Actividad 3: Herramientas para el análisis de riesgos

Seguridad Informática

09/10/2014

Brais López Yáñez

CONTENIDO

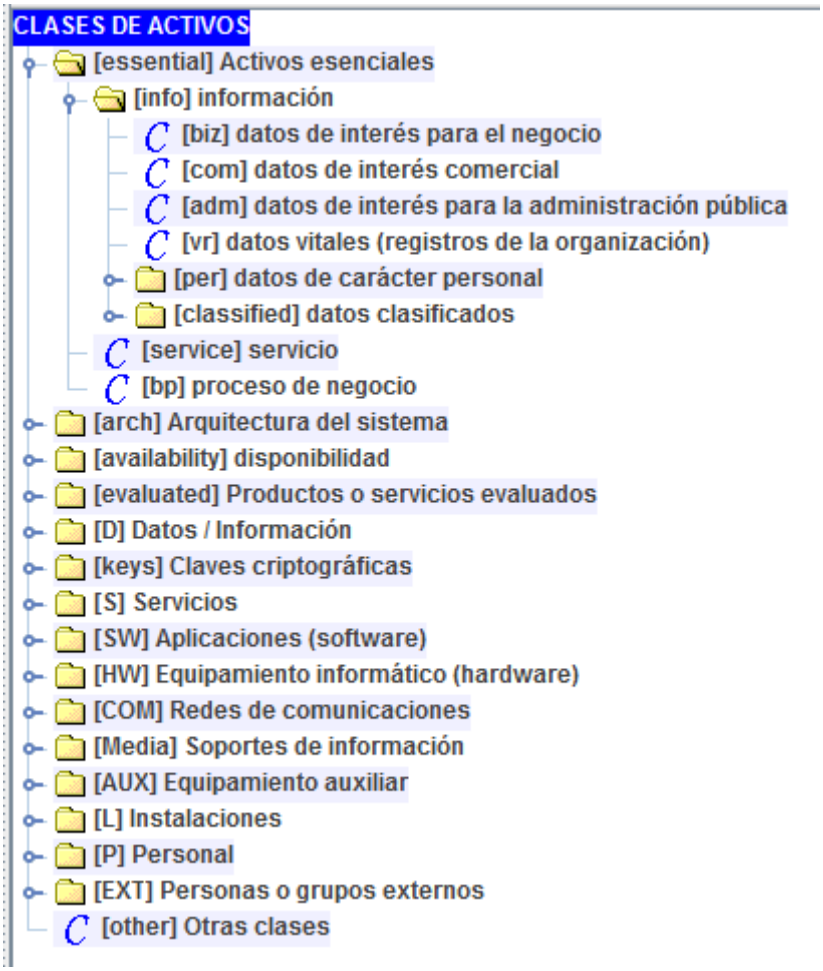
PRIMERA PARTE: HERRAMIENTA PILAR

EXPLORACIÓN DE LOS DISTINTOS TIPOS DE ACTIVOS.

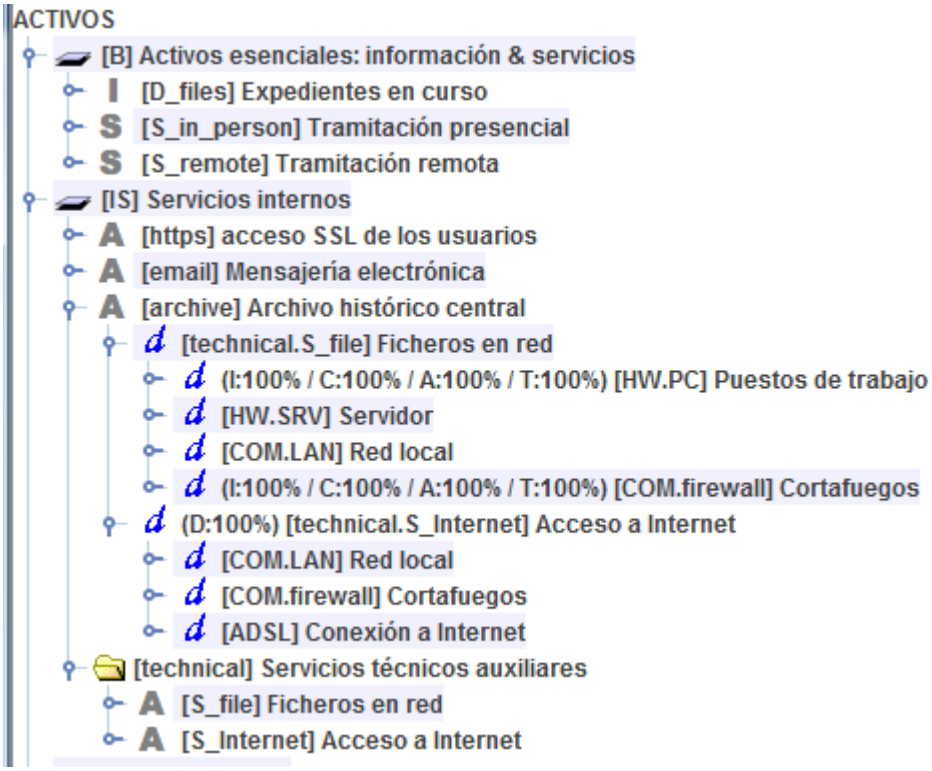
Anotación de algunos (al menos 5) ejemplos de cada apartado. Localización a qué activos afectan los errores de usuario y a qué activos afecta el fuego. Localización de amenazas que afecten a los datos de los usuarios, y amenazas que afecten al procesado de datos. Identificación de alguna de las amenazas con mayor impacto.

Activos: lista de recursos para conseguir un determinado objetivo.

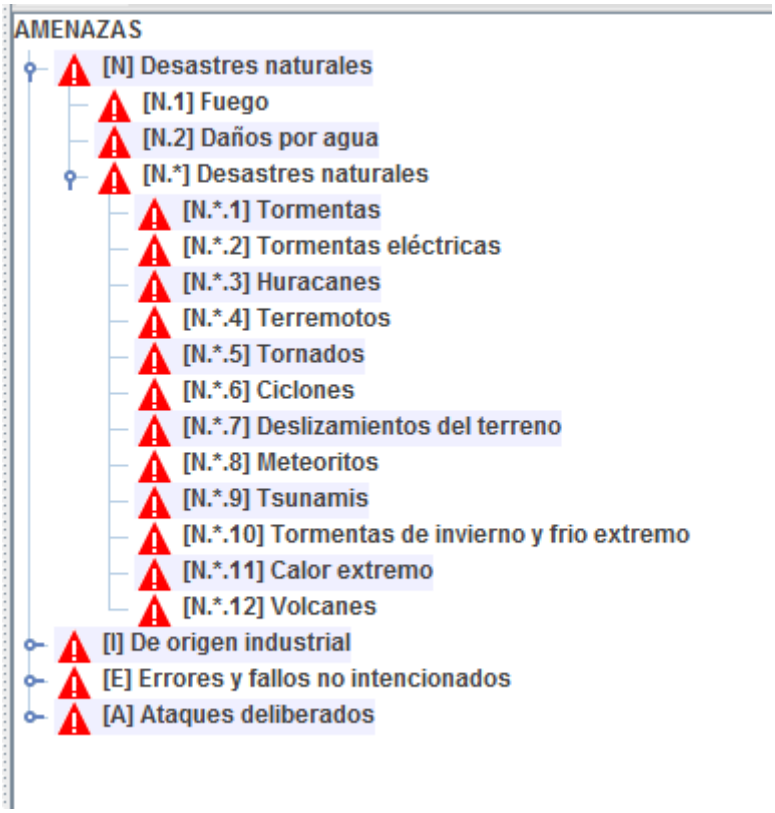
Tipos de activos:



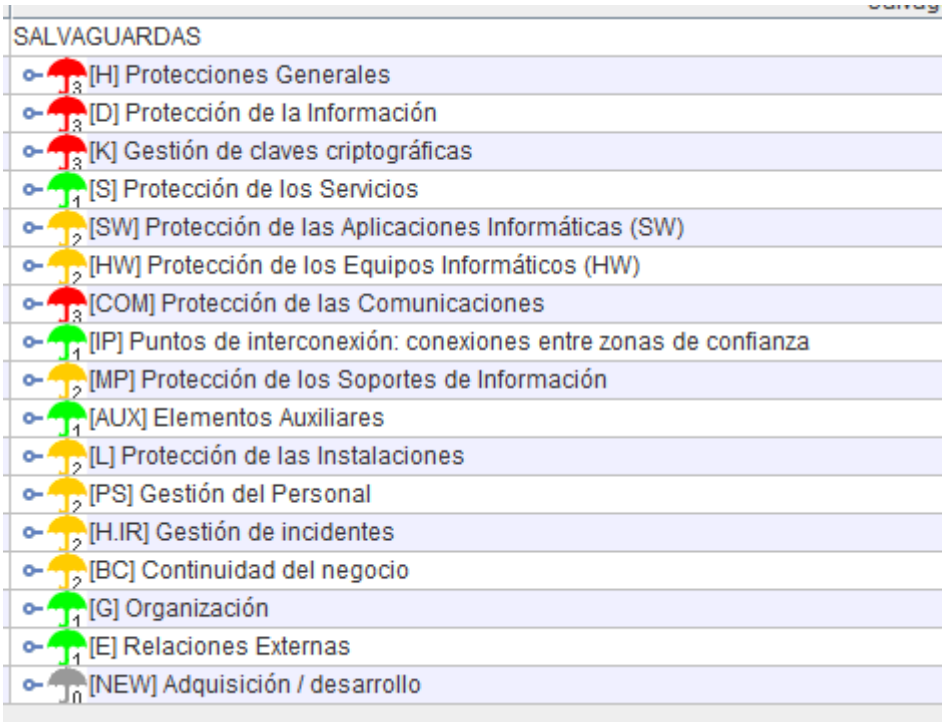
Dependencias: Se pueden ver las dependencias de los diferentes tipos de activos.



Amenazas: Ejemplos de las amenazas de desastres naturales.



Salvaguardas: se pueden observar los tipos de protecciones que existen.



Fuego:

Los activos que son afectados por el fuego son los siguientes: Equipos informáticos, soportes de información, equipamiento auxiliar e instalaciones.

[N.1] Fuego

[N.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: incendios: posibilidad de que el fuego acabe con recursos del sistema. **Ver:** EBIOS: 01- INCENDIO	

Errores de los usuarios: Los errores de usuarios pueden afectar a los activos datos/información, claves criptográficas, servicios, aplicaciones y soportes de información.

[E.1] Errores de los usuarios

[E.1] Errores de los usuarios	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [Media] soportes de información	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc. **Ver:** EBIOS: 38 - ERROR DE USO	

AMENAZAS QUE AFECTAN A LOS DATOS DE LOS CLIENTES Y AL CENTRO DE PROCESO DE DATOS

- **Datos de los clientes**
  - **Errores y fallos no intencionados:** Errores de administrador, errores de usuario, escapes de información, alteración accidental de la información, fugas de información, destrucción de información.
  - **Ataques intencionados:** Abuso de privilegios de acceso, suplantación de la identidad del usuario, acceso no autorizado, modificación deliberada de la información, divulgación de información, destrucción de información.
- **Centro de proceso de datos**
  - **Origen industrial:** daños por agua, fuego, desastres industriales, contaminación electromagnética, contaminación mecánica, avería de origen

físico o lógico, condiciones inadecuadas de temperatura y humedad , emanaciones electromagnéticas.
- **Desastres naturales:** daños por agua, fuego..
- **Errores y fallos no intencionados:** errores de configuración o mantenimiento de equipos, pérdida de equipos, caída del sistema por agotamiento, alteración accidental de la información.
- **Ataques intencionados:** Abuso de privilegios de acceso, robo, ataque destructivo, manipulación de equipos.

AMENAZAS CON MAYOR IMPACTO

- Acceso no autorizado
- Suplantación de identidad.

SALVAGUARDAS.

Ejemplos de salvaguardas: para la protección de las comunicaciones, para el control de los accesos físicos a las instalaciones, y para la gestión de claves criptográficas.

- **Para la protección de las comunicaciones:** autenticación del canal, seguridad wireless.
- **Para el control de acceso físico a las instalaciones:** pases o identificadores, se evita el trabajo no supervisado, se prohíben equipos de registro.
- **Para la gestión de claves criptográficas:** se dispone de normativa y procedimientos de gestión de claves, generación, distribución y almacenamiento de claves.

ANALIZACIÓN DE LA VENTANA DE IMPACTO Y RIESGO-> VALORES ACUMULADOS.

Muestra de algún ejemplo de los riesgos potenciales más elevados, y de los menos relevantes, indicando a qué activo afectan.

Riesgos potenciales más elevados:

Tramitación remota –> Afecta al activo: Capa de negocio.

Servidor – > Afecta al activo: Equipamiento.

Suplantación de la identidad del usuario –> Afecta al activo: Equipos

Modificación de la información – > Afecta al activo: Servicios internos

Acceso no autorizado – > Afecta al activo: Servicios internos

Riesgos potenciales menos relevantes:

Destrucción de la información –> Afecta al activo: Servicios internos y comunicaciones

Errores de los usuario –> Afecta al activo: Instalaciones

Mensajería electrónica –> Afecta al activo: Servicios Internos:

PARTE DE INFORMES

Identificación de los dos riesgos potenciales más elevados, y los dos actuales más elevados. Poned un ejemplo de activo al que sólo se le requiera la dimensión de Disponibilidad, y otro con un riesgo alto en la Integridad.

- **Riesgos potenciales más elevados:**
  - Confidencialidad de los datos –> Acceso SSL a los usuarios
  - Integridad y Confidencialidad de los datos – > Servidores

- **Riesgos actuales más elevados:**
  - Cortafuegos(Integridad de los datos) –> Autenticidad de los usuarios y de la información.
  - Servidor –> Confidencialidad de los datos.

- **Activo al que solo se le requiera la dimensión de disponibilidad:**
  - Mensajería y conexión a internet

- **Activo con un riesgo alto en la Integridad:**
  - Servidor (Integridad de los datos)

PERFILES DE SEGURIDAD: COMPARACIÓN DE LOS DIFERENTES INFORMES DE SEGURIDAD SEGÚN LAS NORMAS ISO/IEC 27002 Y REGLAMENTO LOPD.

****El archivo .rtf no se puede cargar, tanto en las aulas informáticas como los propios ordenadores. Por lo tanto se ha procedido a una evaluación del archivo del ejemplo*

Definiciones del programa:

La valoración de pilar con respecto a los perfiles de seguridad nos aporta 3 estados:

Actual: Es la valoración actual que tienen los diferentes apartados.

Pilar: Es la valoración que otorga PILAR y que tienen los diferentes apartados.

Objetivo: Es la valoración deseada, que se quiere llegar a tener en los diferentes apartados.

Normas ISO/IEC 27002

control	dudas	fuente	aplica...	come...	actual	objetivo	PILAR
[27002:2013] Código de buenas prácticas para la Gestión de la Seguridad de la Información					35%	94%	73%
[5] Políticas de seguridad de la información					0%	100%	50%
[6] Organización de la seguridad de la información					30%	89%	74%
[7] Seguridad ligada a los recursos humanos					10%	100%	n.a.
[8] Gestión de activos					40%	97%	71%
[9] Control de acceso					47%	98%	82%
[10] Criptografía					55%	85%	70%
[11] Seguridad física y del entorno					29%	89%	84%
[12] Gestión de operaciones					45%	96%	78%
[13] Seguridad de las comunicaciones					34%	95%	83%
[14] Adquisición, desarrollo y mantenimiento de los sistemas					27%	98%	78%
[15] Relaciones con proveedores					83%	99%	56%
[16] Gestión de incidentes de seguridad de la información					38%	94%	74%
[17] Aspectos de seguridad de la información en la gestión de la continuidad del negocio					14%	89%	77%
[18] Cumplimiento					43%	90%	66%

Organización de la seguridad de la información

- **Organización interna:** Actual: 49% Objetivo: 80% Pilar: 78%
  La valoración es muy positiva en cuanto al programa, a la valoración actual se encuentra a medio camino de llegar a su meta.
- **Dispositivos móviles y teletrabajo:** Actual: 10% Objetivo: 98% Pilar: 70%
  A pesar de la buena valoración que Pilar otorga, la valoración actual está muy lejos de llegar a su objetivo.

Reglamento LOPD

control	dudas	fuente	aplica...	come...	actual	objetivo	PILAR
[RD 1720] Protección de datos de carácter personal (11.5.2010)					44%	87%	79%
[B] Medidas de seguridad de nivel básico			M		55%	96%	81%
[M] Medidas de seguridad de nivel medio			M		23%	95%	77%
[A] Medidas de seguridad de nivel alto					53%	70%	81%

Medidas de seguridad nivel básico

- **Funciones y obligaciones del personal:** Actual: 25% Objetivo: 100% Pilar: 55%
  Como vemos, falta mucho que mejorar para llegar a la valoración deseada, aunque el programa Pilar aporta una valoración más positiva.
- **Gestión de las incidencias:** Actual: 100% Objetivo: 100% Pilar: 90%
  En este caso, la valoración actual y la deseada alcanzan el máximo valor permitido. Sin embargo para el programa Pilar no llega al máximo.

SEGUNDA PARTE: HERRAMIENTAS DE AUTOEVALUACIÓN DE LA NORMATIVA ISO/IEC

En esta parte hemos supuesto que nuestra empresa se dedica al desarrollo de software, es una empresa pequeña pero en proceso de crecimiento, cuenta con un número de 25 trabajadores y está transformándose en una mediana empresa. La meta de la empresa será de de aumentar su capacidad de desarrollo para poder realizar frente a los nuevos pedidos de la compañía.

CUESTIONARIO ISO/IEC 27001 (SGSI). SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. NORMA CERTIFICABLE

Findings: aspectos a mejorar obtenidos de investigaciones previas, en algún punto determinado. Si un apartado concreto presenta unas valoraciones inferiores a la media o a las exigidas, se examinarán los determinados requisitos para dichas cualificaciones y qué es lo que cumple o no ese determinado apartado. Una vez analizado eso podemos proponer los "findings".

****En el excel adjunto contienen los ejemplos de findings sobre algunos de los puntos con peores calificaciones.*

Domain	Status (%)
Security Policy	48%
Organization of Information Security	44%
Asset Management	51%
Human resources security	52%
Physical and Enviornmental security	45%
Communication and Operations Management	45%
Access Control	48%
Information system acquisition, development and maintanence	57%
Information security incident management	44%
Business Continuity Management	38%
Compliance	53%

Los resultados obtenidos por la ISO/IEC 27001 muestran unos porcentajes muy similiares, no hay ningún capítulo que resalte de manera considerable más que los otros ni ninguno que haya que mejorar mucho para llegar a los niveles de los otros. Aún así todos los puntos tratados, deberían de mejorar para estar en unos niveles notables y buenos para la gestión de la seguridad en la empresa.

Aún así el mejor y peor capítulo serían:

- **Mejor Capítulo:** Con un 57% de valoración sería el de; Sistema de información de adquisición, desarrollo y mantenimiento.
- **Peor Capítulo:** Con un 38% de valoración sería el de; Gestión de continuidad del negocio. Muy importante mejorar en este factor si se quiere crecer a nivel de ventas.

CUESTIONARIO ISO/IEC 27002. BUENAS PRÁCTICAS DE SEGURIDAD.

- **Políticas de seguridad:** Se cumple el 66.67 % de los puntos, no se cumple el 33.33 % restante. Se podría mejorar implantando mecanismos y controles para verificar las normas y las políticas.
- **Organización de la seguridad:** Se cumple el 66.67 % de los puntos, no se cumple el 33.33 % restante. Contratando a empresas externas se podrían incrementar las valoraciones.
- **Clasificación y control de activos:** Se cumple el 40.00 % de los puntos, no se cumple el 60.00 % restante. Si se mejora el proceso de los ítems del inventario se lograría un aprobado en esta parte.
- **Seguridad del personal:** Se cumple el 50.00 % de los puntos, no se cumple el 50.00 % restante. Con un poco de trabajo extra, formación y poner en conocimiento al personal de los peligros de la seguridad se incrementaría la calificación.
- **Seguridad física y del entorno:** Se cumple el 45.45 % de los puntos, no se cumple el 54.45 % restante. Aumentar el proceso de seguridad dentro de la empresa ayudaría a delimitar los problemas en este punto, incrementando su nota considerablemente.
- **Gestión de comunicaciones y operaciones:** Se cumple el 50.00 % de los puntos, no se cumple el 50.00 % restante. Un plan de adecuación de las políticas incrementaría notablemente este capítulo.
- **Control de accesos:** Se cumple el 43.75 % de los puntos, no se cumple el 56.25 % restante. Catalogando a los usuarios y empleados de la empresa se lograría aumentar la calificación de este apartado.
- **Desarrollo y mantenimiento de los sistemas:** Se cumple el 80.00 % de los puntos, no se cumple el 20.00 % restante. Se lograría el sobresaliente implementando controles criptográficos.
- **Gestión de la continuidad del negocio:** Se cumple el 40.00 % de los puntos, no se cumple el 60.00 % restante. Implementando procesos para la continuidad del negocio, se aprobaría este punto.
- **Conformidad:** Se cumple el 66.67 % de los puntos, no se cumple el 33.33 % restante. Se lograría la perfección si se hicieran auditorías de los sistemas y se tuvieran en cuenta.

CONCLUSIÓN GENERAL: LOS MEJORES Y PEORES CAPÍTULOS DE LA NORMA ISO/IEC 27002

El mejor: Desarrollo y mantenimiento de los sistemas con 80% de los ítems cumplidos.

Los peores:

- Gestión de la continuidad del negocio 40% de los ítems cumplidos.
- Clasificación y control de activos 40% de los ítems cumplidos.

Con todos estos datos presentados si comparamos las 2 ISOS comparadas en esta parte, podemos concluir que ambas tienen en mayor o menor medida las mismas similitudes variando en algún porcentaje. Pero a grandes rasgos, exponiendo la misma información.