



SEGURIDAD DE LA INFORMACIÓN

Headquarter
7 Morning Glory Circle
Santa Fe, New México
87506 – USA
Phone: 505 660 5251
Fax: 505 820 0410
info@santafeassociates.com
www.santafeassociates.com

Quito Office
La Pradera N30-258 y Mariano Aguilera
Edificio Santorini, piso 3
Teléfono: +593-2-2568 068
Fax: +593-2-2557 182
info@santafeassociates.com.ec
www.santafeassociates.com.ec

Seguridad de la información



AGENDA A DESARROLLAR:

- Riesgos e impacto en los negocios
- Laboratorios
- Enfoque ISO 17799

Paso 1: Por que?

Reconocer los riesgos y su impacto en los negocios

Algunos datos

11:22 | EL GUSANO SE LLAMA "ZAFI.D"

Un nuevo virus se esconde en tarjetas navideñas

Un virus informático llamado "Zafi.D", que se esconde en una tarjeta electrónica de felicitación, comenzó a circular por la red, informó [Panda Software](#). La compañía advirtió a los usuarios que extremen las medidas de seguridad durante estas fiestas.

ESTAFAS EN INTERNET

El "phishing" ya pesca en todo America

Detectaron casos que afectaron a numerosas empresas y a los clientes de bancos estadounidenses y del resto de America.

INTERNET

Nadie logra controlar la epidemia: el "correo basura" invade las casillas de todo el mundo

Apenas 150 "spammers" norteamericanos son los responsables del 90 por ciento de los mensajes no deseados que atestan las computadoras de todo el mundo. Todavía no hay leyes para limitar su impacto económico.



Algunas premisas

- No existe la “verdad absoluta” en Seguridad Informática.
- No es posible eliminar todos los riesgos.
- La Dirección está convencida de que la Seguridad Informática no hace al negocio de la compañía.
- Cada vez los riesgos y el impacto en los negocios son mayores.

Algunas realidades

En mi compañía ya tenemos seguridad porque ...

... implementamos un firewall.

... contratamos una persona para el área.

... en la última auditoría de sistemas no me sacaron observaciones importantes.

... ya escribí las políticas.

... hice un penetration testing y ya arreglamos todo.

Algunos datos



En general todos coinciden en:

El **80%** de los incidentes/fraudes/ataques son efectuados por personal interno

Fuentes:

The Computer Security Institute

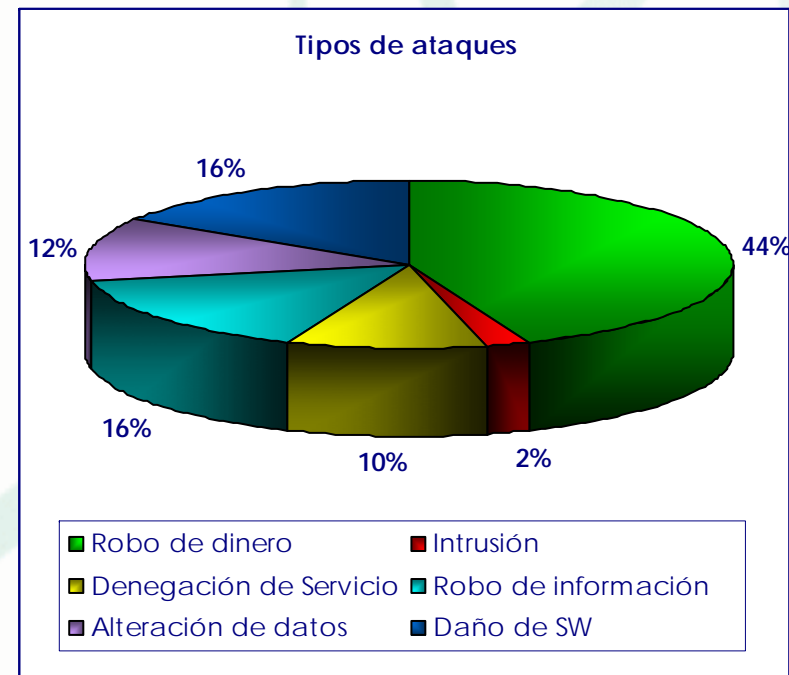
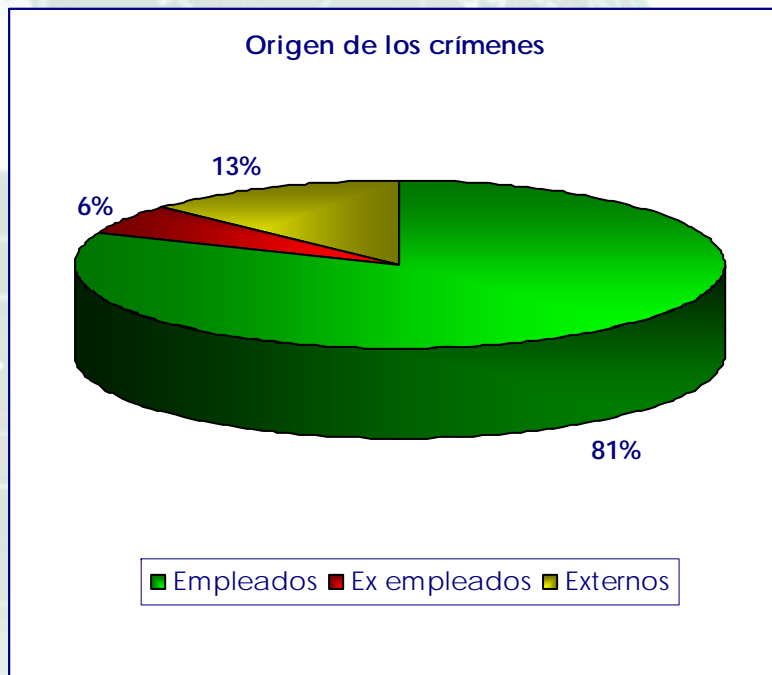
Cooperative Association for Internet Data Analysis (CAIDA)

CERT

SANS

Algunos datos

¿Quiénes pueden atacarme y para qué?



Fuentes:
Data Processing Management
Computer Security Institute
CAIDA
CERT
SANS

¿ Qué debo proteger ?

La información que está básicamente...

- Impresa.
- Escrita en papel.
- Almacenada electrónicamente.
- Transmitida por correo o utilizando medios electrónicos.
- Presentada en imágenes.
- Expuesta en una conversación.
- En el conocimiento de las personas.

¿ Qué debo proteger ?

**¡ No se puede hacer una buena
defensa si no se conoce lo que se
defiende !**

**Incluso cuando se
conozca lo que se
defiende, hay que
entender la mentalidad
del atacante**



Principios de Seguridad

CONFIDENCIALIDAD:

Medidas enfocadas a garantizar que la información está disponible para aquellos que estén autorizados a conocerla. Es crítica cuando los datos proporcionan ventaja competitiva en fabricación o confianza del consumidor.

INTEGRIDAD:

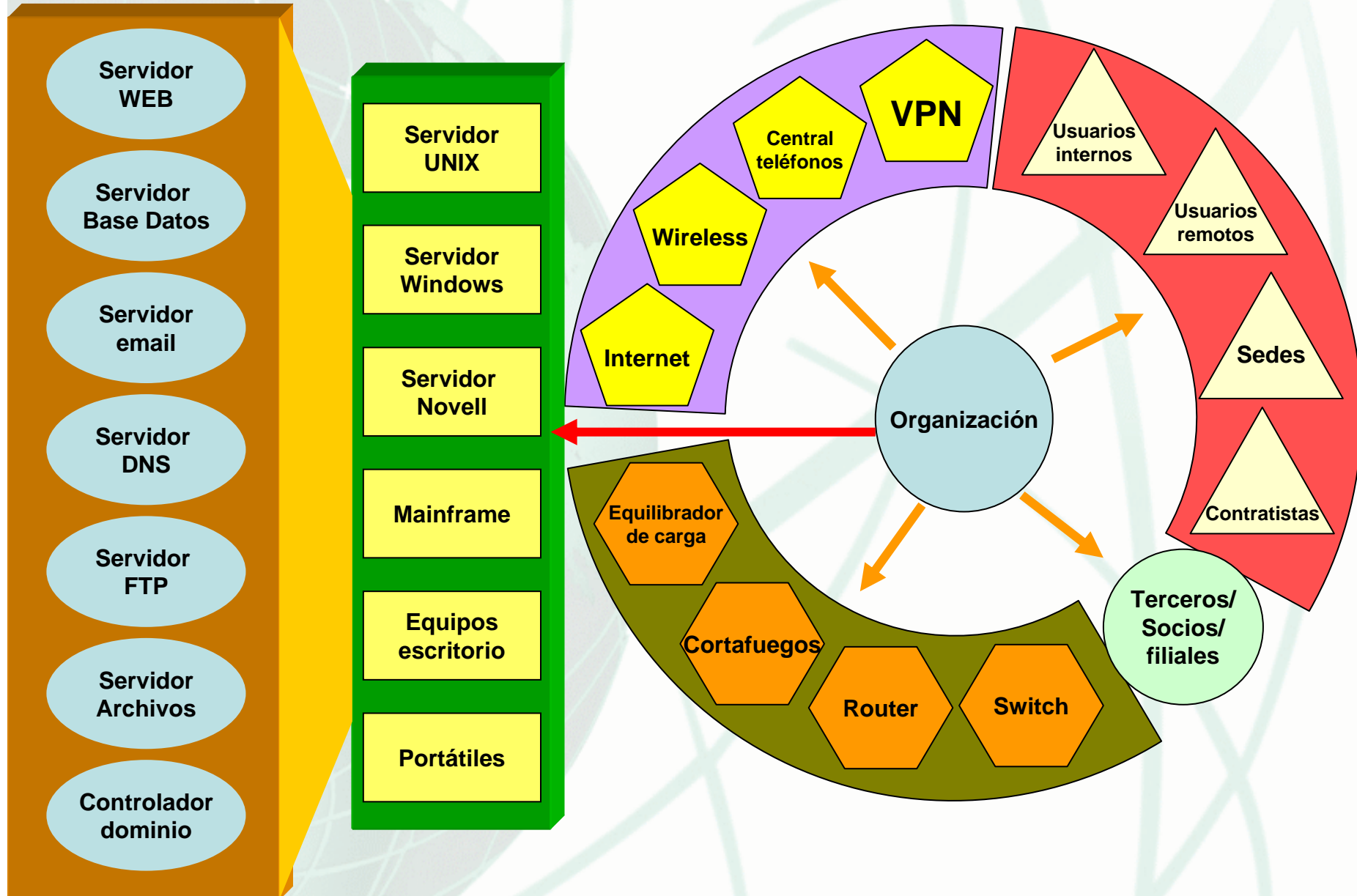
Garantizar que la información es fiable y que no se ha modificado. Es crítica cuando se trata de datos que serán utilizados en análisis estadísticos, o cálculos matemáticos.

DISPONIBILIDAD:

Garantizar que los datos son accesibles el momento que se los necesita. Es crítica cuando se tiene que acceder a datos en tiempo real.



Modelo del Objetivo



Que se traduce en...



Mails "anónimos" con información crítica o con agresiones **Robo de información**

Spamming **Violación de e-mails** Destrucción de equipamiento

Violación de contraseñas Intercepción y modificación de e-mails

Virus Incumplimiento de leyes y regulaciones Violación de la privacidad de los empleados

Ingeniería social empleados deshonestos

Fraudes informáticos

Programas "bomba"

Propiedad de la Información

Captura de PC desde el exterior

Interrupción de los servicios

Destrucción de soportes documentales

Acceso clandestino a redes

Robo o extravío de notebooks

Acceso indebido a documentos impresos

Software ilegal

Indisponibilidad de información clave

Intercepción de comunicaciones

Falsificación de información para terceros

Agujeros de seguridad de redes conectadas

Que se traduce en...



Instalaciones *default*

Escalamiento de privilegios

Password cracking

Puertos vulnerables abiertos

Man in the middle

Exploits

Servicios de log inexistentes o que no son chequeados

Denegación de servicio

Últimos parches no instalados

Backups inexistentes

Desactualización

Port scanning

Replay attack

Keylogging

Unos ejemplos prácticos...

1

Mi pana el hombre araña (hackeando un email)

2

El superpoderoso buscador (hackeando con Google)

3

Olfateando el aire (hackeando Wireless)

2

Matando la araña (hackeando a la web)

Principales riesgos y su impacto en los negocios



En estos tipos de problemas es difícil:

- Darse cuenta que pasan, hasta que pasan.
- Poder cuantificarlos económicamente, por ejemplo ¿cuánto le cuesta a la compañía 4 horas sin sistemas?
- Poder vincular directamente sus efectos sobre los resultados de la compañía.

Principales riesgos y su impacto en los negocios



Se puede estar preparado para que ocurran lo menos posible:

- sin grandes inversiones en software
- sin mucha estructura de personal

Tan solo:

- ordenando la Gestión de Seguridad
- parametrizando la seguridad propia de los sistemas
- utilizando herramientas licenciadas y libres en la web

Paso 2:

Si igual voy a hacer algo, ¿por qué no lo hago teniendo en cuenta las Normas Internacionales aplicables?

Normas aplicables

Entre los distintos organismos relacionados comercial y/o institucionalmente con los temas de Seguridad de la Información, podemos encontrar los siguientes:

- Information Systems and Audit Control Association - ISACA: COBIT
- British Standards Institute: BS
- International Standards Organization: Normas ISO
- Departamento de Defensa de USA: Orange Book / Common Criteria
- ITSEC – Information Technology Security Evaluation Criteria: White Book
- Sans Institute
- Sarbanes Oxley Act, HIPAA Act

Normas aplicables

International Standards Organization: Normas ISO

- La principal norma de Evaluación e Implementación de medidas de Seguridad en Tecnologías de la Información es la NORMA ISO 17799.
- Está organizada en diez capítulos en los que se tratan los distintos criterios a ser tenidos en cuenta en cada tema.

Paso 3:

**Que pide la Norma ISO 17799
Gestión de Seguridad?**

Seguridad de la Información

La información = activo comercial

Tiene valor para una organización y por consiguiente debe ser debidamente protegida.

“Garantizar la continuidad comercial, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades”

“La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados”

Normas de Gestión ISO 17799



Está organizada en diez capítulos en los que se tratan los distintos criterios a ser tenidos en cuenta en cada tema para llevar adelante una correcta:

GESTION DE SEGURIDAD DE LA INFORMACION

Alcance

Recomendaciones para la gestión de la seguridad de la información

Base común para el desarrollo de estándares de seguridad

Normas de Gestión ISO 17799



Preservar la:

confidencialidad:

accesible sólo a aquellas personas autorizadas a tener acceso.

integridad:

exactitud y totalidad de la información y los métodos de procesamiento.

disponibilidad:

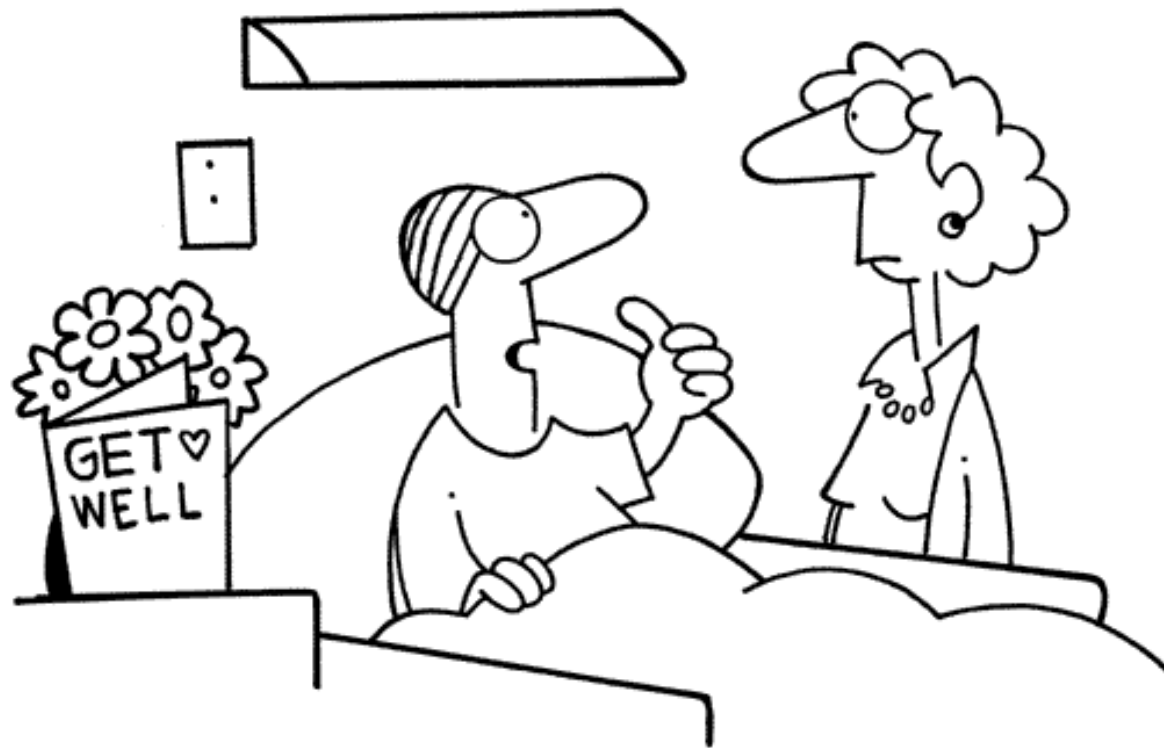
acceso a la información y a los recursos relacionados con ella toda vez que se requiera.

Normas de Gestión ISO 17799



- 1. Política de Seguridad**
- 2. Organización de Seguridad**
- 3. Clasificación y Control de Activos**
- 4. Aspectos humanos de la seguridad**
- 5. Seguridad Física y Ambiental**
- 6. Gestión de Comunicaciones y Operaciones**
- 7. Sistema de Control de Accesos**
- 8. Desarrollo y Mantenimiento de Sistemas**
- 9. Plan de Continuidad del Negocio**
- 10. Cumplimiento**

Lo que se viene en seguridad



“Como conozco mucha información confidencial, mi JEFE me instaló un FIREWALL en mi cabeza”

Lo que se viene en seguridad

A veces los resultados no acompañan



“Ayer cambié las contraseñas de todos los usuarios y les puse PASSWORD, les mandé un mail a cada uno explicándoles, puse un cartel en la pared y puse etiquetas en todas las tazas de café de la gente. Adivina CUANTOS USUARIOS ME LLAMARON ESTA MAÑANA PORQUE OLVIDARON SU PASSWORD????”

Lo que se viene en seguridad

A veces acompañan demasiado



“Disculpa esta situación, pero por SEGURIDAD tengo tatuadas las PASSWORDS debajo de mis PIES”

Lo que se viene en seguridad

Haga buen uso de la información crítica

Un hombre se va a dar una ducha en el momento en que su esposa está terminando de hacerlo.

En ese preciso instante suena el timbre de la puerta.

Después de algunos segundos de duda deciden que ella irá, por lo cual se envuelve en una toalla,

ella abre la puerta y se encuentra con el vecino. Antes de que ella pronuncie una palabra, el vecino le dice:

Le doy US\$1.000 si deja caer la toalla en el suelo.

Ella piensa unos segundos, se decide, dejar caer la toalla y se queda sin nada frente al vecino que , después

de unos segundos mete al mano al bolsillo, saca \$1000, saca la plata, se lo entrega y se va.

Muy confundida, cierra la puerta rápidamente, se envuelve la toalla y regresa al baño a secarse el cabello.

Cuando llega el marido le pregunta quien había tocado la puerta

El vecino de al lado, dice ella y el marido le pregunta:

Te devolvió los \$1000 que le presté.

Muchas veces, compartir la información crítica le ayudará.

Muchas gracias



• **Preguntas?**

pedroponce@email.com