

El Análisis de Riesgos en el contexto del ENS

Por **Rafael González**, asociado senior de Governance, Risk & Compliance de ECIJA

Hasta el momento, una implantación de un **Sistema de Gestión de Seguridad de la Información (SGSI)** seguía un guión claramente establecido:

- Definición de un alcance para el sistema de gestión.
- Definición de unas políticas y una declaración de intenciones por parte de la Gerencia para comunicar al personal.
- Realización de un análisis de riesgos basado en un inventario de activos previo.
- Desarrollo de un plan de tratamiento del riesgo en función de los resultados del análisis.



Evidentemente faltan muchos pasos y envolverlo todo en un modelo de mejora continua basado en ciclos (PDCA).

El RD 3/2010, Esquema Nacional de Seguridad (ENS), cambia este guión para establecer sus propias fases:

- Inventario de servicios electrónicos a los ciudadanos.
- Categorización de esos servicios en base a los criterios de la guía CCN-STIC-803 Valoración de Sistemas (las guías no son de obligado cumplimiento como lo es un Real Decreto, pero son una base sobre la que trabajar).

- En base a esa valoración se aplican los controles establecidos en el ANEXO II del ENS. El propio CCN pone a disposición de las entidades una aplicación para determinar exactamente los controles que aplican.
- Se exige una cierta documentación como pueda ser la Declaración de Aplicabilidad o el Análisis de Riesgos.

El objeto de este artículo es ofrecer algunas reflexiones sobre el **análisis de riesgos** en el contexto de un proyecto de ENS.

El alcance

El alcance viene definido según la Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos y abarca los servicios electrónicos que las distintas administraciones prestan a los ciudadanos.

Se "complica" este alcance con alguna indicación dada en la guía CCN-STIC-803 Valoración de Sistemas donde dice: "el Esquema Nacional de Seguridad se limita a valorar aquellos tipos de información que son relevantes para el proceso administrativo y pueden ser tratados en algún servicio afecto a la ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos".

Esta matización da lugar a curiosas paradojas como por ejemplo dejar fuera del alcance ciertos sistemas que no tienen que ver con el procedimiento administrativo directamente pero que pueden ser puerta para importantes brechas de seguridad que si podrían afectarle de forma indirecta.

Categorización

Hay que destacar que la categorización hay que hacerla en función de los criterios dados en la citada guía, no son criterios "informáticos" basados en un impacto producido por la materialización de una amenaza. La valoración debe hacerla el responsable de la información o del servicio, e insisto, en base a los criterios de la guía. Esto significa que primero se los tiene que leer, entender y aplicar posteriormente.

En caso de no identificar al responsable, la valoración debe hacerla el responsable de seguridad y en tal caso hay que insistir en que los criterios de valoración son los de la guía, no los tradicionales criterios que tenemos los informáticos que por lo general tendemos a magnificarlo todo.

El concepto de "categorización" en un SGSI tiene otras connotaciones, es más, no existe el concepto tal y

INFORMACIÓN RELACIONADA

Un investigador italiano revela 14 nuevas vulnerabilidades en sistemas SCADA

Oracle emite un parche de emergencia para cubrir una vulnerabilidad en HTTP Server

Ya puedes descargar, gratis, la versión digital de Verano Tech

¿Qué han hecho los hackers por nosotros?

Submit

Whitepapers

- Observatorio Computerworld-IDC (1er.trimestre 2011)
- Respaldo y recuperación: nuevas estrategias con soluciones basadas en disco
- Cómo modernizar el respaldo para acelerar la transición hacia la virtualización
- Aspectos fundamentales de la deduplicación para su negocio
- El Estado de Internet
- Cómo crear un entorno virtualizado seguro
- Un entorno 100% web, el modelo de TI del futuro

Últimas noticias

Computerworld muestra la nueva realidad del protocolo IPv6

Un investigador italiano revela 14 nuevas vulnerabilidades en sistemas SCADA

Oracle emite un parche de emergencia para cubrir una vulnerabilidad en HTTP Server

Google parchea 32 fallos de seguridad en Chrome

Windows 8 introducirá importantes mejoras de seguridad

Artículos más votados

¿Son seguros los smartphones? La importancia de una buena gestión de la reputación online de la empresa
Cinco cosas que hacer antes de comprar más tecnología de seguridad
Elegir una contraseña adecuada, una de las claves para garantizar la seguridad informática
Datos 'blindados' en la organización

Ofertas Canal Compras



Monitor Panorámico E2211h Serie.
 Productos DELL para empresas.
119,20 €
 ★★★★★

iPhone Ipod Radio Reproductor.
 ¡Ahorra tiempo y dinero! **54,99 €**

como lo entiende el ENS. La criticidad de un sistema va en función del impacto que produce la materialización de una amenaza.

La Declaración de Aplicabilidad

La declaración de aplicabilidad hasta ahora era un inventario de controles (en función de la norma que se aplicara) cuyo objetivo es reparar uno a uno los que aplican y los que no aplican. Era importante dejar claro el motivo de exclusión de un determinado control.

En el contexto del ENS, los controles no se eligen, viene impuestos por la categoría del sistema por lo tanto la declaración de aplicabilidad no deja de ser un documento formal que a todos los efectos aporta poco.

No tiene sentido intentar justificar la no inclusión de un control porque el motivo es muy sencillo: "lo refleja el Real Decreto". En el artículo 13 hay una indicación sobre la justificación de la no inclusión de controles, pero de una forma inconexa con respecto a la declaración de aplicabilidad.

Hay que recordar que en ISO 27001 es un matiz obligatorio a la hora de hacer la declaración de aplicabilidad (control ISO 27001 4.2.1.j-3).

El Análisis de Riesgos

¿Qué dice la guía 803 del Centro Criptológico Nacional sobre el análisis de riesgos?

Nada, o mejor dicho, en el apartado de ABREVIATURAS cuando habla del significado de MAGERIT.

¿Qué dice el ENS sobre el análisis de riesgos?

o Artículo 6. Gestión de la seguridad basada en los riesgos.

"1. **El análisis y gestión de riesgos** será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.

2. **La gestión de riesgos** permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, **los riesgos** a los que estén expuestos y las medidas de seguridad."

¿Cómo? La gestión de la seguridad se hace en base a la categorización del sistema no en base al riesgo.

o Artículo 13. **Análisis y gestión de los riesgos.**

El punto 2 dice "Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente".

Volvemos al mismo punto, si un Real Decreto obliga a que hay que tomar una determinada medida, huelga evaluar si esa medida obedece a un análisis o no. De hecho, en implantaciones del ENS en alguna administración, directamente el responsable de seguridad suele afirmar que se implanta algo por "imperativo legal" pero no por necesi

Autor: CSO
19/09/2011
Votos: 0

Más sobre: **Ecija actualidad políticas**

 Me gusta        Más

Votar |

Noticias más votadas

Los hackers han estado robando mensajes de Hotmail más de una semana

Un ex hacker da su visión sobre el ataque a PlayStation Network

Google añade defensa frente a descargas y cubre 15 vulnerabilidades con Chrome 12

Netmind trae la formación en seguridad informática de Mile2 a España



Busca Productos y Compara Precios



Ofertas de Informática
Ofertas de Imagen y Sonido
Ofertas de PDAs y GPS
Ver Más Ofertas



Los usuarios online más activos son también más vulnerables al phishing

Hoy en IDG.es



Noticias

- Aena confía a Esri sus sistemas de información aeronáutica
- Repsol y el BSC crean un centro para desarrollar tecnologías de exploración de hidrocarburos
- Google prepara una actualización de Android "para todos"
- Visita Barcelona en Gótico con el iPad 2
- Microsoft lanza un ERP dirigido a las grandes corporaciones
- Marcos digitales AgfaPhoto
- Interoute compra Quantix, un proveedor de servicios cloud
- Canon anuncia su compatibilidad con el AirPrint de Apple
- La nueva realidad del protocolo IPv6, jornada gratuita
- La nueva realidad del protocolo IPv6, a examen

Artículos

- 8 usos para tu viejo smartphone
 - Microsoft Windows 8: Todas sus novedades
 - Presente y futuro del cloud computing
 - (Análisis) Sony Ericsson Xperia Play
 - "Queremos estar cerca de nuestros clientes, ser parte de ellos y de su día a día" José María García, Esprinet Ibérica
- ZTE Skate, en exclusiva con Movistar**



Informativo semanal de IDG TV (16/09/11)

[Contactar](#) [Publicidad](#) [Suscripciones](#) [Hemeroteca IDG](#) [Atención al Cliente](#) [Perfil](#) [Acta de privacidad](#)

Webs de IDG [IDG.es](#) [ComputerWorld](#) [PC World](#) [CIO](#) [PC World Digital](#) [GamePro TV](#) [Macworld](#) [NetworkWorld](#) [iWorld](#) [DealerWorld](#)
[iPhoneWorld](#) [IDG TechStyle](#) [MALWARE](#)

©2011 IDG COMMUNICATIONS, S. A. U. Prohibida la reproducción total o parcial en cualquier medio (escrito o electrónico) sin autorización expresa por escrito de la editorial. En particular, IDG COMMUNICATIONS, S.A.U., se opone de manera expresa, salvo consentimiento por escrito, a la reproducción, recopilación, distribución, comunicación pública o puesta a disposición por parte de terceros de los contenidos publicados en los medios de su titularidad (ya se editen éstos en papel, a través de Internet o cualquier otro soporte), de conformidad con lo establecido en el artículo 32 de la Ley 23/2006, de 7 de julio, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril. En caso de estar interesado en una autorización para reproducir, distribuir, comunicar, almacenar o utilizar en cualquier forma los contenidos titularidad de IDG COMMUNICATIONS, S.A.U. debe dirigir su petición a la siguiente dirección de correo electrónico :

idg_nt@idg.es

