear Phishing (phishing dirigido a personal de la empresa objetivo).*

Medidas de Protección:

- *Seguridad en redes.*
- *Mínimo privilegio.*
- *Rotación.*
- *Segregación de funciones.*
- *Bloquear uso de medios de almacenamiento.*
- *Concientización.*

3.3. Ciberterrorismo

- ***Ataque premeditado contra la información, sistemas de información, sistemas de cómputo y datos motivados por ideología política o económica.***
- ***Uso de computadores y la conectividad de Internet para lanzar ataques terroristas.***

Casos:

- *Oficinas del gobierno de Estonia (2007): Ataques de denegación de servicio.*
- *Sitios del gobierno de Estados Unidos y Corea del Sur (2009).*
- *Sitios de Entidades del Estado, Perú (2017).*

3.3. Ciberterrorismo (APT, armas)

APT (Advanced Persistent Thread)

- *Serie de ciberataques avanzados los cuales se mantienen por un periodo de tiempo (persistentes).*
- *Los primeros fueron originados desde China y duraron 7 años.*

Otro importante: ***Hacker Rusos***

Armas:

Malware, sea spyware, virus, troyanos, bombas lógicas, etc.

- *Stuxnet*
- *Flame (2012)*
- *Wannacry (2017)*

3.3. Ciberterrorismo (TOR, Dark Web)

TOR

- *Consiste en miles de servidores voluntarios propagados a nivel mundial.*
- *Usan encriptación por capas.*
- *Imposible de rastrear el tráfico de red.*
- *Provee privacidad.*
- *Al tráfico de información en esta red se le denomina **Dark Web**.*

Lo malo: se usa para fines ilícitos y criminales:

- *Números de tarjetas de crédito robadas.*
- *Venta de información financiera.*
- *Venta de pasaportes.*
- *Servicios de sicariato.*
- *Venta de armas.*
- *Venta de drogas.*
- *Pornografía infantil.*

3.3. Ciberterrorismo (Incidentes)

Incidente	% de Organizaciones
Un ataque de phishing fue exitoso e infectó sistemas en nuestra red con malware	37%
Uno o más de nuestras terminales tienen archivos encriptados debido a un ataque exitoso de ransomware	24%
Un malware se ha infiltrado en nuestro sistemas internos, pero no sabemos a través de qué canal	22%
Información confidencial o sensible fue accidentalmente divulgada a través de correo	22%
Uno o más de nuestros sistemas fue vulnerado exitosamente debido a navegación web de los empleados	21%

Osterman Research, Enero 2017

3.4. Malware (Tipos)

- *Zero-day*
- *Virus*
- *Gusanos*
- *Bombas Lógicas*
- *Puertas traseras (backdoor)*
- *Troyanos*
- *Botnets*
- *Ransomware (Wannacry, Petya)*
- *Rootkits*
- *Spyware*
- *Adware*

3.5. Ingeniería Social

Es la práctica de técnicas sociales para obtener información.

Algunos de los **métodos** usados:

- Engaño
- Asumir una posición de autoridad
- Presionar a alguien para realizar una acción arriesgada o entregar información.
- Suplantar a alguien.
- Seguir a personal autorizado sin proveer credenciales

3.5. Ingeniería Social

Técnicas:

- Suplantación
- Mirar encima del hombro
- Engañar a usuarios con bromas / trucos
- Buscar en recicladores
- Spam
- Phishing

¿Por qué funciona?

- Voluntad natural del ser humano de ayudar
- Autoridad
- Intimidación
- Prueba Social
- Urgencia
- Confianza

3.6. Otros Ataques

- Spear Phishing
- Whaling
- Spim
- Vishing

4. Especialidades en Seguridad

- Seguridad de Información y seguridad Informática
- Sistemas de Gestión de Seguridad de Información
- Continuidad de Negocios
- Evaluaciones de Seguridad
- Informática Forense

4.1. Seguridad de Información y Seguridad Informática

Conjunto de medidas y controles de las organizaciones aplicados para resguardar y proteger la información.

Pilares:

- Confidencialidad
- Integridad
- Disponibilidad

<u>Seguridad Informática:</u> Conjunto de medidas y controles aplicados a la infraestructura tecnológica y sus componentes y la información contenida en éstas.

4.2. Sistema de Gestión de Seguridad de Información

Sistema de Gestión: Conjunto de reglas, principios y herramientas relacionados entre sí para contribuir a la gestión de procesos de una organización.

- ISO 27001:2013
- NTP 27001:2014

- Preserva la **confidencialidad, integridad y disponibilidad** de la información aplicando un **proceso de gestión de riesgos**.
- Proporciona confianza a las **partes interesadas** que los riesgos se tratan adecuadamente.
- Se integra a los procesos de la organización.

4.3. Continuidad de Operaciones y Recuperación de Desastres

Continuidad de Operaciones

Asegura que la organización pueda continuar en un evento de desastre.

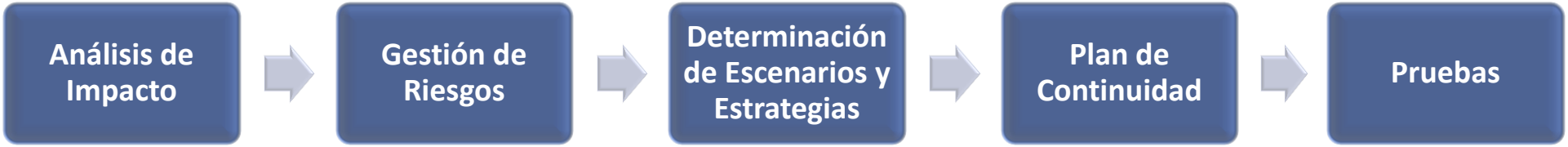
- Prioriza el capital humano.
- Se centra en los procesos críticos de la organización

Recuperación de Desastres

Recupera la tecnología tan pronto como sea posible.

- Datos, hardware y software necesario para restaurar operaciones críticas.
- Es uno de los aspectos del plan de continuidad.

4.3. Continuidad de Operaciones (Etapas)



4.5. Evaluaciones de Seguridad

Auditoría de Seguridad:
- Se enfoca en personas como procesos.
- Evalúa la seguridad organización versus determinados criterios.
- Técnicas: Interacción o entrevistas, revisión de infraestructura o componentes, acceso físico.
- Uso de Guías y Checklists.
- Ejemplos: PCI DSS, Circular G-140

Análisis de Vulnerabilidad:
- Proceso de definir, identificar y clasificar vulnerabilidades en un sistema o la red.
- Uso de herramientas de escaneo de vulnerabilidades.
- Aparición de falsos positivos.
- No explota vulnerabilidad.
- La precisión depende también de cómo se ha realizado el análisis.

Pruebas de Penetración:
- Simula las acciones de un atacante real para medir el impacto de la explotación de vulnerabilidades.
- Muy especializado, debe ejecutarse con mucho cuidado para evitar impactos.
- Más efectivo para tener certeza de que un ataque se puede realizar.

4.6. Informática Forense (Cyber Forensics)

- Su objetivo es examinar dispositivos de cómputo usando métodos científicos para extraer evidencia de manera que ***pueda ser presentada en la corte o juzgado***.
- Relativamente un campo nuevo.
- Ha desarrollado los últimos 20 años.

Aspectos:

- Herramientas especializadas.
- PCs, móviles (iOS, Android), virtual (cloud), network.
- Browser.
- Logs y registros del sistema.
- Archivos borrados.
- Documentos recientes, últimas visitas.
- Software desinstalado.

5. Marcos de Referencia y Organizaciones

- ISC2 – CISSP
- ISACA – CISM, COBIT
- ISO 27001
- NIST
- OWASP
- ONGEI - PECERT

5.1. ISC2 - CISSP

ISC2

- Asociación internacional sin fines de lucro.
- Más de 125,000 miembros.
- **CBK:** Cuerpo de conocimientos en materia de seguridad de información.

Certified Information Systems Security Professional (CISSP):

- Competencia
- Conocimiento
- Experiencia

En Seguridad de Información.

6 horas de Evaluación.

5.2. ISACA - CISM

ISACA

- Asociación internacional sin fines de lucro.
- Buenas Prácticas en Tecnologías de Información (Auditoría, Riesgo, Seguridad)
- Más de 140,000 miembros.

CISM

- Competencia
- Conocimiento
- Experiencia

En Seguridad de Información.

COBIT

- Marco de Referencia.
- Guía para las mejores practicas, dirigida al control de las Tecnologías de Información.
- Contiene aspectos de Seguridad de Información.

5.3. ISO 27001

ISO 27001

- Sistema de Gestión de Seguridad de Información.
- Certificable por la organización y bajo un alcance definido.
- Última versión: 2013

Beneficios

- Gestión de Riesgos y Cumplimiento de Controles de Seguridad.
- Cumplimiento normativo.
- Ventaja competitiva.
- Compromiso de la Alta Dirección con la seguridad de información.
- Mejora Contínua.

5.4. NIST

NIST (National Institute of Standards and Technology)

- Parte del Departamento de Gobierno de los Estados Unidos.
- Publicaciones técnicas: **http://csrc.nist.gov/publications/PubsSPs.html**

Ejemplos:

- Guía para recuperación en Ciberseguridad.
- Seguridad de aplicativos móviles.
- Gestión de Riesgos de Seguridad de Información.

5.5. OWASP

OWASP (Open Web Application Security Project)

- Sin fines de lucro.
- Objetivo: mejorar la seguridad del software.
- Libre.

Proyectos:

- OWASP Top Ten. Las 10 más vulnerabilidades más críticas en Aplicaciones Web.
- OWASP ASVS. Estándar que define un conjunto de niveles para ejecutar verificaciones de seguridad en las aplicaciones.

5.6. PeCert - SeGDi

PeCERT (Coordinación de Emergencias en Redes Teleinformáticas)

- Objetivo: Promover la coordinación entre las entidades de la Administración Pública, para la prevención, detección, tratamiento, recolección de información y desarrollo de soluciones para los incidentes de seguridad.

SeGDi (Secretaría de Gobierno Digital)

- Órgano de línea, con autoridad técnico normativa, responsable de formular y proponer políticas y planes nacionales en materia de Informática y Gobierno Electrónico.
- http://www.gobiernodigital.gob.pe

5.7. OTROS

- SANS Institute
- EC-Council
- DRI (Disaster Recovery Institute)
- PECB
- OAS

6. Normativas

- Bancos
- SGSI para Entidades Estatales
- Continuidad de Negocio
- Ley de Protección de Datos Personales
- Ley de Delitos Informáticos

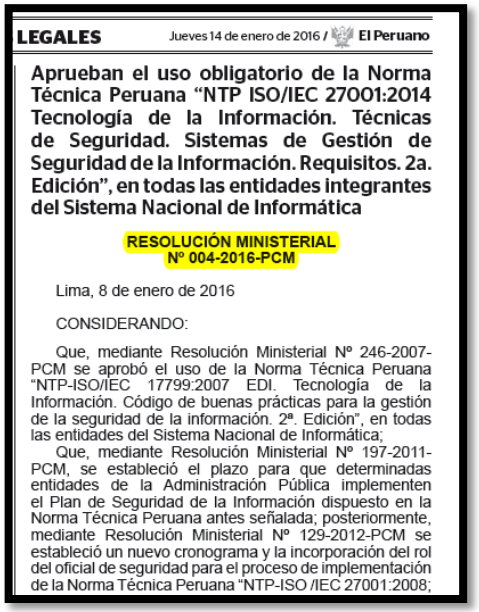
http://www.ongei.gob.pe/
http://www.gobiernodigital.gob.pe/banco/ongei_BUSQ_NORMAS.asp

6.1. Circular N° G-140-2009 y modificatorias

- Aplica a Empresas Bancarias, Financieras, Cajas, Cooperativas, Seguros, AFPs.
- Implementación de un SGSI.
- Estructura organizacional.
- Controles de seguridad de información.

6.2. RM N° 004-2016-PCM (08/01/2016)

- Aplica a Entidades del Estado.
- Uso obligatorio de la **NTP ISO/IEC 27001:2014**.
- Plazo de 2 años para la implementación.
- Formación del Comité de Gestión de Seguridad de Información.
- Designación de un Oficial de Seguridad de la Información.



LEGALES Jueves 14 de enero de 2016 / El Peruano

Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática

RESOLUCIÓN MINISTERIAL Nº 004-2016-PCM

Lima, 8 de enero de 2016

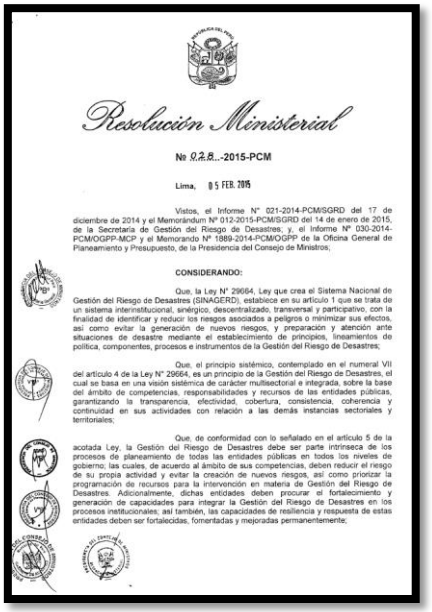
CONSIDERANDO:

Que, mediante Resolución Ministerial Nº 246-2007-PCM se aprobó el uso de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición", en todas las entidades del Sistema Nacional de Informática;

Que, mediante Resolución Ministerial Nº 197-2011-PCM, se estableció el plazo para que determinadas entidades de la Administración Pública implementen el Plan de Seguridad de la Información dispuesto en la Norma Técnica Peruana antes señalada; posteriormente, mediante Resolución Ministerial Nº 129-2012-PCM se estableció un nuevo cronograma y la incorporación del rol del oficial de seguridad para el proceso de implementación de la Norma Técnica Peruana "NTP-ISO /IEC 27001:2008;

6.3. RM N° 028-2015-PCM (05/02/2015)

- Establecimiento de Lineamientos para la **Gestión de la Continuidad Operativa** de las entidades públicas.
- Implementación de los lineamientos.
- Basada en la ISO 22301.



Resolución Ministerial

Nº 028-2015-PCM

Lima, 05 FEB. 2015

Vistos, el Informe N° 021-2014-PCM/SGRD del 17 de diciembre de 2014 y el Memorandum Nº 012-2015-PCM/SGRD del 14 de enero de 2015, de la Secretaría de Gestión del Riesgo de Desastres; y, el Informe Nº 030-2014-PCM/OGPP-MCP y el Memorando Nº 1889-2014-PCM/OGPP de la Oficina General de Planeamiento y Presupuesto, de la Presidencia del Consejo de Ministros;

CONSIDERANDO:

Que, la Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD), establece en su artículo 1 que se trata de un sistema interinstitucional, sinérgico, descentralizado, transversal y participativo, con la finalidad de identificar y reducir los riesgos asociados a peligros o minimizar sus efectos, así como evitar la generación de nuevos riesgos, y preparación y atención ante situaciones de desastre mediante el establecimiento de principios, lineamientos de política, componentes, procesos e instrumentos de la Gestión del Riesgo de Desastres;

Que, el principio sistémico, contemplado en el numeral VII del artículo 4 de la Ley N° 29664, es un principio de la Gestión del Riesgo de Desastres, el cual se basa en una visión sistémica de carácter multisectorial e integrada, sobre la base del ámbito de competencias, responsabilidades y recursos de las entidades públicas, garantizando la transparencia, efectividad, cobertura, consistencia, coherencia y continuidad en sus actividades con relación a las demás instancias sectoriales y territoriales;

Que, de conformidad con lo señalado en el artículo 5 de la acotada Ley, la Gestión del Riesgo de Desastres debe ser parte intrínseca de los procesos de planeamiento de todas las entidades públicas en todos los niveles de gobierno; las cuales, de acuerdo al ámbito de sus competencias, deben reducir el riesgo de su propia actividad y evitar la creación de nuevos riesgos, así como priorizar la programación de recursos para la intervención en materia de Gestión del Riesgo de Desastres. Adicionalmente, dichas enticlades deben procurar el fortalecimiento y generación de capacidades para integrar la Gestión del Riesgo de Desastres en los procesos institucionales; así también, las capacidades de resiliencia y respuesta de estas entidades deben ser fortalecidas, fomentadas y mejoradas permanentemente;

6.4. LEY 29733 – Protección de Datos Personales (22/03/2013)

Objetivo General

Garantizar la seguridad de los datos personales contenidos o destinados a ser contenidos en bancos de datos personales, mediante medidas de seguridad que protejan a los bancos de datos personales, de conformidad con la Ley Nº 29733 y su reglamento.

Alcance

Los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realice en el territorio nacional.

6.4. LEY 29733 – Protección de Datos Personales (22/03/2013)

- Protege los datos de las personas naturales.
- Aplicable a todas las empresas, sean privadas o públicas.
- Implica la aplicación de directivas de seguridad de información (NTP 27001).
- Otorga derechos a los titulares de los datos personales.
- Responsabilidad en caso de vulnerar los derechos. Sanciones hasta 100 UITs.

PODER LEGISLATIVO

CONGRESO DE LA REPUBLICA

LEY Nº 29733

EL PRESIDENTE DE LA REPUBLICA

POR CUANTO:

El Congreso de la República
ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

LEY DE PROTECCIÓN DE DATOS PERSONALES

Título Preliminar: Disposiciones generales.
Título I: Principios rectores.
Título II: Tratamiento de datos personales.
Título III: Derechos del titular de datos personales.
Título IV: Obligaciones del titular y del encargado del banco de datos personales.
Título V: Bancos de datos personales.
Título VI: Autoridad Nacional de Protección de Datos Personales.

6.5. LEY 30096 – Delitos Informáticos (22/10/2013)

Artículo 2:

"El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado."

6.5. LEY 30096 – Delitos Informáticos (22/10/2013)

Objetivo:

- Prevenir y sancionar conductas ilícitas que afectan sistemas y datos informáticos, cometidas mediante la utilización de tecnologías de información o comunicaciones.

Ultima modificatoria:

Ley 30171 (11/03/2014)

Tipifica los delitos:

- Contra datos y sistemas
- Contra indemnidad y libertad sexuales
- Contra la intimidad y secreto de las comunicaciones
  - Interceptación de datos
- Contra el patrimonio
  - Fraude
- Contra la fé pública
  - Suplantación de identidad

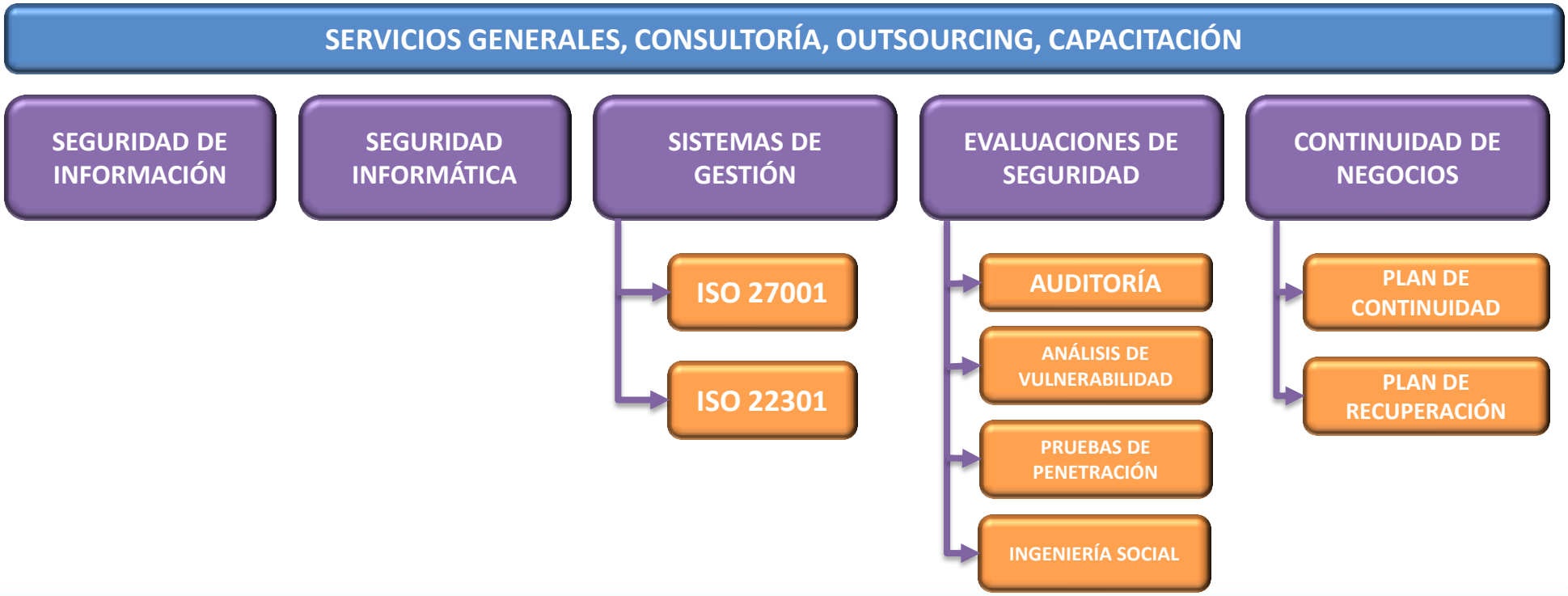
7. Beneficios de aplicar Seguridad de la Información

- **Protección de los activos de la organización**
- **Contribuye a asegurar la continuidad de operaciones**
- **Minimiza daños o impactos**
- **Mejora la imagen de la organización**
- **Contribuye a la mejora de procesos**
- **Reduce costos**
- **Permite obtener ventaja competitiva**

7. Conclusiones y Recomendaciones

1. **LA HISTORIA HA DEMOSTRADO QUE LA SEGURIDAD SIEMPRE ESTÁ UN PASO ATRÁS QUE EL MISMO DESARROLLO DE LAS TECNOLOGÍAS.**
2. **ESPECIALIZACION DE LA SEGURIDAD SE PRODUCE CON LA ESPECIALIZACION DE LAS TECNOLOGÍAS.**
3. **CONCIENTIZACION DEBE SER PERMANENTE, EL PERSONAL Y LAS ORGANIZACIONES SIEMPRE CAMBIAN.**
4. **LA PREVENCIÓN ES LA MEJOR ARMA PARA PROTEGERSE.**

INTELITECH PERU



FIN

Carlos Gonzales Fung
cgonzales@intelitech.com.pe