INSTITUTO URUGUAYO DE NORMAS TECNICAS

INSTITUTO URUGUAYO DE NORMAS TECNICAS

Implantación y Certificación de un Sistema de Gestión de Seguridad de la Información (SGSI)

JIAP 2011

Gabriel Fernández
unit-iso@unit.org.uy

INSTITUTO URUGUAYO DE NORMAS TECNICAS

AGENDA

- CONCEPTO DE SEGURIDAD DE LA INFORMACIÓN
- SEGURIDAD DE LA INFORMACIÓN - MOTIVACIÓN
- FAMILIA DE NORMAS UNIT-ISO/IEC 27000
- UNIT-ISO/IEC 27001 – REQUISITOS PARA UN SGSI
- MAPA DE RUTA PARA LA IMPLANTACIÓN DE UN SGSI
- FACTORES CRÍTICOS DE ÉXITO
- CERTIFICACIÓN DE UN SGSI

INSTITUTO URUGUAYO DE NORMAS TECNICAS

ACTIVIDADES DE UNIT
EN BENEFICIO DE LA COMUNIDAD

NORMALIZACION
INIC:1939 2500 NORMAS

INFORMACION
INIC:1939 350.000 – 2 000 000 NORMAS

CAPACITACION
INIC:1971 65.000 PARTIC.

CERTIFICACION DE PRODUCTOS
INIC:1984 1700 PROD.

PROMOCION Y MEJORAMIENTO DE LA CALIDAD

DIVULGACION
PUBLICACIONES –CONGRESOS - -----

CERTIFICACION DE SISTEMAS
INIC:1995 400 CERT.

MIEMBRO DE:

OHSAS OCCUPATIONAL HEALTH AND SAFETY ASSESSMENT SERIES

COMISION PANAMERICANA DE NORMAS TECNICAS

ISO ORGANIZACION INTERNACIONAL DE NORMALIZACION

IEC COMISION ELECTROTECNICA INTERNACIONAL

ASOCIACION MERCOSUR DE NORMALIZACION

INSTITUTO URUGUAYO DE NORMAS TECNICAS

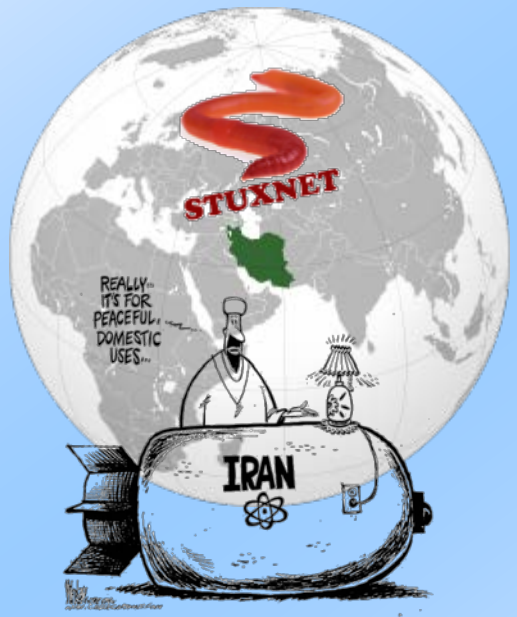
CONCEPTO DE SEGURIDAD DE LA INFORMACIÓN

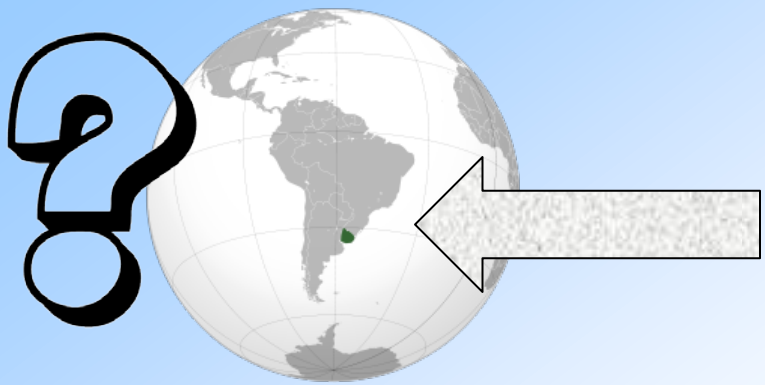
- ¿QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?

http://moplincom.moplin.com/wp-content/uploads/2009/08/joke-redes1.jpg

INSTITUTO URUGUAYO DE NORMAS TECNICAS

Seguridad de la Información
Motivación – Ataques Objetivos





INSTITUTO URUGUAYO DE NORMAS TECNICAS

Seguridad de la Información
Motivación – Ataques Objetivos

despejado | 13ºC

EL PAIS

Inicio | Último Momento | Edición Impresa | Ediciones

Información | Opinión | Deportes | Suplementos | Servicios | Ocio

Los Premios iris Al Espectáculo Uruguayo — Votá a tu favorito aquí

Vota por esta noticia: ★★★★★ Total de votos: ★★★★★ 4 votos — Comentarios: 6

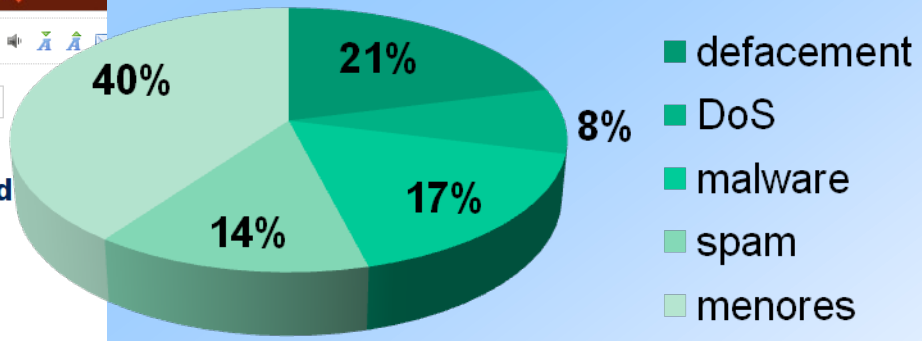
Descargar Archivo Audio MP3

Nacional

Ejecutivo apunta a reforzar su seguridad informática

Ataques. En 2010 se registraron 23 episodios de riesgo alto

Incidentes de alto riesgo 2010
(fuente CERTUy)



Infiltrado en Antel usó costoso equipo para simular voz de Jorge Vázquez

Citaciones. Investigarán a asesores y adscrip

La utilización de un sofisticado maletín de US$ 300 suponer a integrantes del gobierno que se trata d del Poder Ejecutivo.

Se trata de un modificador de voz que le permitió Carvalho y con un ex asesor de Gabriel Perera sin Jorge Vázquez.

Para el gobierno la tesis de que Román solo busc elemento tan sofisticado que no podía ser financia que haber algo atrás", señaló una fuente. La jueza pudo haber hecho solo dicha maniobra.

Autoridades gubernamentales aguardan que en e extiendan a otros funcionarios y asesores de Ante Edgardo Carvalho y la vicepresidente Gladys Urar qué preguntas les formulaba Román. De esa form

011 todos los
l informática

OBSERVA

Home | Actualidad | Economía | Internacionales | Deportes | Vida | Ciencia y Tecnología | Agro

Servicios | Ciudadano | Universitario | Clasificados | El Tiempo | El Observador | Cinemag | Publicidad | Especiales

POLICIAL

Recuperan maletín del ministro Rossi

La Policía desbarató una banda dedicada al robo y desguace de automóviles y en el procedimiento encontraron el portafolio que el secretario de Estado perdió cuando le hurtaron su camioneta

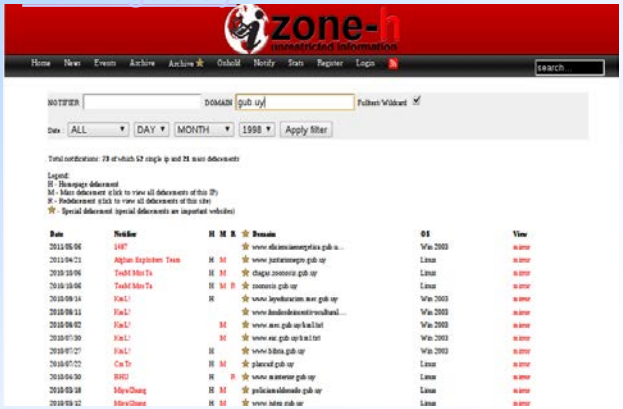
Twittear 0 Me gusta

El Departamento de Automotores de la jefatura de Policía de Montevideo desbarató una banda dedicada al robo y desguace de automóviles.

Durante el fin de semana se realizaron varios procedimientos los que permitieron descubrir el aguantadero de la banda, se encontraron seis vehículos y como consecuencia de las actuaciones, la Justicia Penal procesó a cuatro delincuentes y a dos policías, uno de ellos un Comisario con funciones en Jefatura de Montevideo vinculado a la organización delictiva.

Tras los allanamientos, los policías de Automotores recuperaron también un portafolios y tras las pericias, se confirmó que el mismo pertenece al ministro de Transporte y Obras Públicas Víctor Rossi, quien además lo reconoció como propio.

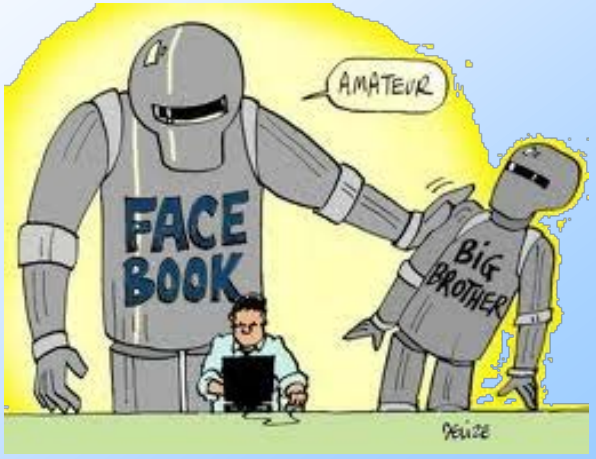
http://www.zone-h.org/archive/filter=1/fulltext=1/domain=gub.uy



INSTITUTO URUGUAYO DE NORMAS TECNICAS

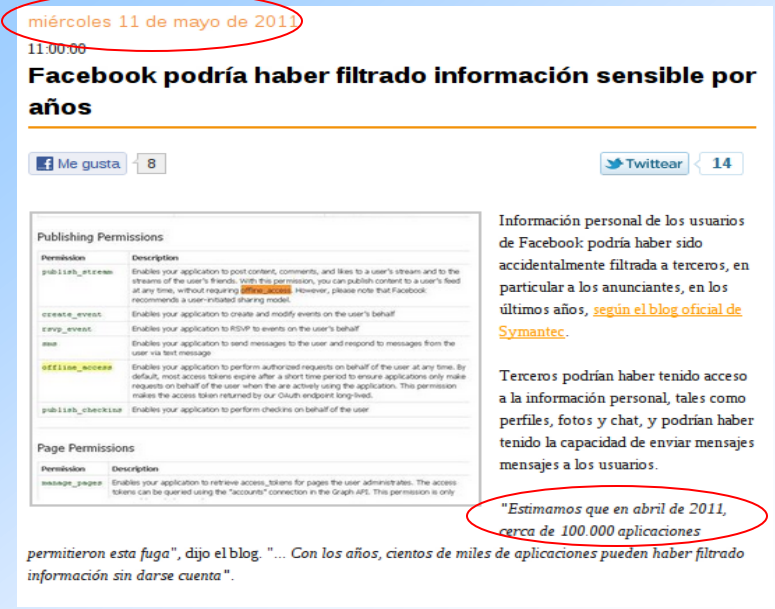
Seguridad de la Información

Redes Sociales + Ing. Social = Compromiso



"Se recomienda el estudio de la protección de los individuos y de las naciones ante el progreso de las técnicas y el registro de las comunicaciones ya que el uso de la electrónica podría intervenir en los derechos fundamentales, como el honor y la intimidad"

Naciones Unidas, Resolución 2450 ,19 de diciembre de 1968



miércoles 11 de mayo de 2011

11:00:00

Facebook podría haber filtrado información sensible por años

Me gusta 8 Twittear 14

Publishing Permissions

Permission	Description
publish_stream	Enables your application to post content, comments, and likes to a user's stream and to the streams of the user's friends. With this permission, you can publish content to a user's feed at any time, without requiring offline_access. However, please note that Facebook recommends a user-initiated sharing model.
create_event	Enables your application to create and modify events on the user's behalf
rsvp_event	Enables your application to RSVP to events on the user's behalf
sms	Enables your application to send messages to the user and respond to messages from the user via text message
offline_access	Enables your application to perform authorized requests on behalf of the user at any time. By default, most access tokens expire after a short time period to ensure applications only make requests on behalf of the user when the are actively using the application. This permission makes the access token returned by our OAuth endpoint long-lived.
publish_checkins	Enables your application to perform checkins on behalf of the user

Page Permissions

Permission	Description
manage_pages	Enables your application to retrieve access_tokens for pages the user administrates. The access tokens can be queried using the "accounts" connection in the Graph API. This permission is only

Información personal de los usuarios de Facebook podría haber sido accidentalmente filtrada a terceros, en particular a los anunciantes, en los últimos años, según el blog oficial de Symantec.

Terceros podrían haber tenido acceso a la información personal, tales como perfiles, fotos y chat, y podrían haber tenido la capacidad de enviar mensajes mensajes a los usuarios.

"Estimamos que en abril de 2011, cerca de 100.000 aplicaciones permitieron esta fuga", dijo el blog. *"... Con los años, cientos de miles de aplicaciones pueden haber filtrado información sin darse cuenta"*.

INSTITUTO URUGUAYO DE NORMAS TECNICAS

Seguridad de la Información

Motivación - Económica

Venta de productos de forma ilegal

2011-05-13

Phishing

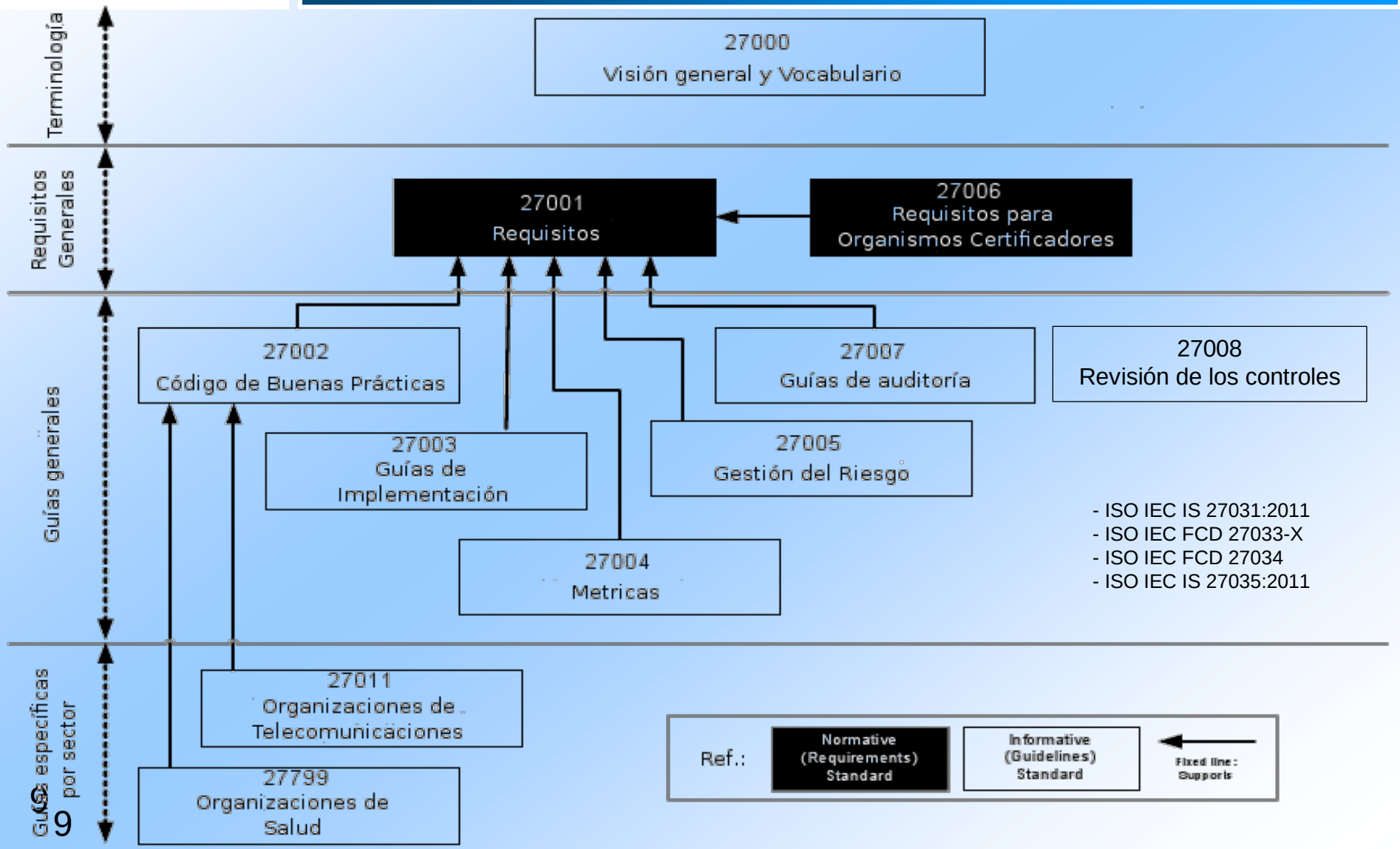
Fuga de información comercial

2011-04-28

3.778 clic hacia el sitio falso + 13% de los usuarios ingresa sus datos por estadísticas = más de 400 cuentas vulneradas

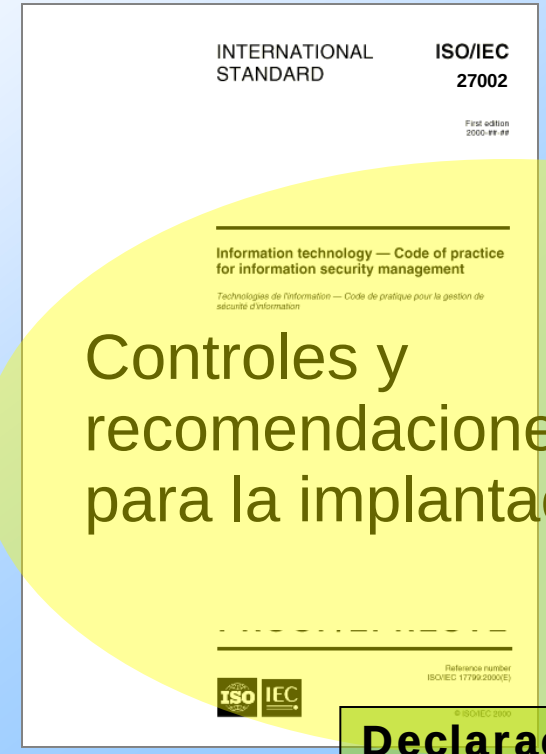
INSTITUTO URUGUAYO DE NORMAS TECNICAS

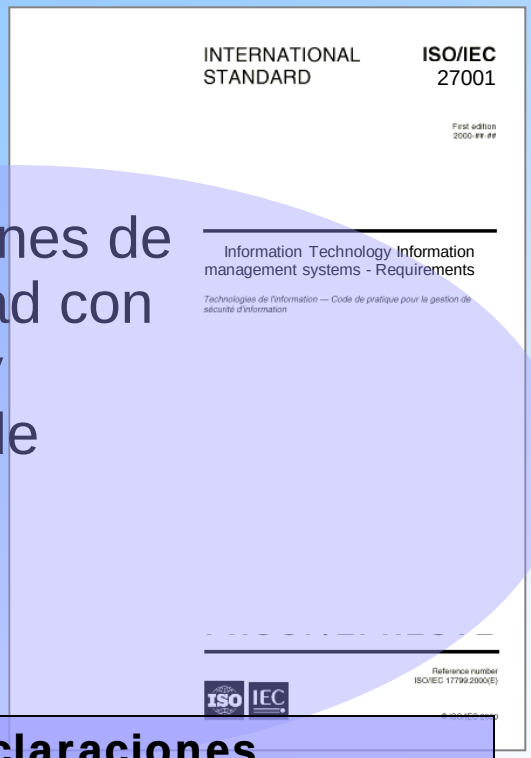
FAMILIA DE NORMAS UNIT-ISO/IEC 27000



INSTITUTO URUGUAYO DE NORMAS TECNICAS

UNIT-ISO/IEC 27002 & UNIT-ISO/IEC 27001





Controles y recomendaciones para la implantación

Controles

Declaraciones de conformidad con procesos y controles de seguridad

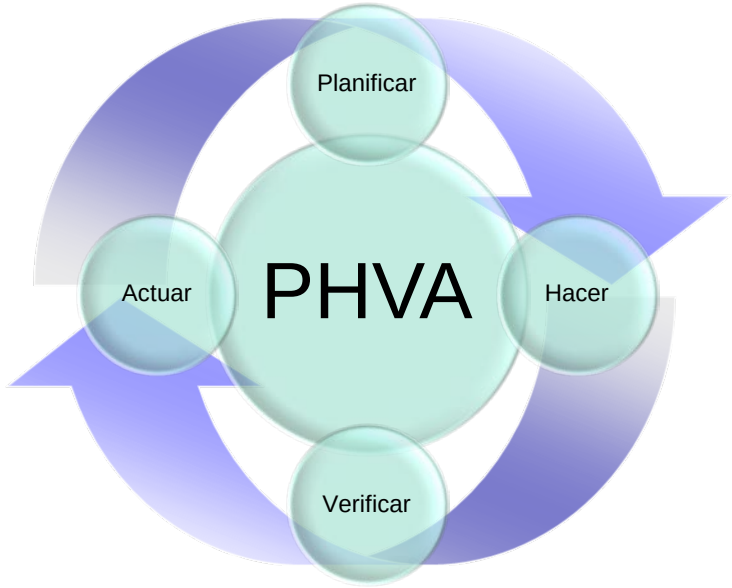
Declaraciones NO Obligatorias

Declaraciones Obligatorias

INSTITUTO URUGUAYO DE NORMAS TECNICAS

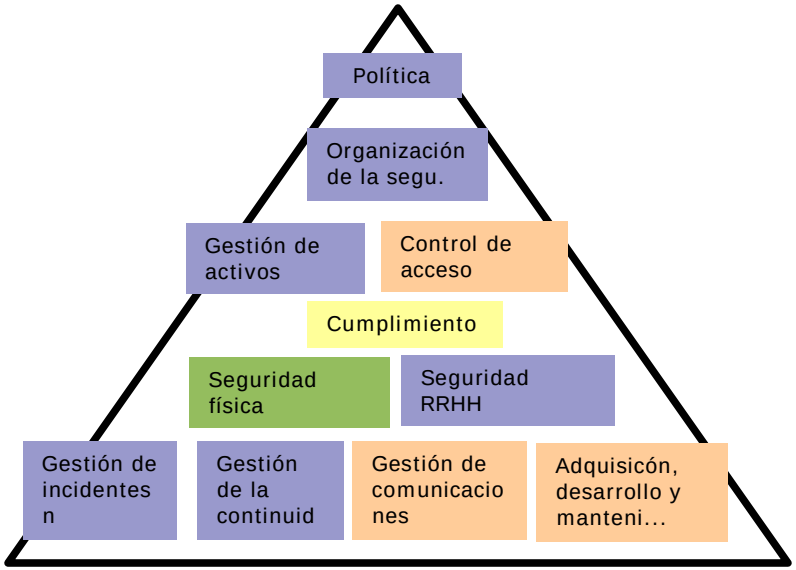
UNIT-ISO/IEC 27001:2005 Requisitos

REQUISITOS DEL SGSI



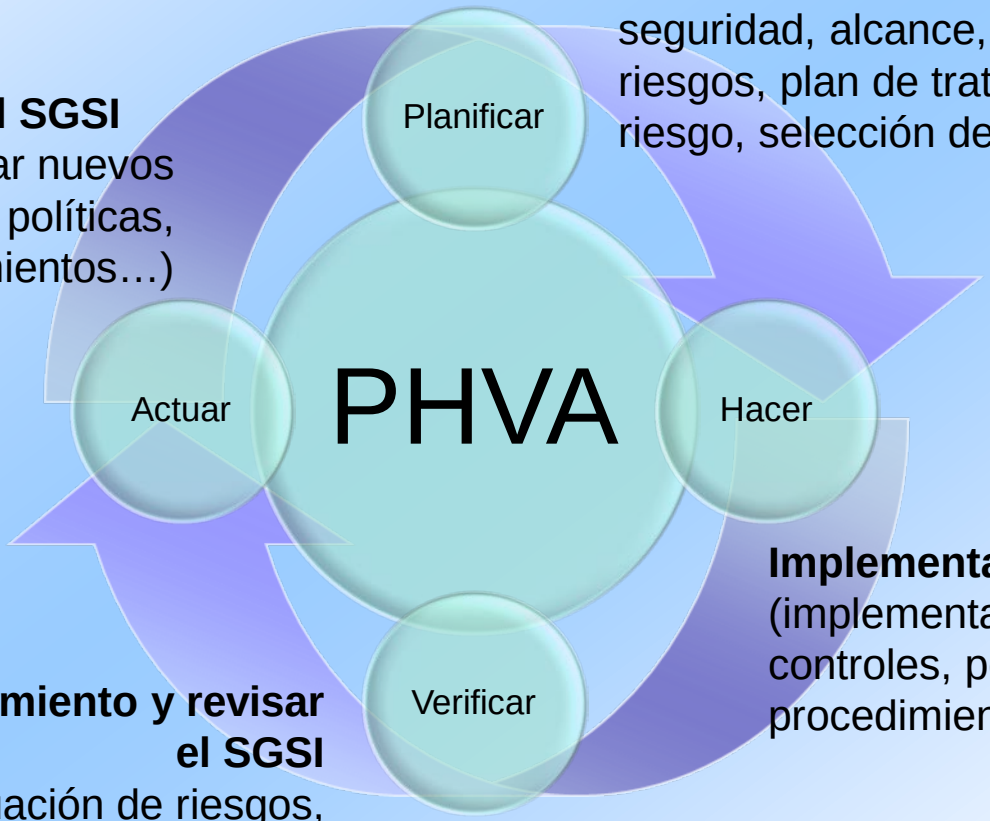
+ Control de la Documentación
+ Responsabilidad de la Dirección
+ Auditorías internas
+ Revisión por la Dirección
+ Mejora

ANEXO A CONTROLES



Modelo PDCA aplicado a los procesos de SGSI

Establecer el SGSI(política de seguridad, alcance, evaluación de riesgos, plan de tratamiento del riesgo, selección de controles…)



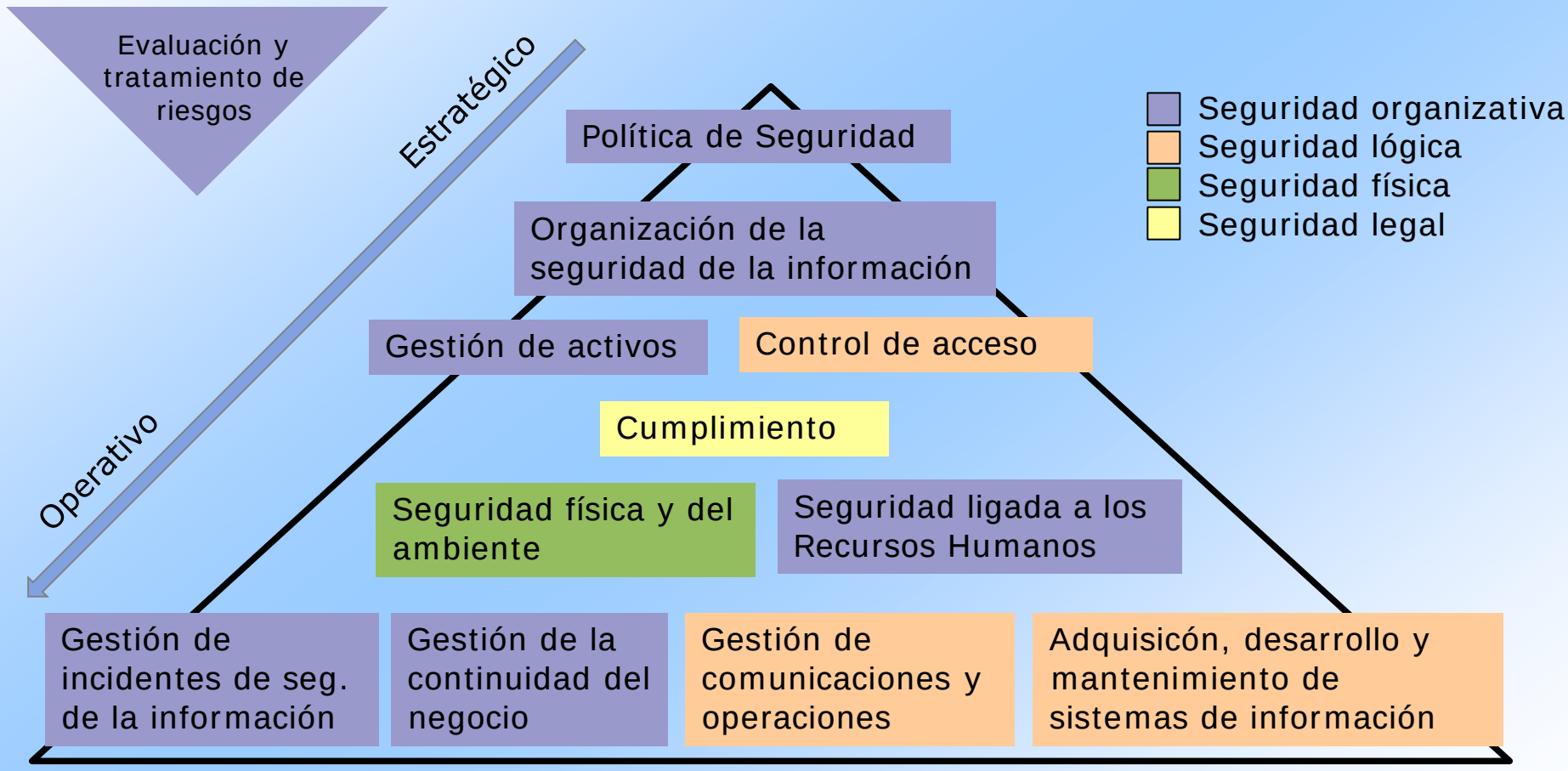
Mantener y Mejorar el SGSI (Mejorar o implementar nuevos controles, políticas, procedimientos…)

Implementar y operar el SGSI (implementar y verificar los controles, políticas, procedimientos, procesos…)

Hacer el seguimiento y revisar el SGSI (reevaluación de riesgos, revisión por la dirección, auditorías…)

INSTITUTO URUGUAYO DE NORMAS TECNICAS

UNIT-ISO/IEC 27001
CONTROLES: DOMINIOS



INSTITUTO URUGUAYO DE NORMAS TECNICAS

MAPA DE RUTA PARA LA IMPLANTACIÓN DE UN SGSI

Iniciación del Proyecto

- Definición SGSI
- Evaluación de riesgos
- Tratamiento de riesgos
- Concientización y formación
- Prepararse para la auditoría
- Auditoría
- Mejora continua

- **Adquirir las normas**
- **Asegurar el compromiso de la dirección.**
- **Seleccionar y entrenar los miembros del comité de seguridad**

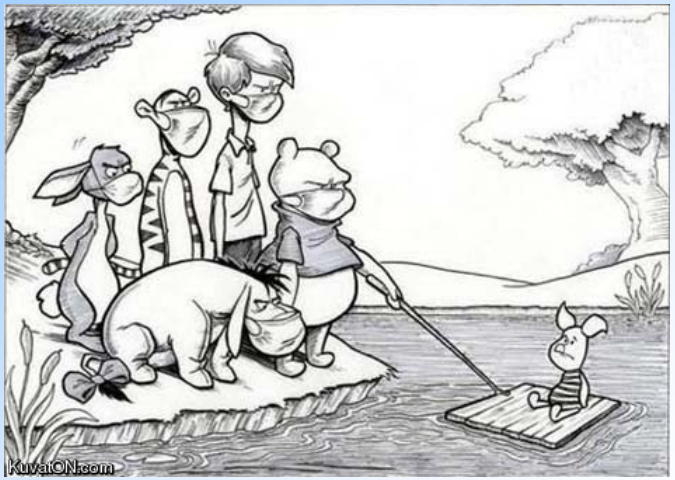
INSTITUTO URUGUAYO DE NORMAS TECNICAS

MAPA DE RUTA PARA LA IMPLANTACIÓN DE UN SGSI

- Iniciación del Proyecto
- **Definición SGSI**
- Evaluación de riesgos
- Tratamiento de riesgos
- Concientización y formación
- Prepararse para la auditoría
- Auditoría
- Mejora continua

Para definir el SGSI, se debe identificar claramente:

- Objetivo
  - Alcance
  - Límites
  - Interfaces
  - Dependencias
  - Exclusiones y justificaciones
  - Estrategia
  - Contexto organizacional



Fiebre Porcina

INSTITUTO URUGUAYO DE NORMAS TECNICAS

MAPA DE RUTA PARA LA IMPLANTACIÓN DE UN SGSI

- Iniciación del Proyecto
- Definición SGSI
- **Evaluación de riesgos**
- Tratamiento de riesgos
- Concientización y formación
- Prepararse para la auditoría
- Auditoría
- Mejora continua

- **Medir el cumplimiento de los controles de la UNIT-ISO/IEC 27001 (Análisis GAP)**
- **Identificación y evaluación de activos**
- **Identificación y Evaluación de Amenazas y Vulnerabilidades**

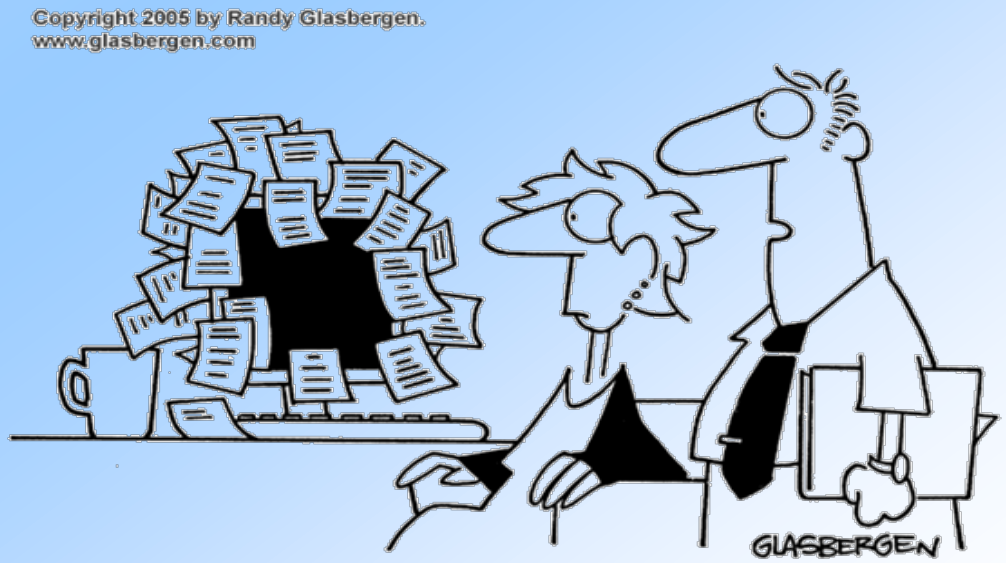
Mis 35 años de experiencia me dicen que su tolerancia al riesgo es baja

INSTITUTO URUGUAYO DE NORMAS TECNICAS

MAPA DE RUTA PARA LA IMPLANTACIÓN DE UN SGSI

- Iniciación del Proyecto
- Definición SGSI
- Evaluación de riesgos
- **Tratamiento de riesgos**
- Concientización y formación
- Prepararse para la auditoría
- Auditoría
- Mejora continua

- **Opciones para el tratamiento del riesgo**
- **Selección de controles**
- **Plan de tratamiento de riesgos**
- **Implementación de controles**



Nosotros respaldamos nuestra información en stickys porque nunca se cuelgan

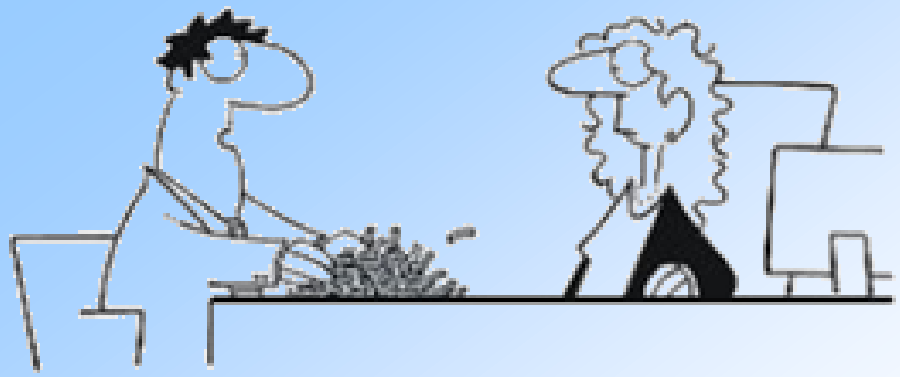
INSTITUTO URUGUAYO DE NORMAS TECNICAS

MAPA DE RUTA PARA LA IMPLANTACIÓN DE UN SGSI

- Iniciación del Proyecto
- Definición SGSI
- Evaluación de riesgos
- Tratamiento de riesgos
- **Concientización y formación**
- Prepararse para la auditoría
- Auditoría
- Mejora continua

Construyendo conciencia y entrenando:

- Definir responsabilidades en materia de SI;
- Proporcionar el entrenamiento apropiado;
- Evaluar la eficacia del entrenamiento proporcionado y de las acciones emprendidas;



"Me estoy postulando para el trabajo de Seguridad informática. Aquí tiene mi CV codificado, encriptado y rallado."

INSTITUTO URUGUAYO DE NORMAS TECNICAS

MAPA DE RUTA PARA LA IMPLANTACIÓN DE UN SGSI

- Iniciación del Proyecto
- Definición SGSI
- Evaluación de riesgos
- Tratamiento de riesgos
- Concientización y formación
- **Prepararse para la auditoría**
- Auditoría
- Mejora continua

- **Finalizar las exigencias de documentación del SGSI**
- **Algunos cubren la Gestión y la operación continua del SGSI, mientras que otros se desarrollan para implementar controles.**
  - Procedimientos exigidos
  - Declaración de aplicabilidad
  - Otros documentos vinculados a los controles

INSTITUTO URUGUAYO DE NORMAS TECNICAS

MAPA DE RUTA PARA LA IMPLANTACIÓN DE UN SGSI

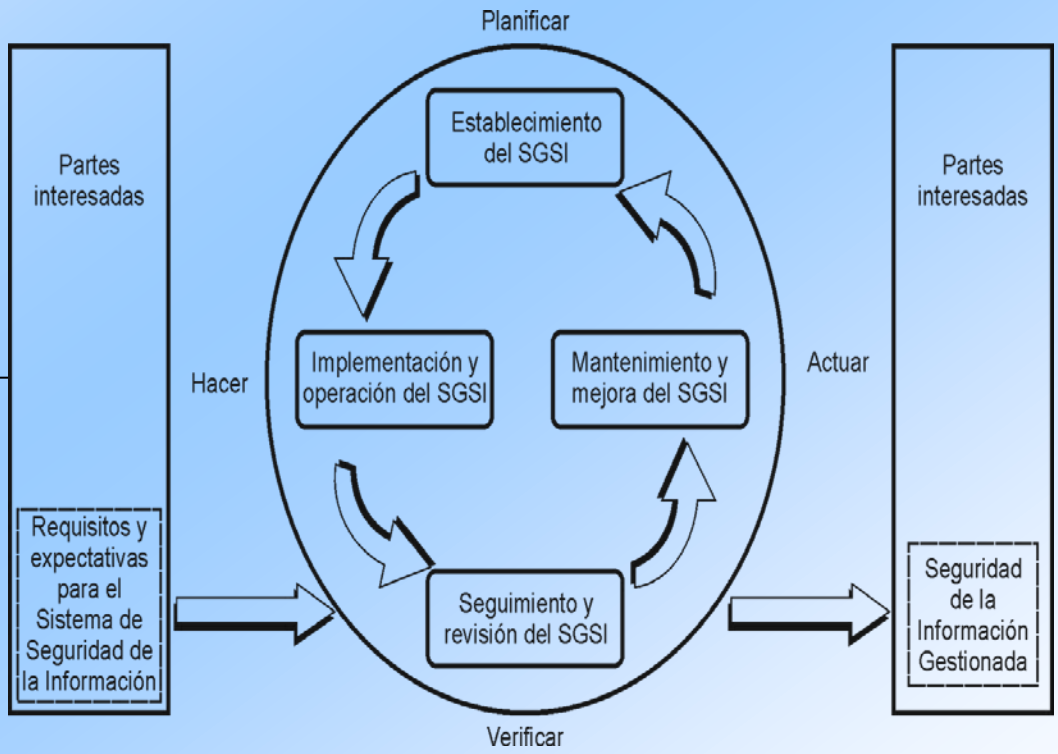
- Iniciación del Proyecto
- Definición SGSI
- Evaluación de riesgos
- Tratamiento de riesgos
- Concientización y formación
- Prepararse para la auditoría
- **Auditoría**
- Mejora continua

- **Auditoría interna:**
  - proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios

INSTITUTO URUGUAYO DE NORMAS TECNICAS

MAPA DE RUTA PARA LA IMPLANTACIÓN DE UN SGSI

- Iniciación del Proyecto
- Definición SGSI
- Evaluación de riesgos
- Tratamiento de riesgos
- Concientización y formación
- Prepararse para la auditoría
- Auditoría
- **Mejora continua**



INSTITUTO URUGUAYO DE NORMAS TECNICAS

FACTORES CRÍTICOS DE ÉXITO

- **El apoyo visible y el compromiso evidente de la alta dirección**
  - **Asignación de recursos económicos y en especial humanos.**
  - **Concientización de los mandos medios.**
- **Un alcance, política y objetivos que reflejen los objetivos del negocio.**
  - **Alinear el SGSI con el negocio.**
- **Ser consciente del esfuerzo permanente que se requiere.**
  - **RRHH.**

INSTITUTO URUGUAYO DE NORMAS TECNICAS

FACTORES CRÍTICOS DE ÉXITO

- **La adecuada capacitación y permanente concientización del personal.**
- **Un sistema de gestión de incidentes que permita centralizar el registro y seguimiento de los eventos e incidentes de seguridad.**
- **Un sistema de estimulo al reporte de eventos e incidentes.**

INSTITUTO URUGUAYO DE NORMAS TECNICAS

FACTORES CRÍTICOS DE ÉXITO

- **Un sistema integrado de indicadores que permita evaluar la eficacia de los controles y procesos implementados.**

- **Herramientas de gestión de permita centralizar el registro y seguimiento de diferentes procesos y controles.**

- **Herramientas de gestión de la documentación y los registros.**

INSTITUTO URUGUAYO DE NORMAS TECNICAS

HERRAMIENTAS DE GESTIÓN

- **http://www.iso27000.es/herramientas.html**

- **https://www.e-pulpo.es**

- **www.ossim.net**

KnowledgeTree

ProcessMaker Workflow Simplified

OrangeHRM NEW LEVEL OF HR MANAGEMENT

INSTITUTO URUGUAYO DE NORMAS TECNICAS

CERTIFICACION
Demostrando Conformidad

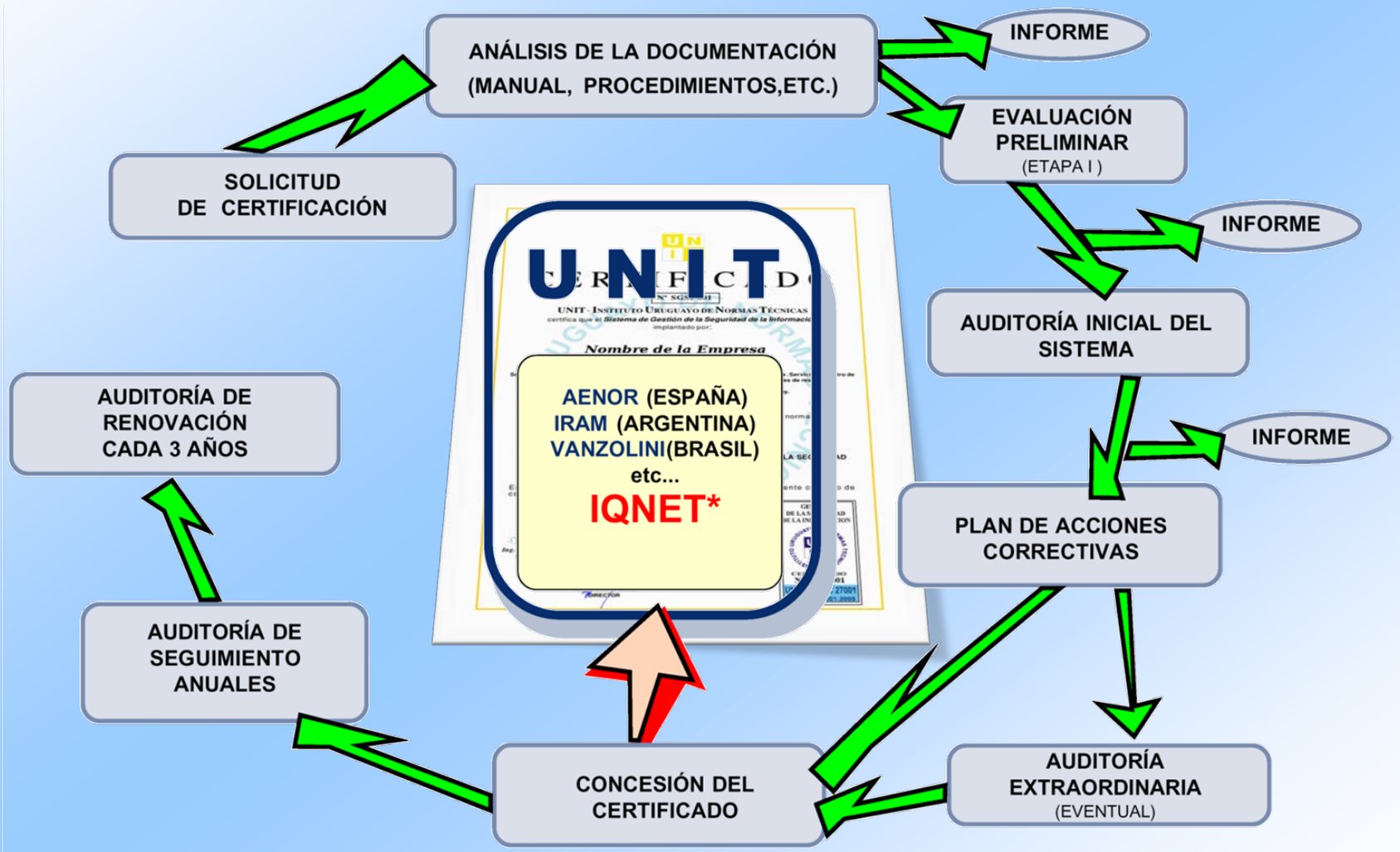
ATESTACIÓN, REALIZADA POR UNA TERCERA PARTE, RELATIVA A PRODUCTOS, PROCESOS, SISTEMAS O PERSONAS

UNIT-ISO/IEC 17000:2005 (Apartado 5.5)

http://cartoonando.blogspot.com/

INSTITUTO URUGUAYO DE NORMAS TECNICAS

PROCESO DE CERTIFICACIÓN DE UNIT



INSTITUTO URUGUAYO
DE NORMAS TECNICAS

INSTITUTO URUGUAYO DE NORMAS TECNICAS

MUCHAS GRACIAS POR SU ATENCIÓN