Estudio de la industria del hardware

Seguridad informática

- Benítez Gutiérrez Rubí Itzel
- Caballero Borjas Mariel
- Colunga Aguilar Juan Omar
- Contreras Martínez Viridiana
- Espinosa Gutiérrez José Antonio
- González Martínez Asja Valeska
- Hernández de los Santos Omar Enrique
- Juárez Zúñiga Arturo
- Luna Canto Nancy
- Morales Álvarez Gerardo

Profa. Edna Martha Servin Palencia

Índice

Objetivo

Presentar información sobre la seguridad informática, su importancia, sus tipos y ejemplos de empresas que se dedican a este rubro basados en distintas fuentes de información.

Introducción

Como parte del estudio de la Industria del hardware y como conocimiento necesario para nuestra carrera, presentamos a continuación el tema de seguridad Informática, en donde hablaremos de la concepto, sus clasificaciones, características, los tipos de amenazas que se pueden generar en ausencia de seguridad informática y mas información relevante.

¿Qué es la seguridad informática?

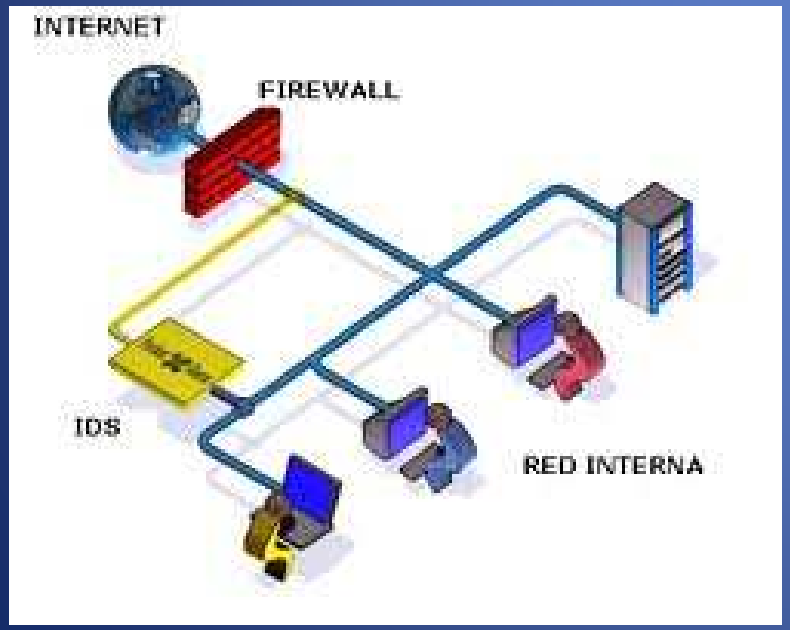
La seguridad informática es una especialidad dedica a el cuidado de la infraestructura computacional (seguridad física) y su información mediante técnicas, disciplinas, protocolos, etc. Es también la encargada de diseñar normas, procedimientos y métodos para conseguir un sistema informático seguro y confiable.

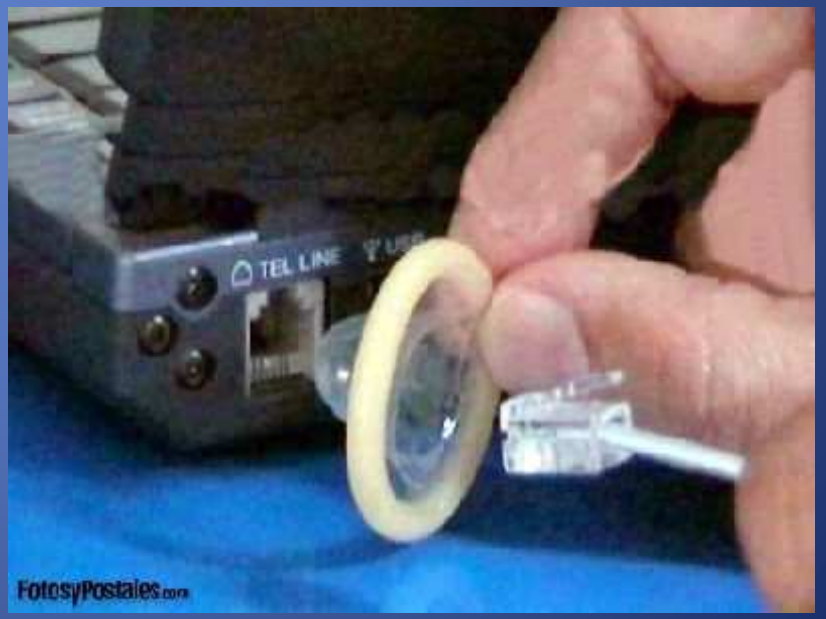
Seguridad Pasiva

Esta formada por las medidas que se implantan para, una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema, por ejemplo, teniendo siempre al día copias de seguridad.

Seguridad Activa

Comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema.
Ejemplos: impedir el acceso a la información a usuarios no autorizados mediante introducción de nombres de usuario y contraseñas; instalación de un antivirus, etc.





Para que un sistema de información se considere seguro…

Integridad

- Es una garantía de que nuestros datos no han sido alterados ni destruidos de modo no autorizado.

Confidencialidad

- La seguridad de que nuestros datos no van a ser vistos por personas ajenas a nosotros que no tienen permiso para ello.

Disponibilidad

- La información disponible para los usuarios autorizados cuando la necesiten.

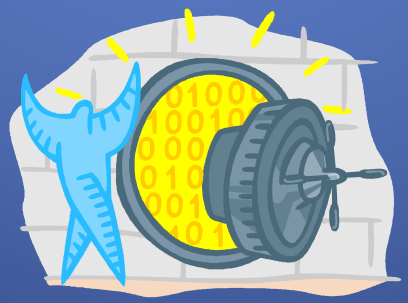
Seguridad Lógica

- Los mecanismos y herramientas de seguridad lógica tienen como objetivo proteger digitalmente la información de manera directa.
  - **Control de Acceso.-** Mediante nombre de usuario y contraseñas.
  - **Cifrado de datos (Encriptación).-** Los datos se enmascaran con una clave especial creada mediante un algoritmo de encriptación. El cifrado de datos fortalece la confidencialidad.
  - **Antivirus.-** Detectan o impiden la entrada de virus y otro software malicioso. Protege la integridad de la información.

•**Cortafuegos (firewall).-** Se trata de uno o más dispositivos de software, de hardware o mixtos que permiten, deniegan o restringen el acceso al sistema. Protege la integridad de la información.

•**Firma Digital.-** Su finalidad es identificar de forma segura a la persona o al equipo que se hace responsable del mensaje o documento. Protege la integridad y la confidencialidad de la información.

•**Certificados digitales.-** Son documentos digitales mediante los cuales una entidad autorizada garantiza que una persona o entidad es quien dice ser, avalada por la verificación de su clave pública. Protege la integridad y confidencialidad de la información.



Mecanismos de Seguridad

- Según la función que desempeñen los mecanismos de seguridad pueden clasificarse en:

Preventivos

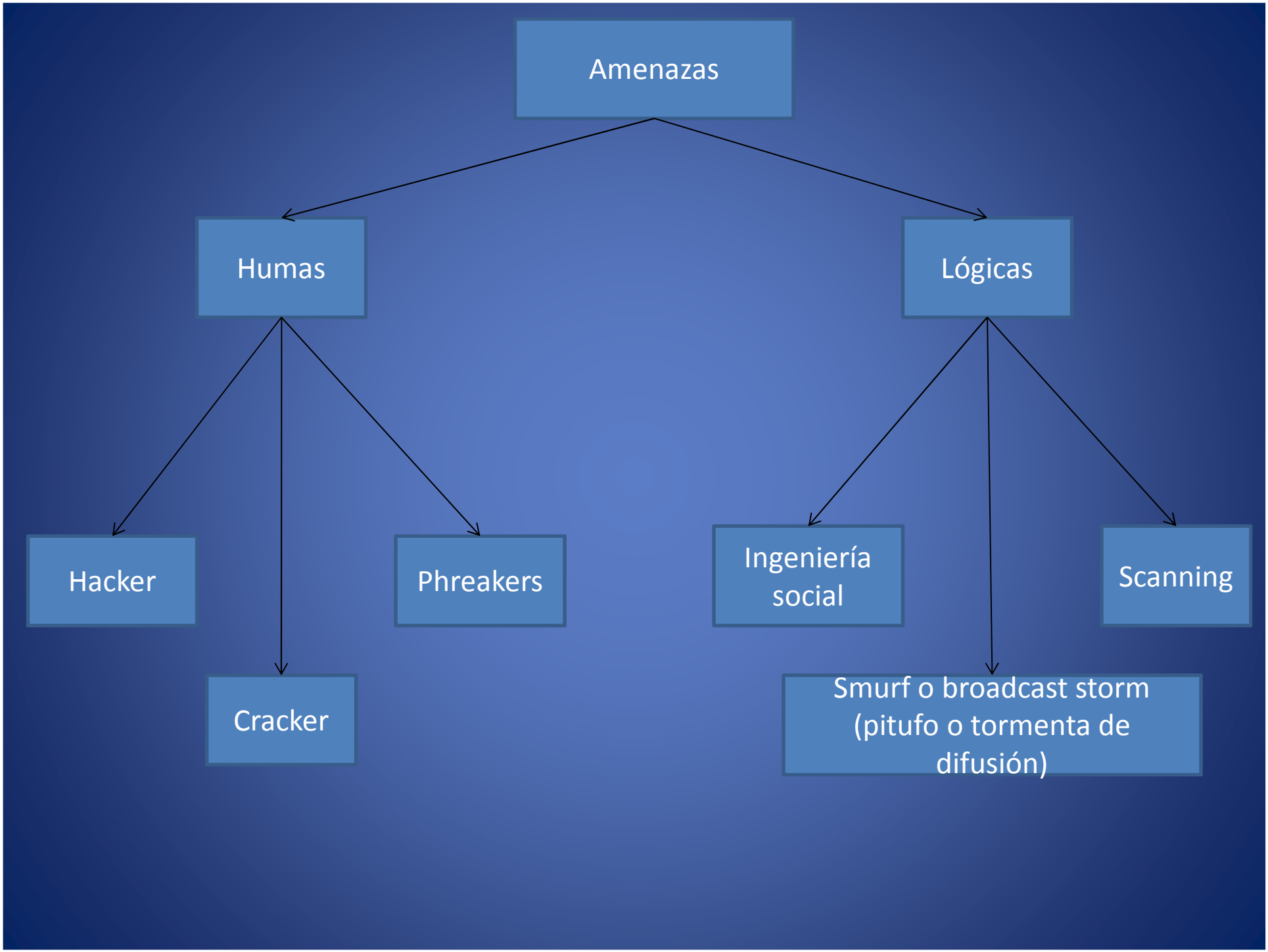
Actúan antes de que se produzca un ataque. Su misión es evitarlo.

Detectores

Actúan cuando el ataque se ha producido y antes de que cause daño en el sistema.

Correctores

Actúan después de que haya habido un ataque y se hayan producido daños. Su misión es la de corregir las consecuencias del daño.


Amenazas
Humas
Lógicas
Hacker
Cracker
Phreakers
Ingeniería social
Smurf o broadcast storm (pitufo o tormenta de difusión)
Scanning

Amenazas Humanas

•Hacker

Personas que están siempre en una continua búsqueda de información, viven para aprender y todo para ellos es un reto; no existen barreras. Son curiosos y pacientes. Quieren aprender y satisfacer.

•Cracker

Un cracker, en realidad es un hacker cuyas intenciones van más allá de la investigación. Es una persona que tiene fines maliciosos.

•Phreakers

Personas con un amplio (a veces mayor que los mismo empleados de las compañías telefónicas) conocimiento en telefonía. Antecesor de hacking ya que es mucho más antiguo. Comenzó en la década de los 60's cuando Mark Bernay descubrió como aprovechar un error de seguridad de la compañía Bell, el cual le permitió realizar llamadas gratuitas.

Amenazas Lógicas

•Ingeniería social

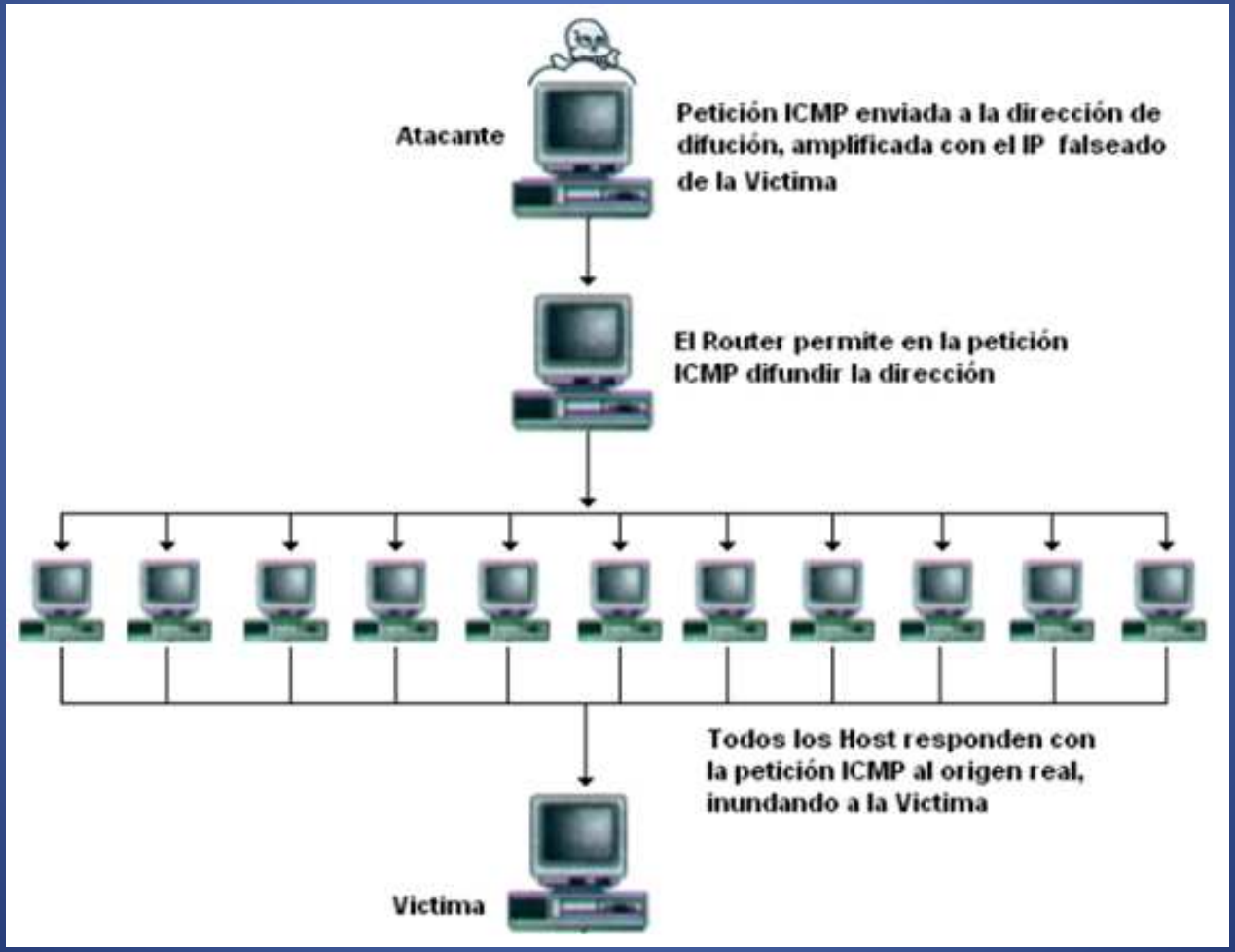
Es el arte de manipular a las personas, con el fin de obtener información que revele todo lo necesario para penetrar la seguridad de algún sistema. Esta técnica es una de las más usadas a la hora de averiguar nombres de usuario y contraseñas.

•Scanning

Método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. Se envía una serie de paquetes para varios protocolos y se deduce que servicios están escuchando por las respuestas recibidas o no recibidas.

•Smurf o broadcast storm

Consiste en recolectar una seria de direcciones Broadcast ó proxys las cuales realizaran peticiones PING a la máquina victima.



VIDEO

Empresas que ofrecen servicios de Seguridad

Juniper Networks

- **Juniper Networks** es una multinacional dedicada a sistemas de redes y **seguridad** fundada en 1996. Su sede principal está Sunnyvale, California.

Celestix Networks

- Fundada en 1999, ha entregado miles de soluciones de seguridad para empresas y organizaciones gubernamentales en todo el mundo. Celestix tiene su sede en Fremont, California, con oficinas en Singapur, Reading, Reino Unido, Chennai, India y otros países.

Cisco Systems

- Fundada en el año 1984 por un grupo pequeño de científicos de la Universidad de Stanford. Es una empresa que ofrece servicios y soluciones altamente demandadas en la industria, principalmente routing y switching, así como también en áreas como seguridad de redes, conectividad en el hogar, etc.

- Esta empresa ofrece una amplia gama de productos (Hardware) relacionados con la seguridad informática, entre los que se encuentran:

Control de Acceso Unificado

NSMXpress

Serie IDP (Detección y Prevención de Intrusiones)

Aplicaciones VPN SSL

Puertas de enlace integradas de alto rendimiento

Puertas de enlace de servicios

Sistemas de seguridad NetScreen

Series SSG

NSM Central Manager

Dispositive Security Threat Response Managers (STRM)

Control de acceso Unificado

- Su objetivo es proporcionar un control de acceso de invitados y socios basado en funciones, gestionar el uso de la red y reducir las amenazas que suponen los usuarios no autorizados y los dispositivos comprometidos.

Serie IDP (Detección y Prevención de Intrusiones

- Dispositivos de detección y prevención de intrusiones de IDP ofrecen protección de seguridad continua de la detección de intrusiones para redes empresariales.

Puertas de enlace integradas de alto rendimiento

- Diseñadas especialmente para ofrecer seguridad de aplicación y de red escalable a empresas grandes, redes portadoras y centros de datos.

Dispositivos de la serie NetScreen

- Proporciona seguridad de cortafuegos/VPN de alto rendimiento a redes de empresas grandes, portadoras y centros de datos.

Celestix Networks

- Entre los productos de seguridad que ofrece se encuentran:

Celestix MSA - Threat Management Gateway Series	Celestix WSA - Unified Access Gateway Series	Celestix HOTPin – Tokenless two-factor authentication
Celestix BSA - Unified Data Protection Series	Celestix XLB - Traffic Manager Series	Celestix BMC - BladeLogic Patch Manager

Celestix MSA - Threat Management Gateway Series

- MSA combinar filtrado web, antivirus, detección de intrusos, firewall de capa de aplicación, VPN IPSec, proxy, proxy inverso, ID / IP y más avanzado para la prevención de amenazas UTM con la industria y las mejores opciones en dispositivos Celestix para facilitar la implementación y gestión.

Celestix WSA - Unified Access Gateway Series

- Son las soluciones de seguridad integral y altamente configurable de conectividad para la publicación de aplicaciones empresariales. Basado en el sistema SSL VPN de Microsoft, los dispositivos WSA también son el mejor método para la gestión de DirectAccess y acceso remoto seguro a BPOS.

Celestix BSA - Unified Data Protection Series

- Asegura que los datos no pueden ser robados o perdidos desde el servidor o en el tránsito, y que los beneficiarios sólo se autoriza puede utilizar, modificar o ver archivos específicos.

Cisco Systems

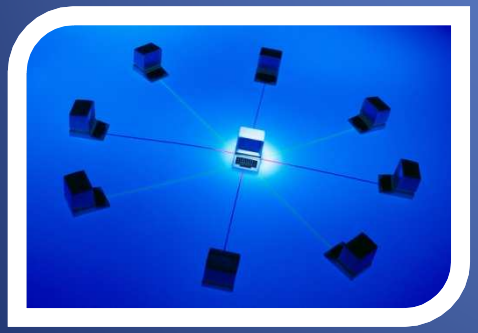
Cisco System ofrece distintos productos relacionados a la seguridad de la información, y los clasifica de la siguiente manera:

- **Seguridad de la red**
  - Dispositivos de seguridad adaptable de la serie Cisco ASA 5500
  - Sistema de prevención de intrusiones de Cisco
  - Seguridad integrada en la próxima generación de ISR

- **Seguridad de Correo Electrónico**
  - Dispositivos de seguridad de correo electrónico IronPort de Cisco
  - Servicios de seguridad del correo electrónico Cisco IronPort
  - Dispositivos de seguridad web IronPort de Cisco
  - Seguridad Web ScanSafe de Cisco

- **Administración de Seguridad**
  - Dispositivos de seguridad de correo electrónico IronPort de Cisco
  - Cisco Security Manager
  - Sistema de supervisión, análisis y respuesta de seguridad de Cisco

- **Control de Acceso Seguro**
  - Dispositivo de control de admisión a la red
  - Sistema de control de acceso seguro de Cisco



Dispositivos de seguridad adaptable de la serie Cisco ASA 5500

- Combina firewall, redes VPN, y seguridad de contenidos y prevención de intrusiones opcionales
- Brinda defensa contra amenazas y servicios de comunicación seguros para detener ataques
- Reduce los costos de implementación y operativos

Dispositivos de seguridad web IronPort de Cisco

- Integra controles de uso web, seguridad de datos, filtrado basado en la reputación y filtrado de software malicioso
- Aplica Cisco Security Intelligence Operations y tecnología de correlación de amenazas globales
- Combate sofisticadas amenazas basadas en la Web con tecnología de seguridad por capas

Dispositivo de control de admisión a la red

- Permitir el acceso sólo a dispositivos de confianza
- Bloquea el acceso por parte de dispositivos no conformes y limita el daño causado por riesgos y amenazas emergentes
- Protege las inversiones existentes mediante compatibilidad con aplicaciones de administración de terceros

En cuanto a software…

- Microsoft nos ofrece una alternativa de seguridad que implanta a nivel empresa, con el nombre de **Microsoft Forefront Security Suite,** la cual, es una solución integral de seguridad de infraestructura de TI que contiene:

Forefront Client Security

*Forefront Security para Exchange Server

*Forefront Security para SharePoint con Service Pack 1

*Forefront Security para Office Communications Server

Exchange Hosted Mail Filtering

Protección contra malware para escritorios comerciales, computadoras portátiles y sistemas operativos de servidor fácil de administrar y controlar

Productos de filtro de contenidos, antispam y antivirus de nivel de servidor que ayudan a las empresas a proteger sus entornos de colaboración y correo electrónico de virus, gusanos, spam y contenido inadecuado.

Servicio de filtro de mensajes que ayuda a proteger el correo electrónico entrante y saliente empresariales de spam, virus, fraudes de phishing y violaciones de políticas de correo electrónico.

Kaspersky: Estudio Global de Riesgos de Seguridad TI

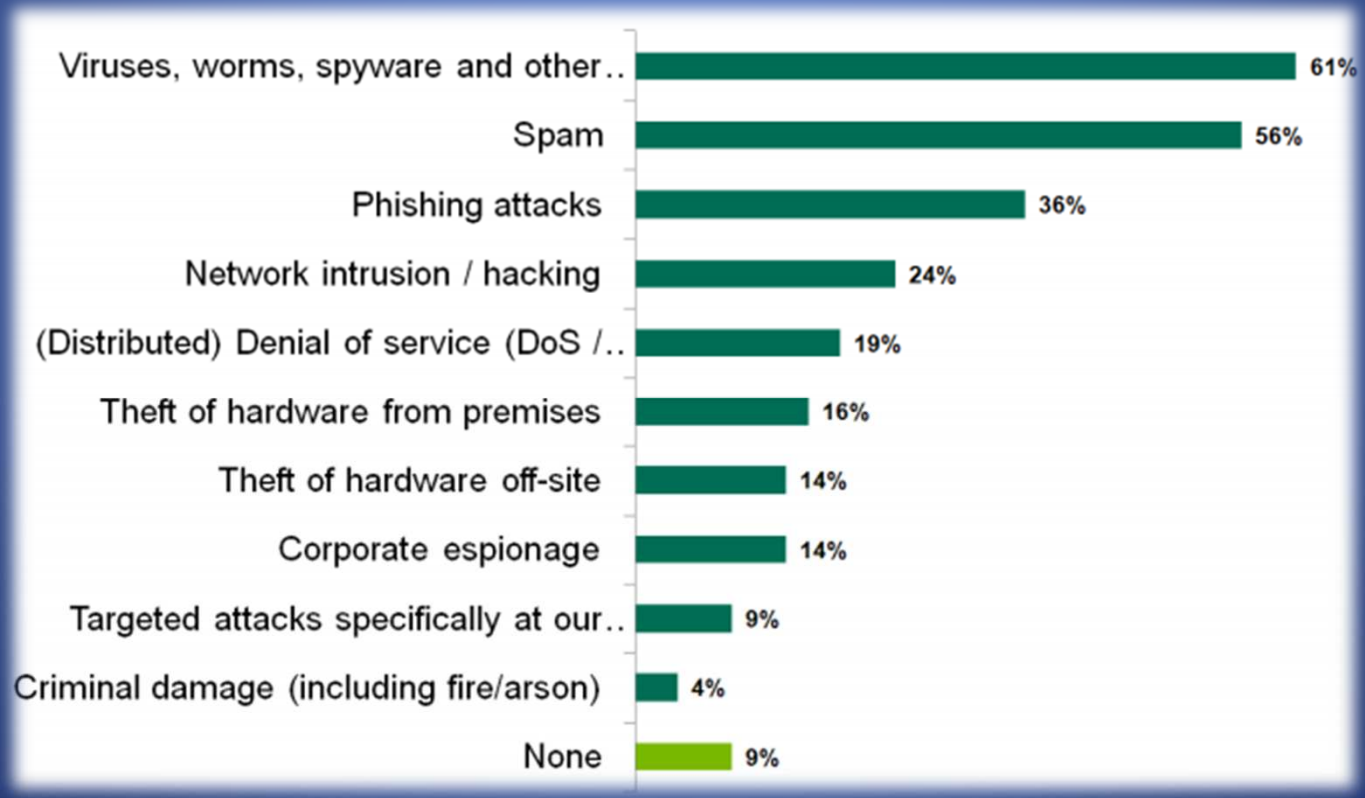
- En junio de este año (2011) Kaspersky publico este Estudio, que fue realizado en colaboración con B2B International y mas de 1300 profesionales de TI en 11 países(Alemania, Brasil, China, España, Estados Unidos, Francia, India, Italia, Japón, Reino Unido y Rusia).

Abarca desde pequeñas a grandes empresas.

Abarca una gama de temas relacionados con seguridad de TI

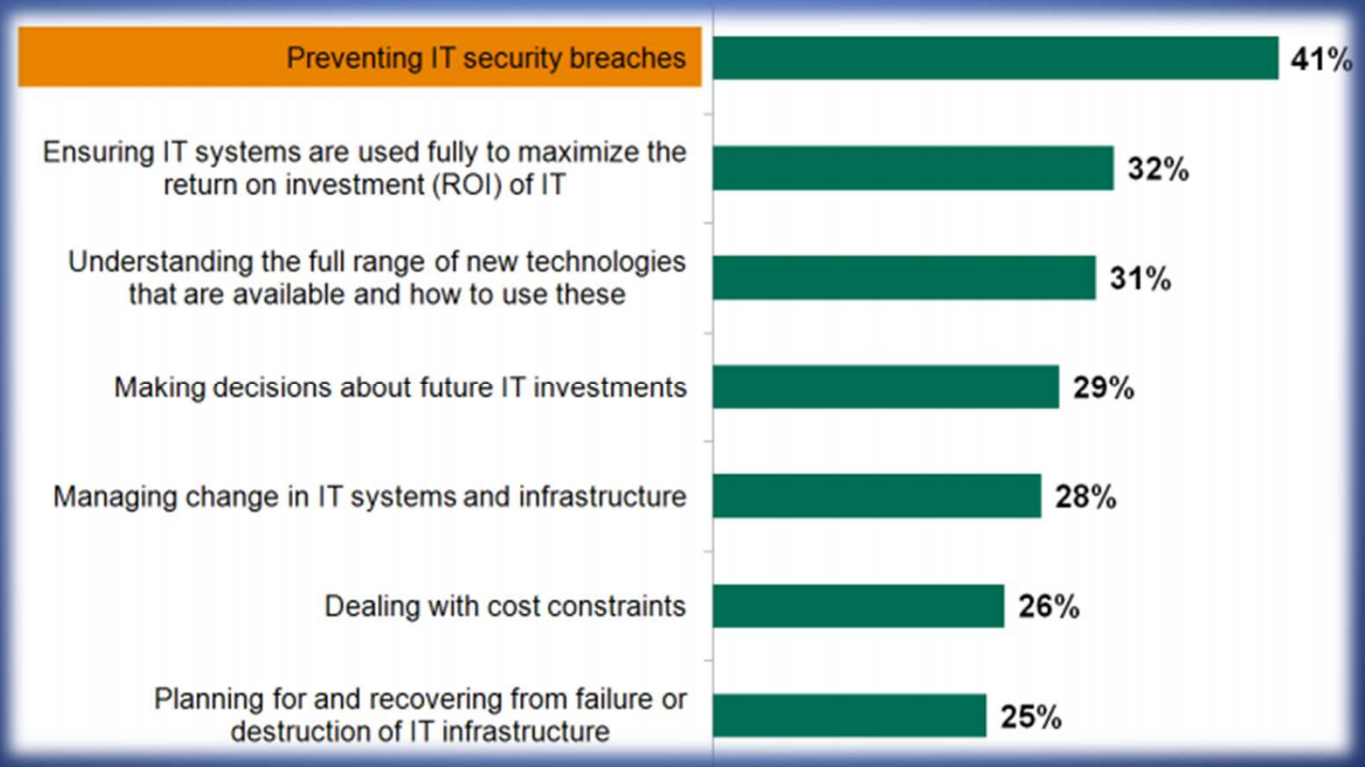
Riesgos del Negocio , medidas adoptadas para proteger en el negocio de TI y los incidentes ocurridos.

- Uno de los resultados más llamativos es que e**l 92% de las empresas españolas declara haber ha sufrido incidentes de seguridad procedentes de fuentes externas**. De ellos, un 55% ha tenido que enfrentarse a virus, gusanos, *spyware* y otro tipo de programas maliciosos, mientras que un 25% ha experimentado pérdida de datos (sensibles y no sensibles) debido a ataques de *malware*.



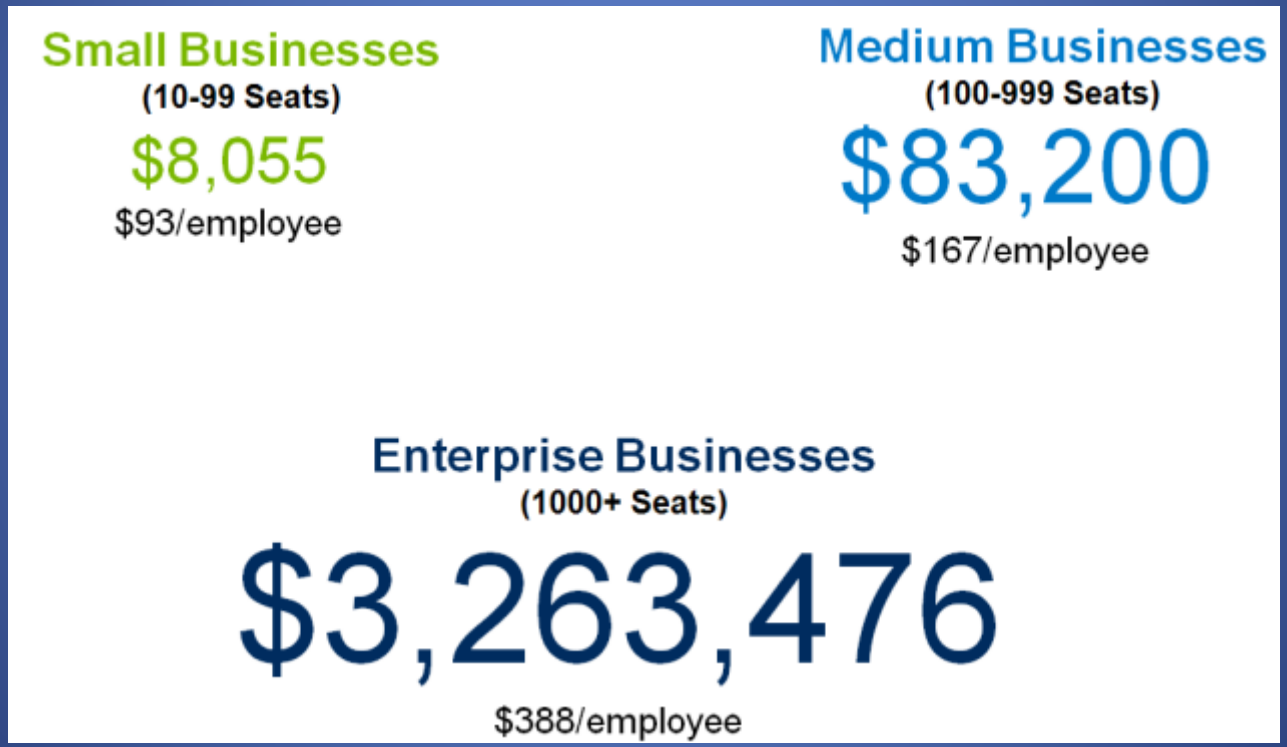
- FUTUROS RIESGOS

En lo referente a la percepción de los ciberataques, **el 30% de los expertos españoles considera que las amenazas en la red se cuentan entre los tres riesgos críticos para sus empresas**, y un 46% opina que en los próximos dos años se convertirán en una de las tres principales amenazas para el ámbito corporativo. El primer porcentaje es muy superior al de la media de los que comparten esta opinión en países desarrollados (un 13%) y en mercados en desarrollo (un 16%).



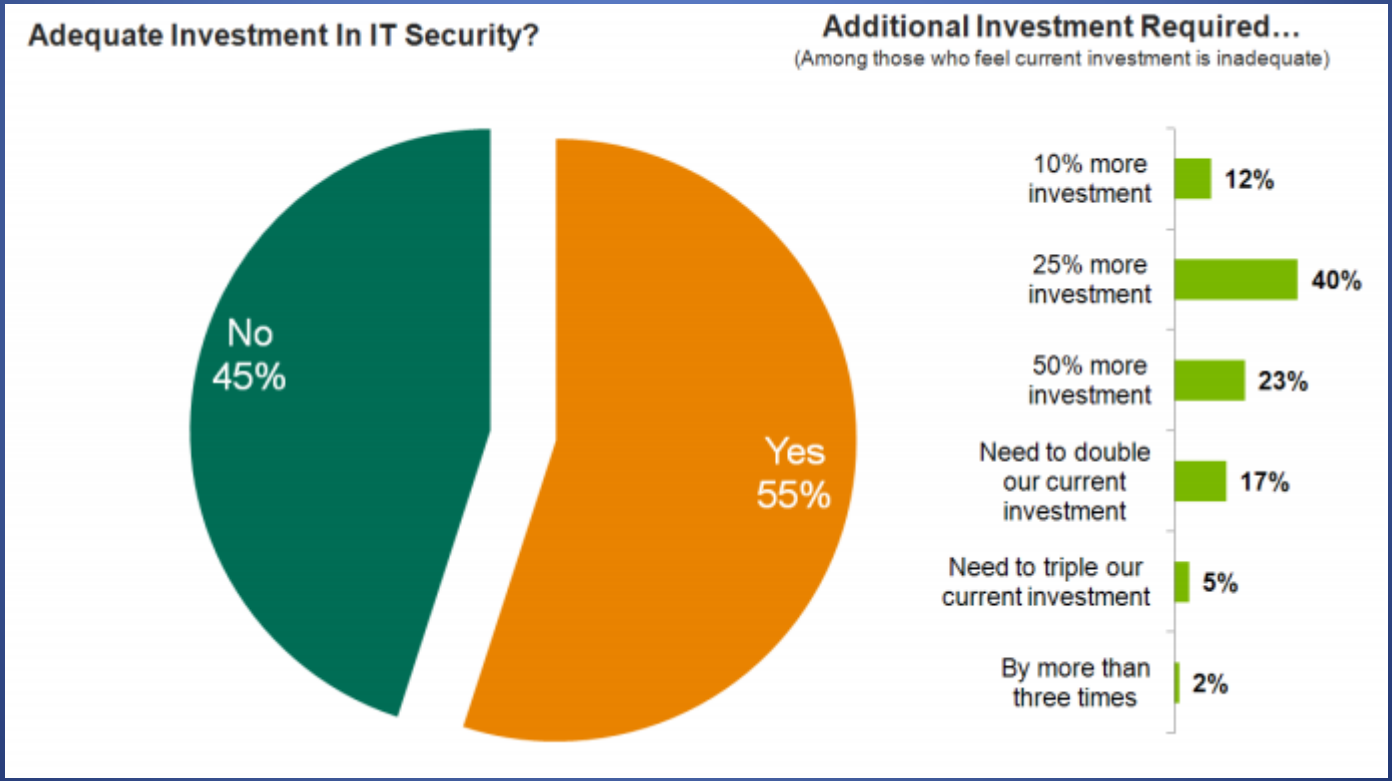
- INVERSION ANUAL

En lo que refiere a la inversión anual en seguridad informática, se registraron los siguientes valores por cada empleado:



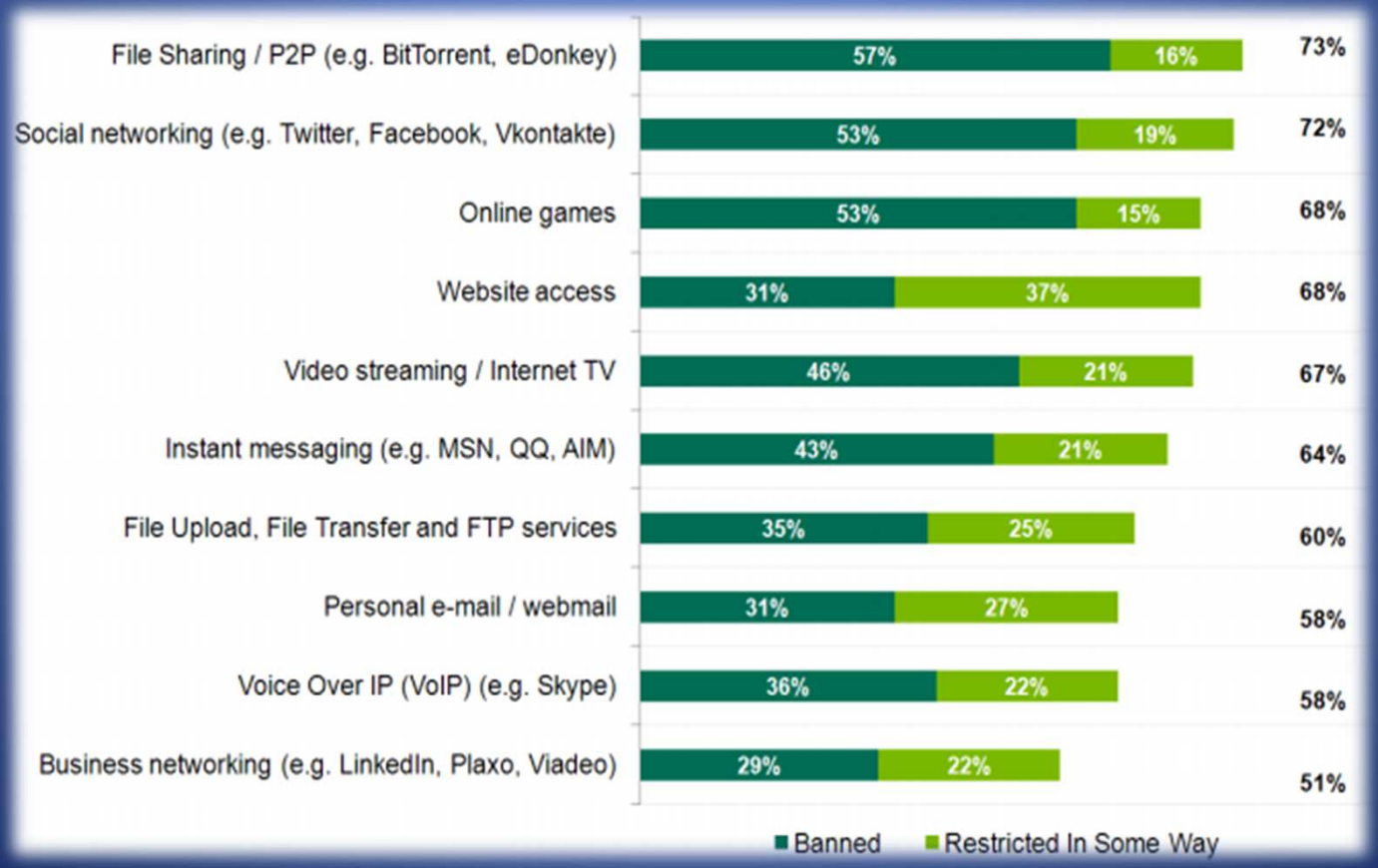
- Sin embargo, este estudio nos permite darnos cuenta que cerca del 55% de las empresas declararon tener una inversión adecuada en cuanto a seguridad informática.

- Por otro lado, de el 45% restante un 40% de estas empresas, piensa que es necesario invertir un 25 por ciento más de lo que se hace actualmente.



- ACTIVIDADES PROHIBIDAS O RESTRINGIDAS

Las empresas están pendientes de los nuevos medios, la mayoría de ellas ha prohibido o restringido de cierta manera, entre sus empleados, el uso de las redes sociales y ciertos sitios web; de esta manera que, aunque el intercambio y descarga de archivos sigue siendo la actividad más restringida, las redes sociales superan incluso juegos en línea, mensajería instantánea y la comunicación personal e-mail



El Estudio realizado por Kaspersky, nos permite darnos cuenta, de la importancia que tiene en la actualidad la Seguridad Informática, y también nos permitió conocer que hace falta una mayor inversión en este sector, ya que de el dependen, en gran medida, todas las empresas que utilizan de algún modo las TIC.

ISO 27000-02

¿Qué es?

Estándar para la seguridad de la información

British Standard BS 7799-1 (1995)

International Organization for Standardization (ISO/IEC 17799:2000)

Comisión Electrotécnica Internacional en el año 2000 ***"Information technology - Security techniques - Code of practice for information security management"***

ISO/IEC 17799:2005.

¿De que trata?

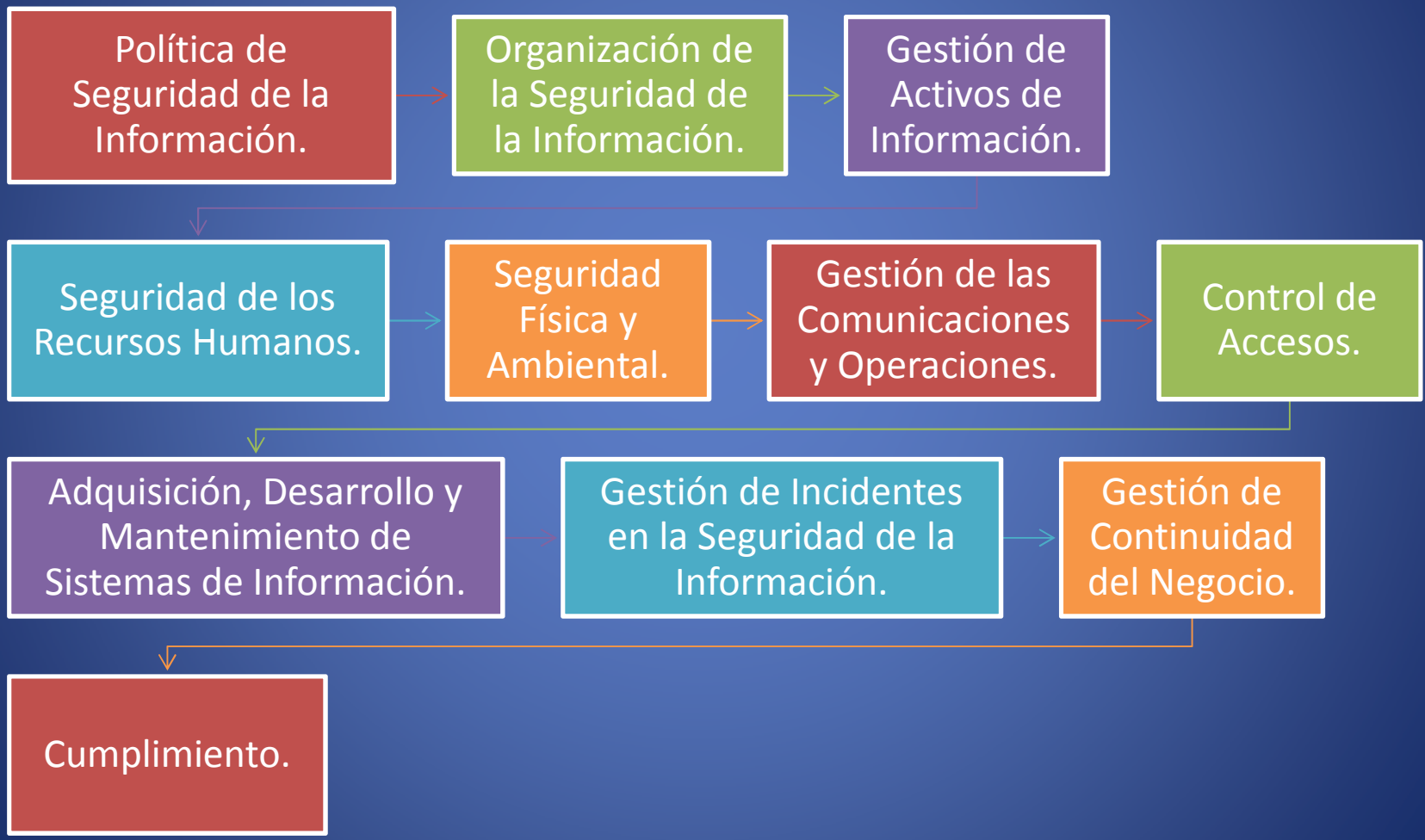
Recomendaciones

Mejores Prácticas en a gestión de la Seguridad de la Información

Iniciar, implantar o mantener sistemas de gestión de la Seguridad de la Información

ISO

Abarca temas como



Dentro de cada sección…

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información.

cada organización debe considerar cuales controles son aplicables según sus propias necesidades.

133 controles para las Seguridad de la Información

Para cada uno de los controles se indica asimismo una guía para su implantación.

Conclusiones

Es importante conocer toda la información posible sobre la seguridad informática ya que es un de la ramas de mayor intereses dentro de la informática, además de ser una de las mejor pagadas. El tener este tipo de conocimientos nos ayudará a tener un mayor conocimiento y lograr importantes puestos laborales.

CIBERGRAFIA

•http://books.google.com.mx/books?id=i6R5uhSeyOkC&pg=PA13&dq=seguridad+inform%C3%A1tica&hl=es&ei=z1u8TvJBsv-xAqHQgd0E&sa=X&oi=book_result&ct=result&resnum=4&ved=0CEYQ6AEwAw#v=onepage&q=seguridad%20inform%C3%A1tica&f=false

•http://es.wikipedia.org/wiki/ISO/IEC_17799

•http://www.juniper.net/us/en/products-services/security/

•http://www.celestix.com/index.php?option=com_content&view=article&id=43&Itemid=54&lang=en

•http://www.arubanetworks.com/products/

•http://www.microsoft.com/en-us/server-cloud/forefront/default.aspx

•http://www.computing.es/Tendencias/201110240018/SEGURIDAD-Kaspersky--Global-IT-Security-Risks-Study.aspx

•http://www.kaspersky.com/images/kaspersky_global_it_security_risks_survey-10-100468.pdf

GRACIAS