Sistemas de Gestión de Seguridad de la Información

Ana Cecilia Vargas
Alonso Castro Mattei

Indice

- Conceptos básicos SGSI
- ISO/IEC 27000
- Implementaciones de ISO/IEC 27000
- La seguridad del lado del usuario.
- El SGSI de la UCR

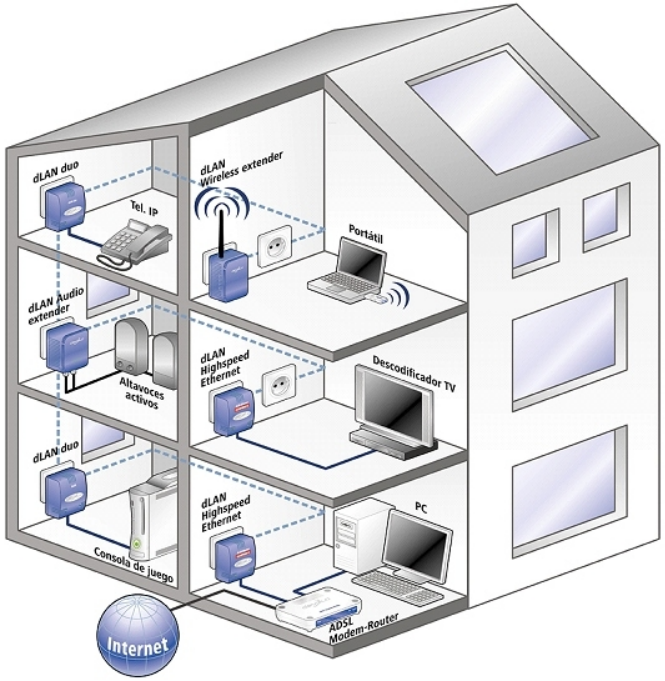
Todos los días tenemos riegos que atentan contra la seguridad de la información:

Usuario internos	Usuarios externos	Desastres naturales
		

¿Qué podemos hacer para proteger datos e información en un entorno como este?

- La respuesta es simple:
  - Se puede implementar un sistema de gestión de seguridad de la información.
- ¿Para qué sirve?
  - Conocer
  - Gestionar
  - Minimizar
    - Los riesgos que atentan contra la seguridad de la información

¿Seguridad informática es lo mismo que seguridad de la información?



*Los activos de información provienen de distintas fuentes y se almacenan en diversos soportes, como BD e inclusiv impresos.

¿Qué nos permite un SGSI?

- Analizar y ordenar la estructura de los sistema de información.
- Establecer los procedimientos de trabajo para mantener su seguridad.
- Disponer de controles para medir la eficacia de lo establecido en el punto anterior.

La idea es alcanzar un nivel de riesgo menor que el soportado por la institución, para preservar la confidencialidad, integridad y disponibilidad de la información.

¿Qué aspectos de seguridad abarca un SGSI?

ISO / IEC 27000

Ana Cecilia Vargas
Alonso Castro Mattei

Normas ISO/IEC 27000

- Contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los SGSI:
  - ISO/IEC 27000 - es un vocabulario estandard para el SGSI. (en desarrollo actualmente).
  - ISO/IEC 27001 - es la certificación para las organizaciones. Especifica los requisitos para la implantación del SGSI. La más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos.

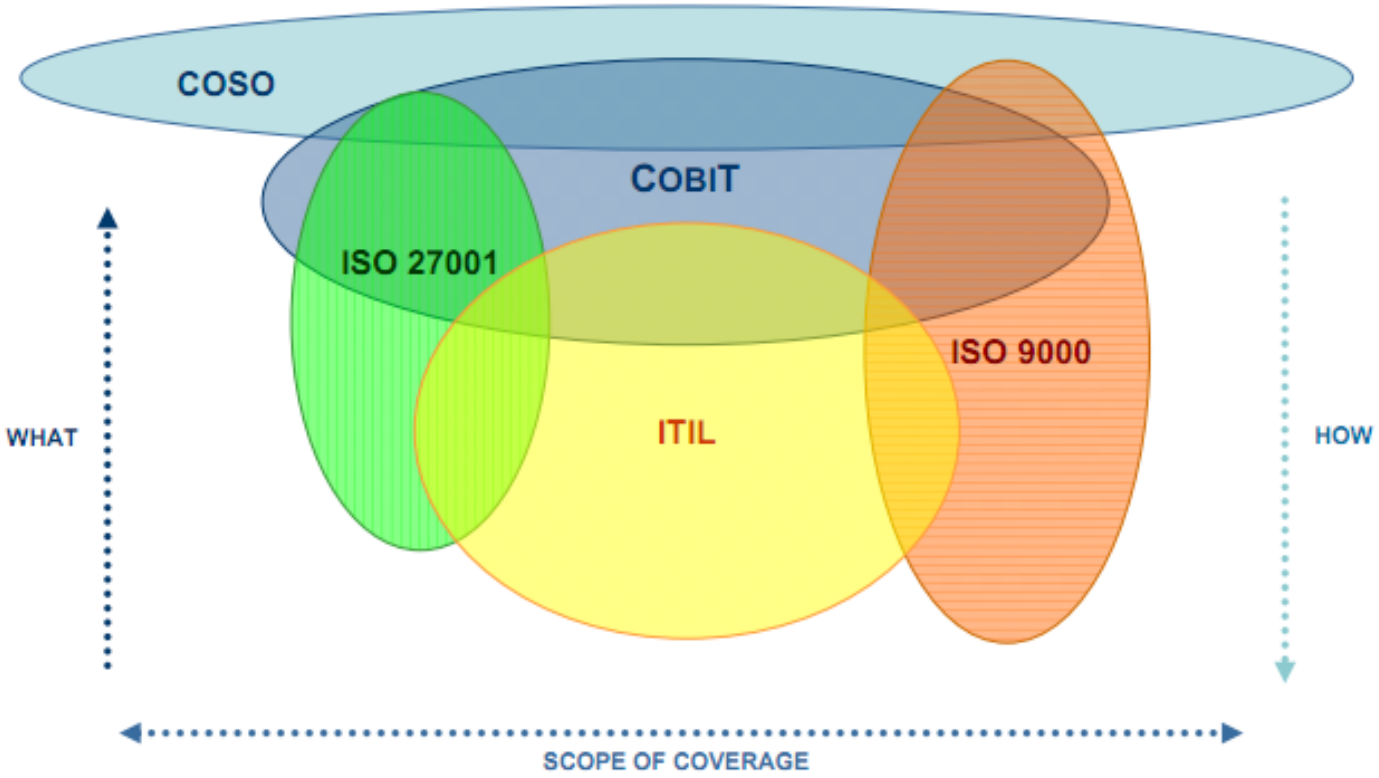
Normas ISO/IEC 27000

- ISO/IEC 27002 - es código de buenas prácticas para la gestión de seguridad de la información.
- ISO/IEC 27003 - son directrices para la implementación de un SGSI.
- ISO/IEC 27004 - son métricas para la gestión de seguridad de la información.
- ISO/IEC 27005 - trata la gestión de riesgos en seguridad de la información.

Normas ISO/IEC 27000

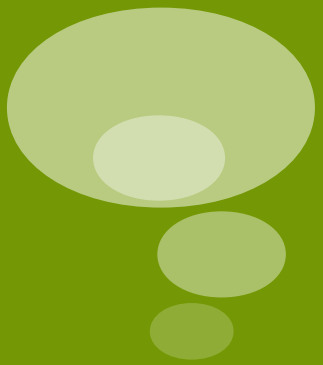
- ISO/IEC 27006:2007 - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información.
- ISO/IEC 27007 - Es una guía para auditar al SGSI.
- ISO/IEC 27799:2008 - Es una guía para implementar ISO/IEC 27002 en la industria de la salud.
- ISO/IEC 27035:2011 – Técnicas de Seguridad – Gestión de Incidentes de Seguridad: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades.

Relación con otras normas



Alcance de la Norma ISO/IEC 27000

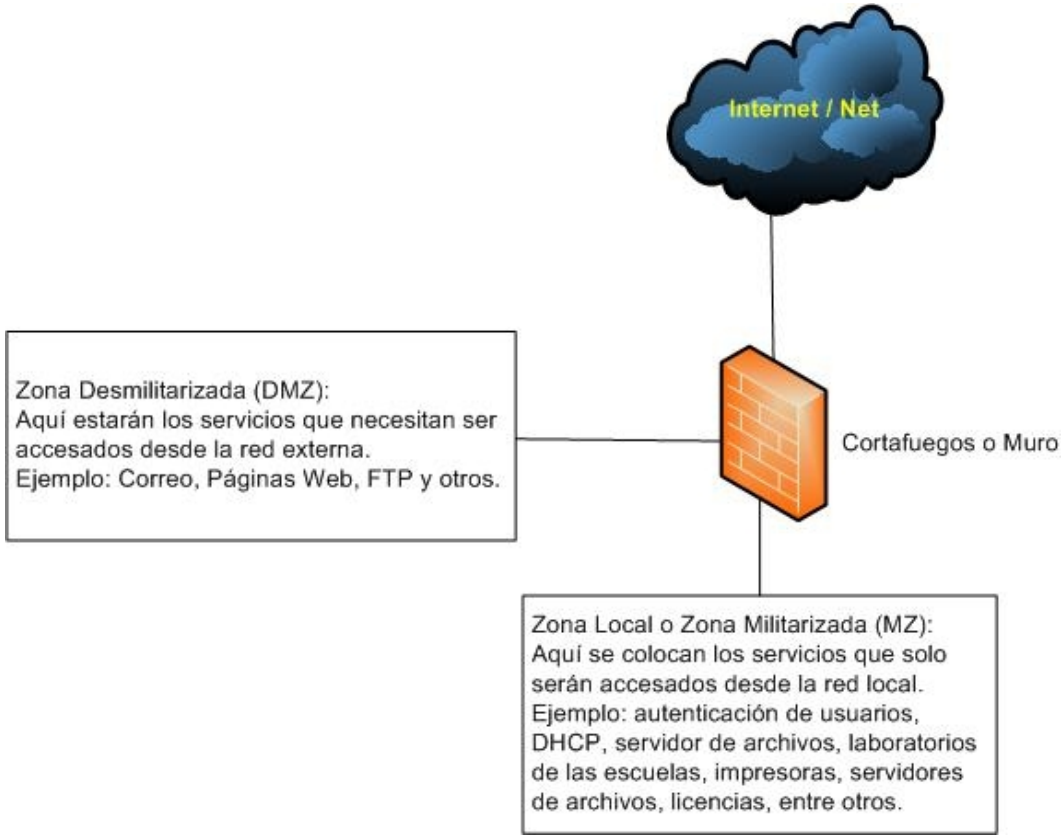
- ISO 27001 propone un marco de gestión de la seguridad de toda la información de la empresa, incluso si es información perteneciente al propio conocimiento y experiencia de las personas o sea tratada en reuniones etc.
- No debemos centrar la atención solamente en los sistemas informáticos por mucho que tengan hoy en día una importancia mas que relevante en el tratamiento de la información ya que de otra forma, podríamos dejar sin proteger información que puede ser esencial para la la actividad de la empresa.



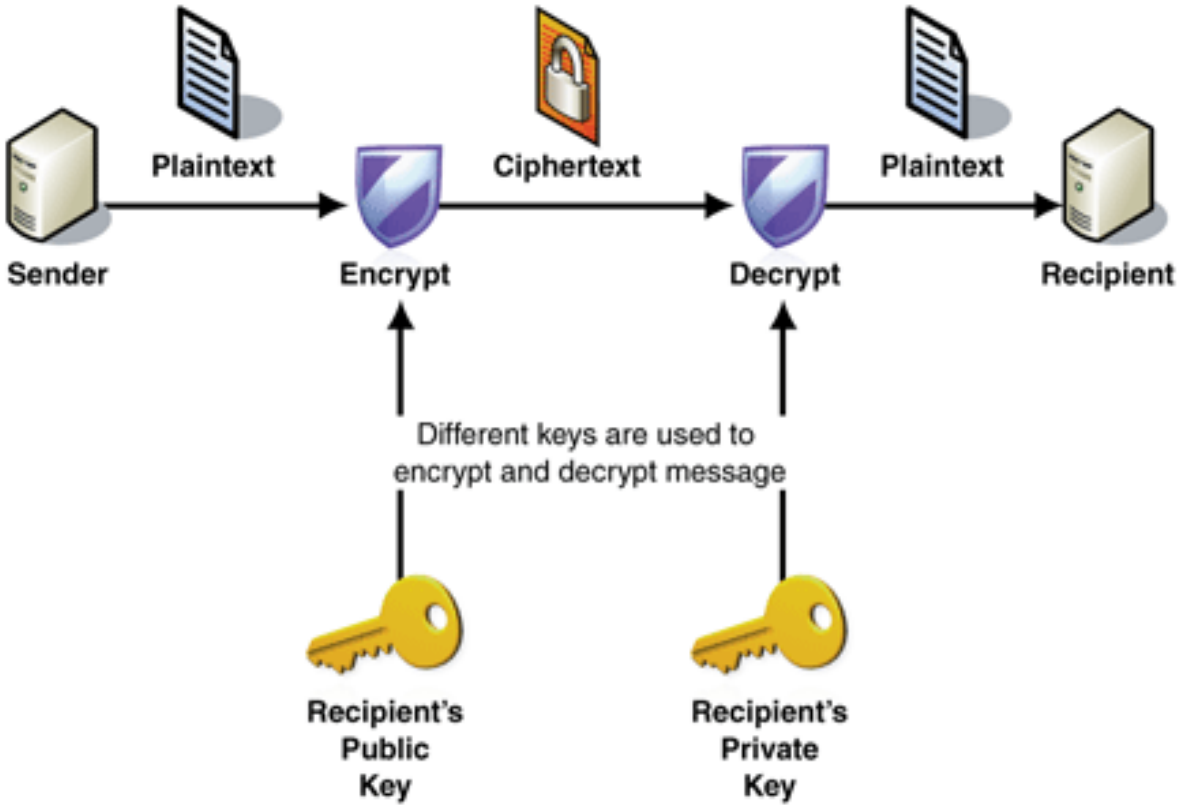
Implementación del ISO/IEC 27000


SGSI
FASE 1
Definir La Política
Documento de la Política
FASE 2
Definir El Alcance Del SGSI
Alcance Del SGSI
FASE 3
Análisis de Riesgos
Análisis de Activos de Información
Definir Amenazas y vulnerabilidades
Análisis de riesgos
Gestión del riesgo desde el punto de vista organizacional
FASE 4
Gestión del Riesgo
Grado de Aseguramiento requerido
Resultados y conclusiones
FASE 5
Controles propuestos por la Norma
Selección de controles a implementar
Controles Seleccionados
Controles Adicionales
FASE 6
Declaración de Aplicabilidad
Controles Seleccionados
Controles propuestos por la norma
Declaración de Aplicabilidad
FASE 7
Revisión del sistema
Revisión del SGSI
Medidas Preventivas
Medidas Correctivas
Propuestas de Mejora
AUDITORIA INTERNA
Plan de Auditorias

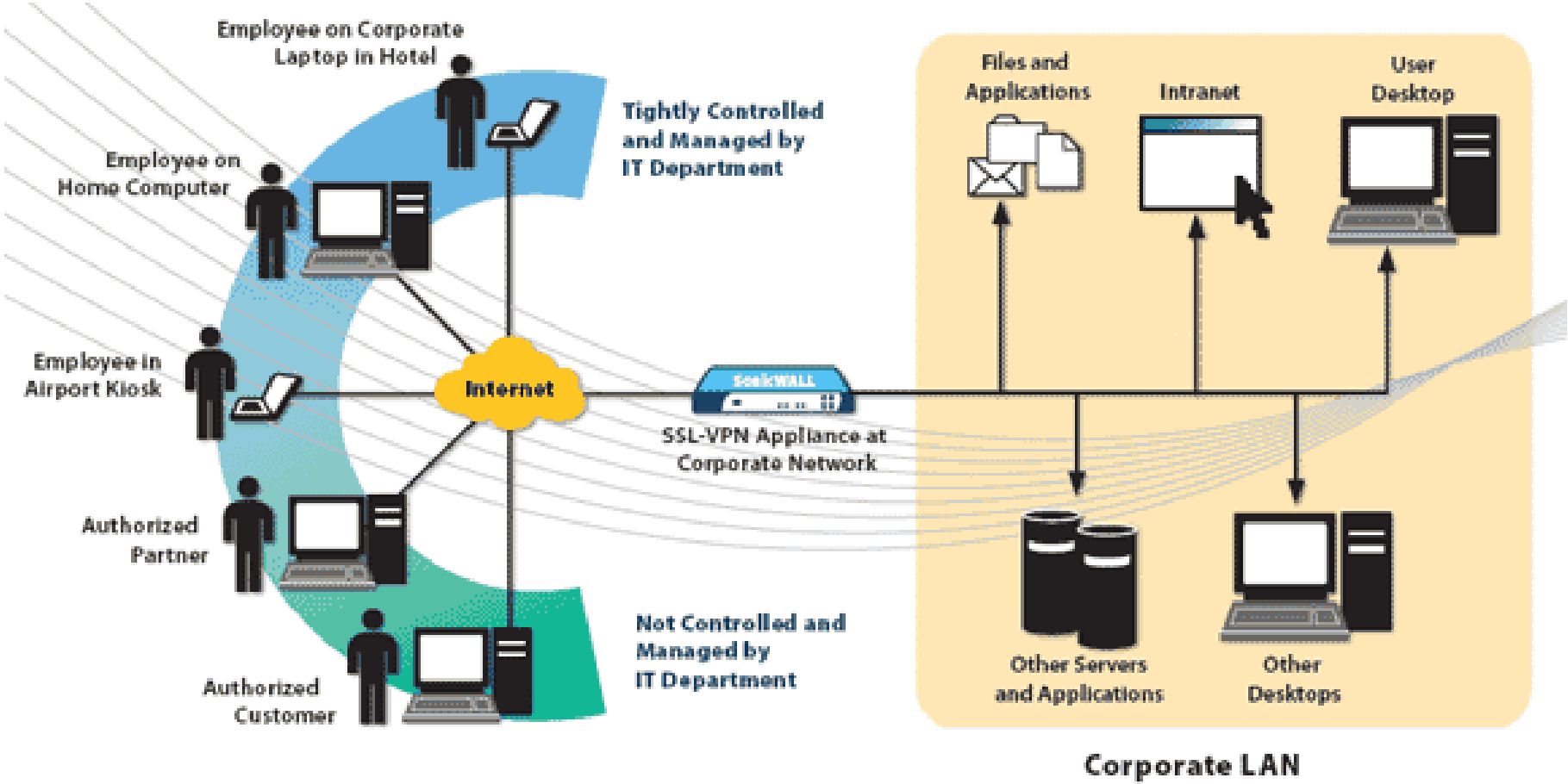
Cortafuegos (firewall)



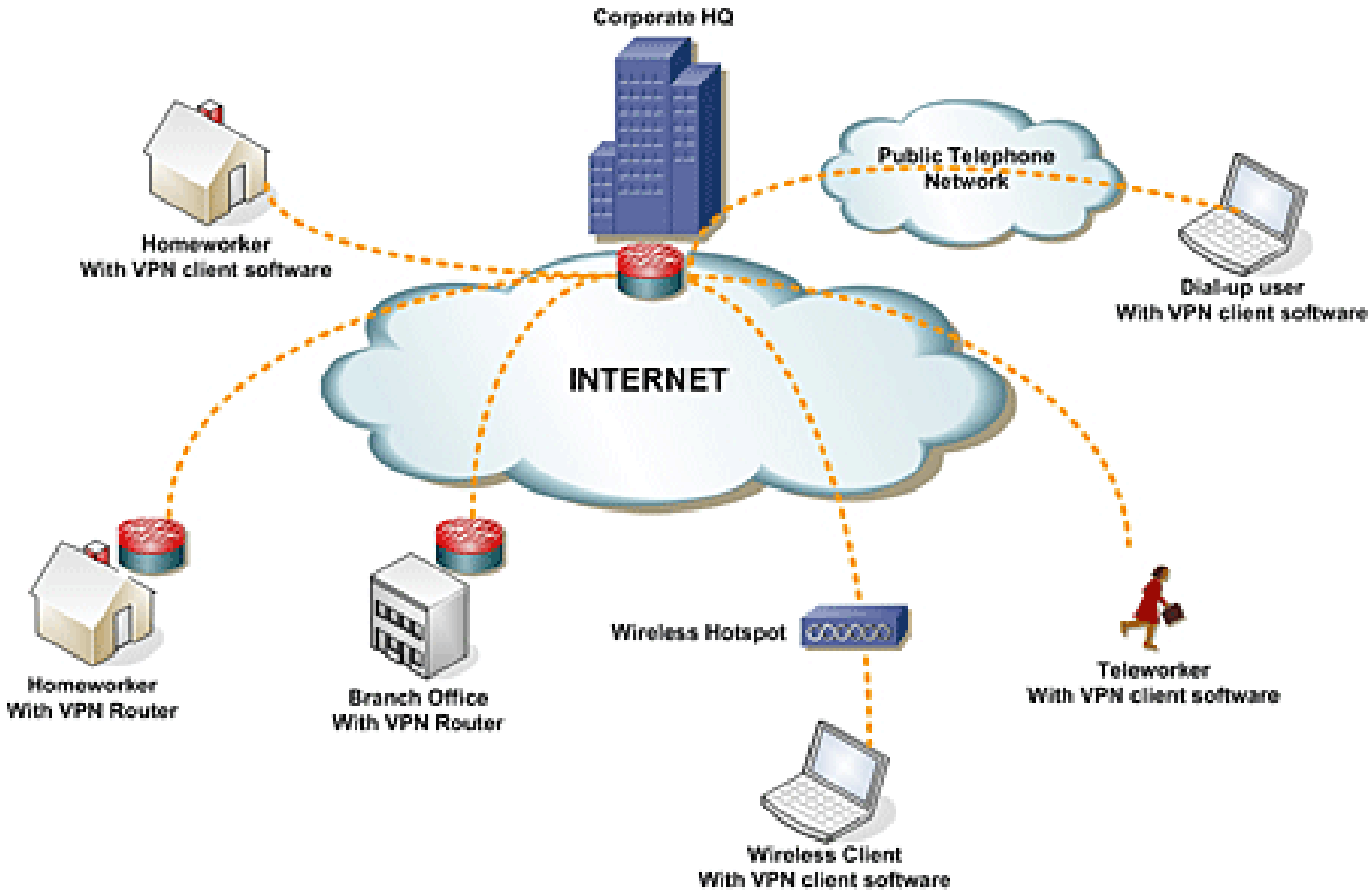
Certificados de seguridad



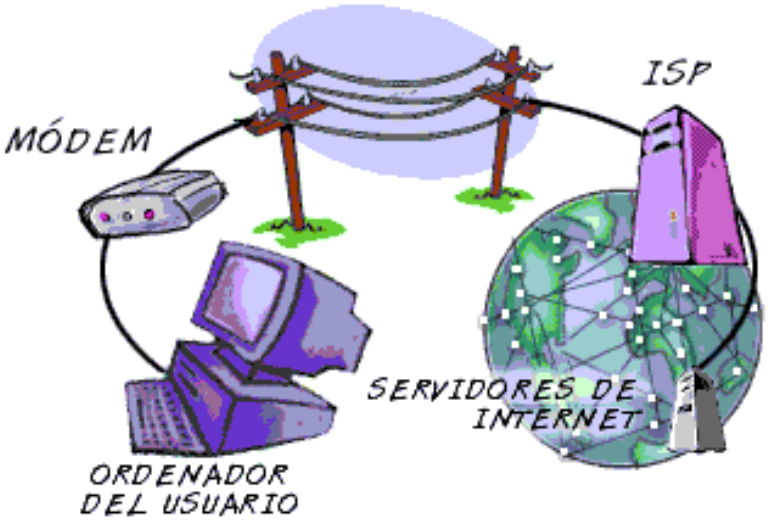
Conexiones cifradas (SSL)



Red Privada Virtual (VPN)



Trabajo colaborativo



Tanto la institución como el ISP, debe asegurar que la información que viaja por la red y por los equipos de comunicación que administra lleguen a su destino seguros.

La seguridad del lado de los usuarios de los sistemas de información

Phishing

From: Banco De Costa Rica <informe@bancocostarica.com>
Subject: **Estimado Cliente!**
Date: August 7, 2007 7:50:23 PM GMT-06:00
To: [redacted]@internetworks.co.cr

BCR Banco de Costa Rica

Estimado Cliente de Banco de Costa Rica,

Banco de Costa Rica le comunica que nuestros servidores de procesos bancarios han sido actualizados y están ya operativos.

Sin embargo debido a la ingente cantidad de usuarios que usan Internet como medio de pago seguro, nos vemos en la obligación de pedirle su colaboración para una rápida restauración de los datos en las nuevas plataformas.
Si no ha entrado en su cuenta bancaria en los últimos 12 minutos se ruega lo haga de inmediato para evitar cualquier posible problema en su cuenta o futura pérdida de datos.

Debe entrar a su cuenta haciendo click sobre el enlace correspondiente a su tipo de cuenta:

Para Personas: http://www.bancobcr.com/login.asp?verificaridentidad=personas

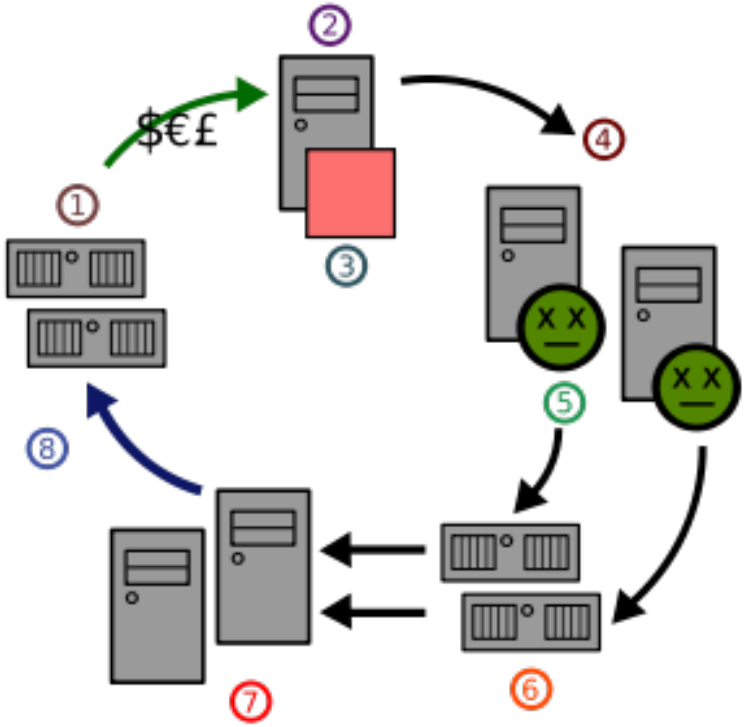
Para Empresas: http://www.bancobcr.com/login.asp?v

http://www.nikolashn.com/ssl/-http-/www.bancobcr.com/servicios/creditos/operaciones/personas/

Banco de Costa Rica pone a su disposición, sin costo adici[illegible] la última tecnología en protección y encriptación de datos.
BANCO DE COSTA RICA

® Banco de Costa Rica, S.A., 2007

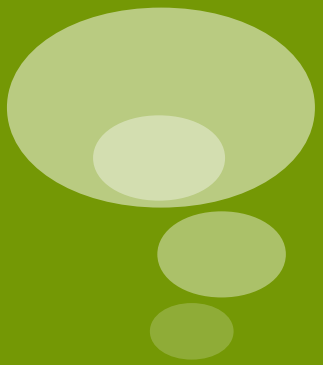
Spam



- (1): Sitio web de Spammers
- (2): Spammer
- (3): Spamware
- (4): Ordenadores infectados
- (5): Virus o troyanos
- (6): Servidores de correo
- (7): Usuarios
- (8): Tráfico Web

Recomendaciones para la seguridad de contraseñas

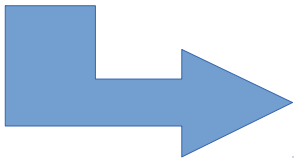
- Cambie periódicamente la contraseña.
- Procure que la contraseña tenga como mínimo 8 caracteres combinando números, letras y símbolos.
- Evite utilizar nombres propios, o temas asociables a su persona.
- Elija un usuario y contraseña distintos.
- Nunca anote las claves en un papel.
- Nunca revele sus claves, y menos por email o teléfono.
- Evite que vean las claves que introduce.



Implementación de un SGSI para la UCR

Administración General de la Seguridad y el Entorno de TI

1	2	3	4	5
Normas de Aplicación General	Planificación y Organización	Implementación de TI	Prestación de Servicios y Mantenimiento	Seguimiento
Gestión de Calidad	Planificación de TI	Implementación de Software	Acuerdos de Servicio	Seguimiento de procesos de TI
Gestión de Riesgos	Modelo de Arquitectura	Implementación de Infraestructura	Administración y Operación de la plataforma tecnológica	Seguimiento y evaluación de Control Interno
Gestión de Seguridad	Infraestructura	Contratación de terceros para implementación y mantenimiento	Atención de requerimientos	Auditoría Interna
Gestión de Proyectos	Independencia del Recurso Humano		Manejo de Incidentes	
Cumplimiento de Obligaciones de la gestión de TI	Administración de Recursos Financieros			



Gobierno de Seguridad de Información
Gestión de Riesgos de Información
Programa continuo de Seguridad
Administración del Programa de Seguridad
Administración de Incidentes de Seguridad

Algunas políticas que estamos implementando

- 4.1 Clasificación, Control y aseguramiento de bienes de cómputo y comunicaciones:
  - 030101 Asignación de responsabilidades sobre los bienes
  - 030102 Inventario de Recursos Informáticos
- 4.2 Resguardo y Protección de Información
  - 040103 De los respaldos y recuperación de la información
- 4.3 Reporte y Manejo de Incidentes de Seguridad
  - 050101 Reporte de Incidentes relativos a la Seguridad de la Información
  - 050102 Reporte de debilidades en materia de Seguridad

Algunas políticas que estamos implementando

- 4.4 Gestión y Administración de la Seguridad de las Operaciones, Responsabilidades y Procedimientos Operacionales
  - 070101 Documentación de los procedimientos operacionales
- 4.5 Planificación y Aceptación de Sistemas
  - 070201 Planificación de la capacidad
- 4.6 Protección contra Instrucciones maliciosas y códigos móviles
  - 070301 Controles contra instrucciones maliciosas

Algunas políticas que estamos implementando

- 4.7 De la Administración y Seguridad de los medios de Almacenamiento
  - 070603 De la Administración de medios informáticos removibles
  - 070605 De los procedimientos de manejo de la información
  - 070606 Seguridad de la documentación de los sistemas
- 4.8 Gestión y Administración de la Seguridad de las Comunicaciones, Intercambio de Información y y software
  - 080106 Política de Uso Aceptable de Internet
  - 080107 Política de Uso Aceptable de Intranet
  - 080108 Política de Uso Aceptable del Correo Electrónico

Algunas políticas que estamos implementando

- 4.9 Control de Accesos, Administración de accesos de usuarios
  - 090201 Asignación de derechos de acceso
  - 090202 Registro de usuarios
  - 090203 Administración de privilegios
  - 090204 Administración de contraseñas de usuario
  - 090205 Revisión de derechos de acceso de usuario
- 4.10 Control de Acceso a la Red
  - 090407 Control de conexión a la red
  - 090409 Seguridad en los servicios de red

Algunas políticas que estamos implementando

- 4.11 Control de acceso y demás controles aplicables a las bases de datos
  - 090701-500 Implementación de los controles de acceso y demás controles aplicables a las bases de datos de la UCR
- 4.12 Monitoreo del uso y acceso a los sistemas
  - 090902 Monitoreo del uso de los sistemas

Muchas gracias!!

Ana Cecilia Vargas
Alonso Castro Mattei