



GUÍA DE SEGURIDAD (CCN-STIC-815)

ESQUEMA NACIONAL DE SEGURIDAD MÉTRICAS E INDICADORES

Edita:



© Editor y Centro Criptológico Nacional, 2013

Fecha de Edición: julio 2013

Informática de la Comunidad de Madrid (ICM) ha participado en la redacción de documento.

El Ministerio de Hacienda y Administraciones Públicas ha financiado el desarrollo del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del **Centro Criptológico Nacional**, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

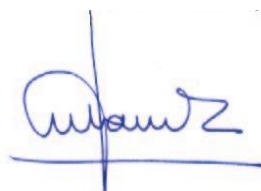
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Julio de 2013



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN.....	5
1.1. DEFINICIONES.....	5
2. OBJETO.....	7
3. ALCANCE.....	8
4. MEDICIÓN DE LA SEGURIDAD.....	8
4.1. DATOS.....	9
4.2. MEDIDAS.....	10
4.3. MÉTRICAS.....	10
4.4. INDICADORES.....	11
4.5. TIPOS DE MÉTRICAS E INDICADORES.....	11
4.6. EXPLOTACIÓN.....	12
4.7. CUADRO DE MANDO.....	14
4.8. EL PROGRAMA DE MÉTRICAS E INDICADORES.....	14
4.9. METODOLOGÍA DE DESARROLLO DE NUEVOS INDICADORES.....	15
4.9.1. <i>MÉTRODO GQM</i>	15
4.9.2. <i>MÉTODO CIENTÍFICO</i>	16
5. DATOS.....	17
5.1. SISTEMAS.....	17
5.2. INCIDENTES DE SEGURIDAD.....	17
5.2.1. <i>TIEMPOS</i>	17
5.2.2. <i>IMPACTO O CONSECUENCIAS DEL INCIDENTE</i>	18
5.2.3. <i>CAUSA DEL INCIDENTE</i>	18
5.2.4. <i>INCIDENCIAS DEL INCIDENTE</i>	19
5.3. GESTIÓN DE VULNERABILIDADES.....	20
5.4. AUDITORÍAS.....	20
5.5. CONTINUIDAD DEL SERVICIO.....	21
6. MÉTRICAS.....	21
6.1. PORCENTAJES.....	21
6.2. CALIDAD DEL SERVICIO.....	21
6.3. MADUREZ.....	22
6.3.1. <i>MADUREZ DE UNA ACTIVIDAD O PROCESO</i>	23
6.3.2. <i>MADUREZ COMPUESTA</i>	23
6.4. LEGIBILIDAD DE LA DOCUMENTACIÓN.....	24
6.5. UTILIDAD DE LA DOCUMENTACIÓN.....	24
7. INDICADORES ESTÁNDAR.....	25
7.1. ANEXO II DEL ESQUEMA NACIONAL DE SEGURIDAD.....	25
7.1.1. <i>ÍNDICE DE MADUREZ DEL ENS</i>	25
7.1.2. <i>ÍNDICE DE CUMPLIMIENTO DEL ENS</i>	26
7.2. RD 1720/2007 DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.....	26
7.2.1. <i>ÍNDICE DE MADUREZ DEL RD1720</i>	27
7.2.2. <i>ÍNDICE DE CUMPLIMIENTO DEL RD1720</i>	27
7.3. ORGANIZACIÓN.....	27
7.4. GESTIÓN DE INCIDENCIAS.....	27
7.5. DISPONIBILIDAD DE LOS SERVICIOS.....	29
8. REPORTE ANUAL.....	30
8.1. INVENTARIO.....	30
8.2. ANÁLISIS DE SITUACIÓN.....	30
8.2.1. <i>DOCUMENTACIÓN DE SEGURIDAD</i>	30

8.2.2.	ORGANIZACIÓN	30
8.2.3.	PROCESO DE AUTORIZACIÓN.....	30
8.2.4.	MEDIDAS DE PROTECCIÓN	31
8.2.5.	CERTIFICACIONES.....	31
8.2.6.	ANÁLISIS DE INCIDENTES.....	31
8.2.7.	AUDITORÍAS DE NEGOCIO	31
8.2.8.	AUDITORÍAS TÉCNICAS.....	31
9.	CUADROS DE MANDO	32
9.1.	ÁREAS PROPUESTAS E INDICADORES	32
9.1.1.	RECURSOS.....	32
9.1.2.	PERCEPCIÓN EXTERNA – CALIDAD DEL SERVICIO PRESTADO.....	32
9.1.3.	EXCELENCIA INTERNA.....	32
9.1.4.	ORIENTACIÓN FUTURA.....	33
10.	ORIENTACIONES PRÁCTICAS	34
10.1.	¿POR DÓNDE EMPEZAR?	34
10.2.	¿CÓMO SEGUIR?.....	34
10.3.	PROYECTOS DE SEGURIDAD	35
	ANEXO A - GLOSARIO DE TÉRMINOS Y ABREVIATURAS.....	37
	ANEXO B - REFERENCIAS	40
	ANNEXO C – CVSS.....	42
10.4.	CONFIDENTIALITY IMPACT (C).....	42
10.5.	INTEGRITY IMPACT (I).....	42
10.6.	AVAILABILITY IMPACT (A).....	43
	ANEXO D – RECURSOS.....	44
10.7.	DATOS.....	44
10.7.1.	RECURSOS HUMANOS.....	44
10.7.2.	RECURSOS ECONÓMICOS.....	44
10.7.3.	USUARIOS INTERNOS.....	45
10.8.	INDICADORES.....	45
10.8.1.	PROPORCIÓN DE RECURSOS HUMANOS DEDICADOS A SEGURIDAD DE LOS SISTEMAS..	45
10.8.2.	PROPORCIÓN DE RECURSOS ECONÓMICOS DEDICADOS A SEGURIDAD DE LOS SISTEMAS	45
10.8.3.	PROPORCIÓN DE RECURSOS TIC EXTERNALIZADOS.....	46
10.8.4.	PROPORCIÓN DE RECURSOS STIC EXTERNALIZADOS	46
10.8.5.	OTROS INDICADORES.....	47

1. INTRODUCCIÓN

1. Esta guía establece unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad sin entrar en casuísticas particulares. Se espera que cada organización las particularice para adaptarlas a su entorno singular.
2. El Esquema Nacional de Seguridad (ENS) establece la obligación de evaluar regularmente el estado de seguridad de los sistemas:

Artículo 35. Informe del estado de la seguridad.

El Comité Sectorial de Administración Electrónica articulará los procedimientos necesarios para conocer regularmente el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere el presente real decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las Administraciones públicas.

3. Así mismo, el ENS establece la necesidad de establecer un sistema de medición de la seguridad del sistema:

Anexo II – Medidas de seguridad

4 Marco operacional [op]

4.6 Monitorización del sistema [op.mon]

4.6.2 Sistema de métricas [op.mon.2]

dimensiones categoría	todas		
	básica	media	alta
	no aplica	no aplica	aplica

Categoría ALTA

Se establecerá un conjunto de indicadores que mida el desempeño real del sistema en materia de seguridad, en los siguientes aspectos:

- a) Grado de implantación de las medidas de seguridad.
- b) Eficacia y eficiencia de las medidas de seguridad.
- c) Impacto de los incidentes de seguridad.

4. Esta guía busca una sistematización de ambas obligaciones por medio de la definición de un conjunto ordenado de indicadores que puedan ser utilizados en diferentes momentos y circunstancias según convenga, pero con una definición uniforme.

1.1. DEFINICIONES

5. En este documento se tratan datos, métricas e indicadores. Cuando se observa la realidad, es necesario clasificar o medir lo observado. Usando un procedimiento de medida y unas unidades o valores de referencia, se obtienen mediciones que se usarán como datos. Estos datos pueden tratarse de diferentes maneras para obtener una visión más elaborada, bien sea resaltando algunas características, agregando datos de diferentes formas, o estudiando su evolución. Bajo el nombre genérico de métricas se recogen estos métodos de tratamiento para extraer información relevante de los datos disponibles. Por último, alguna de esta información, más o menos elaborada, puede servir de indicador, entendiendo por “indicador” información concisa que por si sola o en combinación con otros indicadores resume la situación en la que estamos.

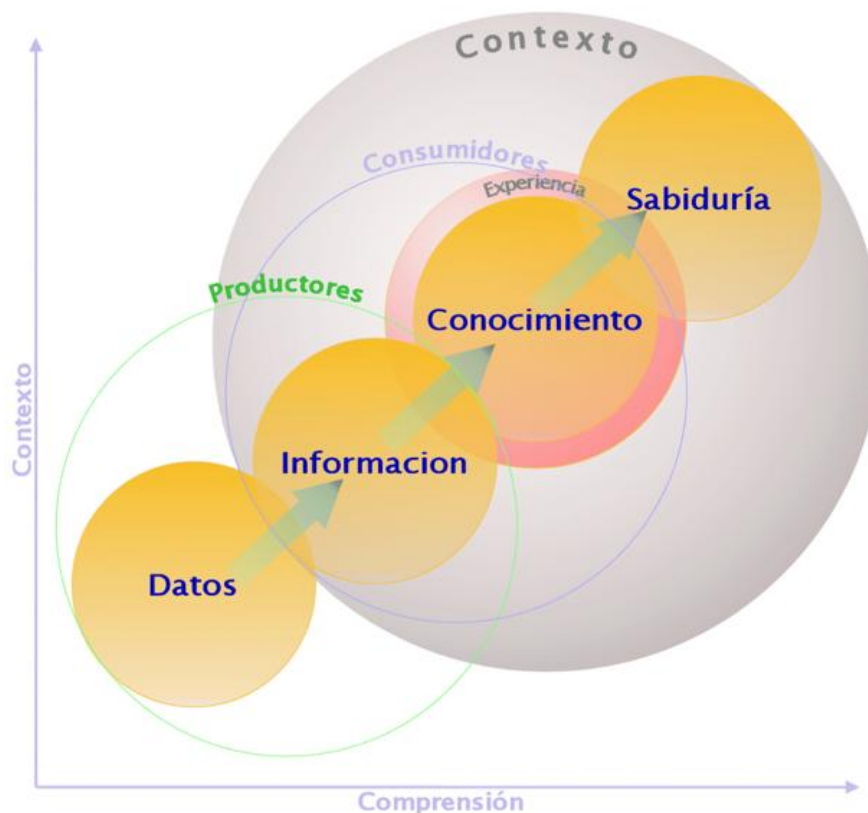
6. Sirva de ejemplo el conjunto de indicadores económicos (como puede ser la productividad de las empresas o el índice de paro) que nos sirven para calificar la situación económica de un país.
7. Nótese que todo son datos más o menos elaborados. Un dato recibe el calificativo de indicador cuando es significativo para reflejar de forma concisa el estado de algo que nos preocupa.
8. En materia de seguridad de la información, ante la avalancha de datos disponibles, es conveniente resumir en unos pocos indicadores que sean suficientemente representativos de la seguridad del sistema, sin perjuicio de poder profundizar en más detalle (aplicando nuevas métricas a los datos primigenios). Para estos resúmenes ejecutivos se emplean los cuadros de mando que, típicamente, presentan una docena de indicadores en cuatro áreas que se consideran estratégicas.
9. Las definiciones que siguen están tomadas del trabajo de Debra S. Herrmann que se cita en las referencias. No pretendemos ser escrupulosamente academicistas, pero sí entender que necesitamos datos, que necesitamos unidades y métodos para medir o clasificar aquellos datos, y fórmulas para combinar medidas y obtener indicaciones de dónde estamos.
10. **Datos.** Representación de la información usando algún formato que permita su comunicación, interpretación, almacenamiento y procesado automático.
11. **Medición.** (1) Proceso consistente en la asignación de números o símbolos a entidades de la realidad de forma que nos permitan describir dichas entidades de acuerdo a unas reglas claramente definidas. (2) Comparación de una propiedad de un objeto con una propiedad similar en otro objeto que se usa de referencia.
12. **Medida.** El número o símbolo asignado a una entidad como resultado de un proceso de medición. La medida sirve para caracterizar un atributo de la entidad.
13. **Métrica.** Por una parte es una unidad de medida (como lo es, por ejemplo, el sistema métrico decimal). Por otra parte, suele tener una finalidad, entendiéndose como una herramienta para entender la realidad y tomar decisiones al respecto. En este documento lo interpretaremos más bien en el segundo sentido.
14. **Indicador.** (1) Instrumento que se utiliza para monitorizar la operación de un ingenio, en sentido general. (2) Química. Un elemento que cambia de color o estructura cuando se dan ciertas circunstancias, sirviendo como mecanismo de detección. (3) Economía. Conjunto de estadísticos que sirven para saber cómo está y a dónde se encamina la economía.
15. **Indicator.** (1) An instrument used to monitor the operation or condition of an engine, furnace, electrical network, reservoir, or other physical system; a meter or gauge. (2) Chemistry. A chemical compound that changes color and structure when exposed to certain conditions and is therefore useful for chemical tests. (3) Ecology: A plant or animal whose existence in an area is strongly indicative of specific environmental conditions. (4) Any of various statistical values that together provide an indication of the condition or direction of the economy.
16. **Cuadro de mando.** Conjunto de indicadores para resumir el desempeño de un sistema.

2. OBJETO

17. Esta guía persigue varios objetivos:

- ☐ Proponer un conjunto de datos a registrar del sistema de información a fin de poder derivar métricas posteriormente, tanto locales del sistema, como del conjunto de la Administración
- ☐ Proponer un conjunto reducido de métricas o indicadores para caracterizar la posición del sistema de información en materia de seguridad de la información
- ☐ Proponer un conjunto de métricas o indicadores para materializar el reporte anual requerido por el artículo 35.
- ☐ Proponer cuadros de mando para escenarios típicos.
- ☐ Establecer las pautas para que cada organismo extienda los indicadores que convengan en cada momento a sus necesidades.

18. Nótese que los indicadores son herramientas para sustentar la toma de decisiones, especialmente en dos aspectos: (1) cumplimiento normativo y (2) ejecución de proyectos. Los aspectos de cumplimiento son relativamente estáticos pues referencian un Real Decreto. En cambio, los proyectos son circunstanciales de cada organismo y de cada momento, por lo que no pueden generalizarse. No obstante, se describe cómo desarrollar indicadores más específicos y esperamos que el conjunto amplio de indicadores del anexo pueda ser reutilizado con frecuencia.



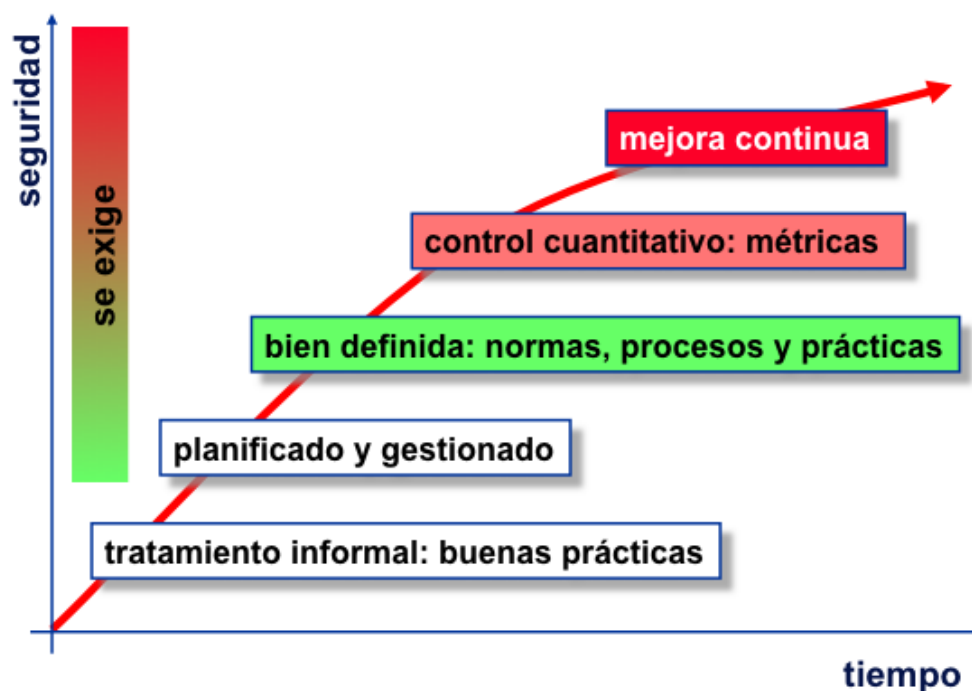
<http://www.infovis.net/printMag.php?num=186&lang=1>

3. ALCANCE

19. Esta guía es de aplicación a los sistemas de información sujetos a la Ley 11/2007 y al Real Decreto 3/2010.

4. MEDICIÓN DE LA SEGURIDAD

20. La seguridad es una preocupación constante, cuando no creciente, tanto para los técnicos a cargo de los sistemas, como para los gestores de la organización. La seguridad técnica de los sistemas es un requisito indispensable; pero más allá de la técnica, los gestores necesitan tener confianza en que el sistema de información permitirá alcanzar los objetivos propuestos y establecer relaciones fructíferas con otras organizaciones. En este contexto, las métricas aparecen como necesarias para conocer el estado actual de la seguridad, mejorarlo y gestionar gastos e inversiones. Se requiere un eficaz alineamiento de los diferentes actores, tanto verticalmente (dentro de la propia organización) como horizontalmente (con otras organizaciones conectadas).
21. Es difícil analizar sobre el papel la seguridad efectiva de un sistema aislado; pero lo es aún más predecir la seguridad de dos sistemas si se interconectan. Los defectos de seguridad pueden afectar más o menos a un sistema aislado; pero presentan una desagradable tendencia a magnificarse cuando unos sistemas se interconectan con otros y pequeños desencuentros tienen consecuencias críticas.



22. ¿Por qué queremos medir la seguridad? Por varias razones:
- ☐ Lo que no se mide no se puede gestionar. Sería conducir a ciegas pretender llevar a cabo una actividad sin concretar objetivos y sin medir si nos vamos acercando a ellos, o no.

- ☐ Saber si está funcionando la seguridad. No puede ser que tras tantos recursos humanos y económicos dedicados a proteger la información y los servicios, no tengamos una realimentación de lo que hemos conseguido. Y esto conviene saberlo antes de que un incidente, o un desastre, nos ponga violentamente en la realidad.
- ☐ ¿Estamos mejorando adecuadamente? Cuando analizamos un sistema de información y proponemos mejoras de seguridad, invertimos en un proyecto que consume recursos, proyecto que debe gestionarse y que debe incluir indicadores de progreso, tanto de las etapas realizadas como de los objetivos alcanzados.

El problema en cada momento es alcanzar los objetivos inmediatos y los indicadores deben permitir si estamos progresando según lo previsto hacia el objetivo deseado. O si vamos adelantados, o atrasados, o va a ser enteramente imposible llegar a donde se pretende en plazo y formas. Cuando los proyectos se expanden en plazos prolongados (años) los indicadores deben dar señales inmediatas de las desviaciones, mientras sea posible reaccionar con el mínimo esfuerzo extra

- ☐ Una metodología sencilla para lograr un buen nivel de seguridad. La seguridad de un sistema de información tiene tantas facetas que es fácil olvidar alguna. Por otra parte muchas facetas de la seguridad se describen con palabras, a menudo con objetivos negativos (que no ocurra tal cosa). Todo ello hace difícil marcarse unos objetivos de forma constructiva. Un buen conjunto de indicadores simplifica las reglas de forma radical:

hay que llevar todos los indicadores a la zona verde

Al tiempo hay que ser conscientes de que un mal indicador puede hacernos errar completamente en nuestras decisiones y confundirnos respecto de dónde estamos realmente en materia de seguridad.

23. El poder medir la seguridad de un sistema de información permite llevar a cabo una serie de actividades de gestión:
- ☐ tomar decisiones, tanto técnicas como de adjudicación de recursos
 - ☐ valorar la eficacia y eficiencia de la arquitectura de seguridad desplegada
 - ☐ facilitar la rendición de cuentas (*accountability*) de los responsables
24. Todo lo anterior se resume bajo el epígrafe de **permitir la gobernabilidad de la seguridad del sistema de información**.

4.1. DATOS

25. Los sistemas de información son capaces de suministrar millones de detalles siempre y cuando se les requiera con anterioridad. Hay que saber lo que se necesita para apuntarlo cuando se sabe (después ya es tarde) y hay que saber lo que no se necesita para poder desecharlo. O, algo intermedio, saber qué necesitamos durante cuánto tiempo de forma que los registros de actividad (logs) no nos desborden y el sistema dedique su actividad a su propia medición antes que su misión última. En la práctica
- ☐ hay que decidir de antemano que vamos a registrar
 - ☐ hay que establecer un plan de destrucción progresiva de logs
 - ☐ en cada destrucción hay que guardar parte de la información, bien en bruto, bien consolidada

- ☐ hay que automatizar todo el proceso de captura y gestión de logs para prevenir errores humanos, olvidos y ataques intencionados
26. La recolección de datos es mecánica; pero la decisión de qué se mide y qué se conserva durante cuánto tiempo debe hacerse con un objetivo. Los objetivos los marcan, en última instancia, las necesidades del servicio para gestionarlo en sus diferentes niveles de responsabilidad.

4.2. MEDIDAS

27. Los datos, en bruto, son poco relevantes. Desde cualquier punto de vista, la información atomizada es irrelevante. La información pasa a ser interesante cuando se mide (clasifica) y sobre todo cuando se agrega.
28. Cuando los datos se analizan utilizando algún criterio de evaluación, obtenemos una medida. Se dice que medimos. Las medidas quedan definida por una serie de valores de referencia (o unidades) y un algoritmo para deducir la medida a partir de los datos. Así, por ejemplo, para medir longitudes utilizamos el Sistema Métrico Decimal.
29. Hay medidas de varios tipos.
- ☐ Cuantitativas. Típicamente usan un número real que representa la proporción entre el atributo en el objeto medido y una referencia. Por ejemplo, una caja que mide 10cm nos dice que es 10 veces la referencia que hemos acordado como “1 centímetro”.
 - ☐ Cualitativas ordenadas. Típicamente rangos. Son como varios cajones en donde vamos metiendo los objetos medidos siguiendo algún criterio, cajones con la característica de estar ordenados. Por ejemplo, el Anexo I del ENS introduce los niveles BAJO, MEDIO y ALTO para clasificar las necesidades de seguridad.
 - ☐ Cualitativas. Típicamente clases sin orden. Por ejemplo, se puede saber cuánta gente va vestida de rojo, de amarillo ..., sin que un color sea superior a otro.
30. Las medidas permiten estructurar la información y prepararla para un tratamiento, sea este analítico, estadístico, o descriptivo.

4.3. MÉTRICAS

31. Las métricas permiten a los responsables interpretar lo que ocurre. A los más técnicos les permite controlar el comportamiento de los sistemas; a los menos técnicos les permite escudriñar el alineamiento de recursos dedicados y resultados obtenidos.
32. Una buena métrica debe satisfacer algunos criterios básicos de calidad:
- ☐ debe estar claro cómo se calcula a partir de los datos en bruto; si dos aplicaciones diferentes aplican la misma métrica de los mismos datos, el resultado de ambos procesos debería ser equivalente
 - ☐ debe estar claro cuándo (y cada cuánto tiempo) se mide, de forma que desviaciones u oscilaciones rutinarias no oculten desviaciones o comportamientos que denoten un problema
33. Las métricas suelen representarse gráficamente, mostrando su evolución en el tiempo; se necesitan reglas para interpretar el significado de los cambios, ¿cuánto es excesivo? ¿cuánto es demasiado poco? ¿es buena la estabilidad? ¿qué significan los picos? ¿y las variaciones abruptas? Y así un largo etcétera que permita entender el sistema observando la evolución de sus medidas.

34. Para que sea útil, una métrica debe estar bien (formalmente) definida, estando escrita la respuesta a las preguntas de los párrafos anteriores. Es más, desde un punto de vista de buena organización, debe estar claro quién es el responsable de su especificación, de su mantenimiento, de su elaboración regular, de la custodia de sus datos históricos, de la gestión de cambios y de la resolución de incidencias.

4.4. INDICADORES

35. Pese a su indudable interés, las medidas todavía son “nivel medio”. Se necesitan medidas para cada sistema o subsistema instalado: ¿cientos?. Y, por tanto, los ingenieros no pueden arrojárselas sin más a los niveles altos de dirección. Es necesario seguir cocinando (consolidando) los datos para llegar a una sucinta síntesis que refleje el estado de salud general o las situaciones de alarma: para que la dirección esté tranquila o para que tome medidas correctivas. Este es el papel de los indicadores [clave de rendimiento]¹ que, abstrayendo de la minucia de los detalles, son capaces de transmitir el estado general de salud del objeto.
36. Necesitamos unos pocos indicadores que resumen la salud de la organización; pero al tiempo que se adapten a la situación presente. Además, cuando aparece un nuevo indicador en escena, los usuarios no esperan pacientemente a ver cómo evoluciona para aprender a interpretarlo: desde el primer día necesitamos ver cómo hubiera lucido el nuevo indicador en el pasado inmediato. Esto se consigue conservando las series históricas de medidas, lo que permite evaluar los nuevos indicadores sobre los datos del pasado inmediato.
37. Necesitaremos una serie de indicadores predictivos, para anticipar problemas y tomar decisiones sobre síntomas antes de que lleguemos al desastre. Decimos que estos indicadores fallan cuando son incapaces de prevenir un desastre, cuando no perciben los síntomas y, por tanto, no alertan al responsable que debe actuar².
38. A menudo es difícil saber qué es una métrica o un indicador. Por ello los trataremos a la par en lo que sigue.

4.5. TIPOS DE MÉTRICAS E INDICADORES

39. Métricas o indicadores pueden calificarse según los siguientes grupos, no necesariamente excluyentes:

de cumplimiento

Se busca conocer el grado de cobertura de una cierta referencia, que puede ser una política interna, un reglamento, un perfil, etc.

Suelen ser indicadores que miden si se han cumplido los requisitos formales o si se han tomado medidas preventivas. Un buen cumplimiento no garantiza el éxito del sistema frente a un ataque o un incidente, pero sí que el sistema esté mejor posicionado para afrontarlos.

Un mal resultado en estos indicadores es una señal de posibles problemas: caso de ataque o incidente, no estamos todo lo preparados que debiéramos.

¹ Las siglas en inglés (KPI – *Key Performance Indicator*) no tienen una traducción unánime al español. A veces se habla de indicadores clave o indicadores críticos; a veces de indicadores de resultados, de rendimiento o de desempeño. En cualquiera de sus denominaciones se intenta identificar aquel indicador que es clave para entender qué está pasando.

² El indicador de gasolina de un coche indica al conductor cuánto le queda antes de tener que reposar. La luz roja avisa de que es inminente la necesidad de una recarga.

de eficacia

Buscamos conocer el desempeño de una cierta función, desde el punto de vista de en qué medida logramos los resultados apetecidos.

En materia de seguridad, estos indicadores suelen tomar datos de los registros de incidencias, calibrando qué ha ocurrido y cómo hemos reaccionado.

Un mal resultado en los indicadores de hechos ocurridos descubre, tarde, que tenemos un problema con las medidas preventivas, y sugiere que deberíamos mejorar estas.

Un mal resultado en los indicadores que miden la calidad de la respuesta indica que el sistema necesita mejorar sus procedimientos, bien en alcance o en eficacia.

de eficiencia

Buscamos conocer el desempeño de una cierta función, desde el punto de vista de si el consumo de recursos está proporcionado a los resultados obtenidos.

Cuando el sistema es poco eficiente, se buscarán formas más eficientes de alcanzar los mismos objetivos de eficacia. A menudo se persiguen criterios de proporcionalidad ajustando la eficacia y la eficiencia hasta encontrarnos en un punto “razonable”.

de impacto

Se busca traducir los incidentes técnicos en consecuencias para la misión última del sistema: protección de una cierta información y prestación de unos determinados servicios.

Estos indicadores son los que suelen trasladarse a los órganos de gobierno para que tomen decisiones sobre la misión del organismo, sin entrar en los detalles técnicos.

predictivos (*lead indicators*)

Se dice de los indicadores que anticipan lo que va a pasar. Es decir, no miden el pasado, sino que predicen el futuro. Más técnicamente, son los que cambian antes de que tengamos un problema de seguridad. Son muy útiles para organizar las medidas de protección dinámicamente, adaptándonos a la situación.

Por ejemplo, un semáforo en naranja es un indicador que nos permite predecir que el semáforo se va a poner en rojo en poco tiempo. Un aumento del nivel de alcohol en la sangre es un indicador que predice unos reflejos lentos y, probablemente, un accidente.

explicativos (*lagging indicators*)

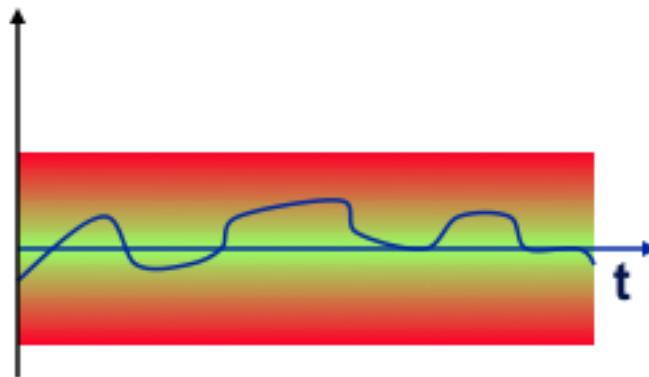
Son los que miden el pasado. Son útiles para entender lo que ha ocurrido y poder reaccionar con conocimiento de causa.

Por ejemplo, un suspenso es un indicador tardío de que no hemos estudiado lo suficiente. La fiebre es un indicador tardío de que estamos enfermos.

4.6. EXPLOTACIÓN

40. Las métricas y los indicadores hay que saber interpretarlos. Para ello se suelen aportar 3 elementos a su especificación:
41. **Objetivo.** ¿Cuál es el valor objetivo? Dado que muchos indicadores son porcentajes, es habitual que se marquen objetivos como 100% de cumplimiento o 0% de incidentes.

42. **Zona verde.** Se denomina así al rango de valores que se pueden considerar como suficientemente cercanos al objetivo como para no preocuparse.
43. **Zona amarilla.** Se denomina así al rango de valores que caen fuera de la zona verde (más alejados del objetivo) y que deben ser investigados y corregidos.
44. **Zona roja.** Se denomina así al rango de valores que caen más allá de la zona amarilla; tan alejados del objetivo que levantan las alarmas para que actuemos urgentemente.



45. No todas las medidas tienen líneas inferior y superior. Por ejemplo, las medidas de cumplimiento no tienen margen superior pues lo ideal es llegar al 100% y quedarse ahí; pero sí tendrán líneas inferiores.
46. Ojo: los números son fáciles de calcular; incluso los modelos formales son fáciles de desarrollar. Pero la última palabra la tiene la cruda realidad. Es decir, el tiempo nos dará la experiencia para saber si un conjunto de métricas es más o menos adecuado como indicador de dónde estamos y qué va a pasarnos. Por ello el sistema de métricas e indicadores debe ser, a su vez, objeto de un proceso de mejora continua de la calidad.
47. Por último, cabe recordar que a menudo manejamos el concepto de confianza, más allá del de seguridad. La confianza es una percepción subjetiva; pero en base a ella tomamos multitud de decisiones. La confianza crece con el tiempo: cada vez que el sistema se comporta como dicen (y predicen) las medidas. La confianza decae cada vez que las medidas yerran en su predicción o diagnóstico. En la medida en que los indicadores prevén los fallos, el sistema está bajo control; cada vez que una medida yerra en la predicción o mera detección, el sistema está fuera de control y el indicador bajo sospecha: hay que retirar la medida, o revisar la métrica o, simplemente, acompañarla de otras mediciones que, como colectivo, sean capaces de un mejor reporte de situación.
48. Son útiles aquellos indicadores que tienen la confianza merecida.

4.7. CUADRO DE MANDO

49. Los indicadores suelen agruparse para su presentación en cuadros, denominados “de mando”³ que típicamente resumen la salud de la organización desde cuatro puntos de vista:
- ☐ salud financiera: razonabilidad del gasto, capacidad para acometer proyectos
 - ☐ percepción de los usuarios y socios comerciales
 - ☐ capacidad para una reacción rápida y efectiva a cambios del entorno
 - ☐ capital humano: estabilidad, compromiso y capacidad para afrontar el futuro a corto y medio plazo

4.8. EL PROGRAMA DE MÉTRICAS E INDICADORES

50. Siendo las medidas una pieza crucial en la dirección de una organización, deben ser cuidadosamente organizadas con previsión para que estén en sus puestos, preparadas para actuar cuando sean requeridas.
51. Si las medidas están disponibles tarde y pobremente, son inútiles⁴. Pero si las medidas se arrojan a los gestores antes de que las necesiten o en cantidades ingentes, también devienen inútiles pues la dirección no estará preparada para cuando hagan realmente falta, sino que puede estar incluso anestesiada por falsas alarmas.
52. Es muy delicado; pero si las medidas se usan para evaluar a la vez a los sistemas y a las personas, tendremos dos problemas y es que ni los unos ni los otros serán objetivamente evaluados. Debe cuidarse escrupulosamente una clara distinción entre lo que interesa a la organización (su misión) y lo que interesa a los empleados (su sueldo y su futuro profesional). Esto lleva a un problema clásico de segregación de funciones.
53. Por último, recordemos, como se indicaba más arriba, que las métricas requieren una definición limpia, objetiva y estable en el tiempo, de forma que se pueda crear una concienciación en toda la organización que mejore la actitud del personal frente a los temas relacionados con la seguridad de los sistemas de información. La gente se puede acostumbrar a pesetas o a euros, a kilómetros o a millas; en realidad es técnicamente indiferente, pero la percepción de los seres humanos no es sólo técnica sino que hay medidas grabadas en el cerebro que proporcionan reacciones instintivas (vitales en las crisis; fuente de malentendidos a diario). Salvo estricta necesidad, es terriblemente costoso cambiar definiciones.
54. Todos estos comentarios se resumen en decir que hay que tomarse el conjunto de métricas muy profesionalmente: planificando, dedicando recursos (tiempo y medios), monitorizando el programa y manteniéndolo al día. Es decir, para disponer de métricas necesitamos un plan para empezar, para mantenerlas y para mejorarlas. No se puede improvisar.

³ El término “*balanced scorecards*” se hizo famoso con los trabajos de Norton y Kaplan relativos al gobierno de las empresas. Se denomina ‘equilibrado’ porque buscan dar una información de gobierno que recoja tanto las perspectivas a corto como a medio-largo plazo.

⁴ En realidad, también hay que ser capaces de análisis post-mortem; para lo que sí pudieran ser útiles métricas a posteriori.

4.9. METODOLOGÍA DE DESARROLLO DE NUEVOS INDICADORES

55. Como se ha indicado anteriormente, los indicadores son útiles para medir la situación de una organización y el progreso de los proyectos. Esto hace que sea difícil generalizar en un documento los indicadores útiles para una organización dada en un momento dado. Hay que personalizarlos.
56. El atributo clave para utilizar un indicador es que nos sirva para entender lo que necesitamos controlar. Por ello los indicadores deben ser consecuencia de un proceso de diseño dirigido por objetivos. A continuación se presentan 2 metodologías, bastante similares en el fondo, aunque difieran en las formas: el método GQM y el método científico.
57. Ambos métodos buscan objetivar opiniones, huyendo de creencias sin fundamento en la realidad. Lo contrario recibe muchos nombres, todos capciosos: “vivir en la nube”, “creer en la magia”, “tocar de oído” ..., planteamientos que, en general, nos llevarán a tomar decisiones cuya idoneidad para los objetivos perseguidos sea pura coincidencia.

4.9.1. MÉTODO GQM

58. **Goal.** Lo primero que necesitamos es declarar lo que deseamos hacer. Esto suelen ser aseveraciones de alto nivel, de gobierno, que no se cuestionan cómo. Simplemente, es nuestra política estar así. Y en consecuencia, queremos saber si ya lo estamos o si estamos más o menos cerca de conseguirlo.
59. **Question.** Una vez tenemos un objetivo, tendremos que concretar qué información me indica el grado de satisfacción del objetivo. Nos hacemos preguntas y, dependiendo de la respuesta, sabemos a qué atenernos. Si la respuesta a la pregunta ni me confirma ni refuta la hipótesis, entonces esa pregunta es poco útil.
60. **Metric.** Una vez sabemos la pregunta cuya respuesta necesitamos, buscaremos qué datos medir y cómo combinar los datos para dar una respuesta.
61. De esta forma tendremos unas medidas que sabemos utilizar para conocer, en última instancia, dónde estamos en relación al objetivo que nos habíamos propuesto.
62. Por ejemplo, podemos proponernos como objetivo que todos los mensajes de correo que intercambian los empleados cifran el contenido según la normativa. Ese objetivo podemos haberlo alcanzado, o no. Para saberlo podemos preguntarnos cuántos mensajes contienen información en claro que debería estar cifrada, midiendo en el servidor corporativo de correo. Esta medida nos permite saber hasta qué punto hemos alcanzado el objetivo o estamos lejos de él.
63. Por ejemplo, podemos proponernos como objetivo que todos los incidentes de seguridad se resuelvan en menos de 24 horas. Si medimos los tiempos reportados por los servicios de resolución de incidentes veremos si el objetivo está alcanzado, o no.
64. Nótese que con frecuencia no tenemos resultados ni blancos ni negros, sino tonos grises que nos dicen cuán cerca o lejos estamos del objetivo propuesto.

4.9.2. MÉTODO CIENTÍFICO

65. **Hipótesis.** Los científicos hacen hipótesis y luego intentan avalarlas o refutarlas experimentalmente. A veces se denominan “suposiciones educadas” o conjeturas.
66. **Experimentos.** Para corroborar o refutar una hipótesis, los científicos se plantean experimentos. Los experimentos deben ser tales que arrojen luz sobre la verdad o falsedad de la hipótesis; es decir, hay que pensar en experimentos cuyo resultado avale o refute la hipótesis. En el método científico, se buscan experimentos objetivos: reproducibles por cualquiera.
67. Las hipótesis se emplean para predecir el resultado de los experimentos: se predice qué se observará, de forma que si se observa lo predicho se corrobora la hipótesis, mientras que si ocurre algo diferente, la hipótesis queda en entredicho.
68. **Medidas.** Los resultados del experimento se miden para entender si cuadra o no con la predicción.
69. Por ejemplo, podemos partir de la hipótesis de que todos los mensajes de correo que intercambian los empleados cifran el contenido según la normativa. Esa hipótesis puede ser verdad, o no. Para saberlo iremos a hacer experimentos de campo, por ejemplo recopilando los mensajes que atraviesan el servidor corporativo de mensajería y midiendo cuántos mensajes contienen información en claro que debería estar cifrada. Esta medida nos permite saber hasta qué punto la hipótesis era cierta.
70. Por ejemplo, podemos partir de la hipótesis de que todos los incidentes de seguridad se resuelven en menos de 24 horas. Si medimos los tiempos reportados por los servicios de resolución de incidentes veremos si la hipótesis es correcta o incorrecta.
71. Nótese que con frecuencia no tenemos resultados ni blancos ni negros, sino tonos grises que nos dicen cuan aproximada es la hipótesis y cuánta distancia hay entre la hipótesis y la realidad.

5. DATOS

72. Esta sección recomienda una serie de datos que conviene registrar en el sistema de información que estamos analizando.
73. No se ha hecho un esfuerzo por extraer todos los datos que más tarde se emplearán en el cálculo de métricas e indicadores. Concretamente, se han obviado aquellos que son evidentes a partir de la definición del indicador.
74. Debe considerarse como conjunto mínimo recomendado, sin perjuicio de que se amplíen en función de los niveles de seguridad requeridos en cada dimensión, la categoría del sistema y los objetivos de seguridad que estamos persiguiendo en cada momento y circunstancia.

5.1. SISTEMAS

75. Por cada activo esencial, su valoración en cada dimensión de seguridad.
76. Por cada sistema, su valoración en cada dimensión de seguridad (la mayor de las de cada uno de los activos esenciales que le afectan) y la categoría del sistema.

5.2. INCIDENTES DE SEGURIDAD

77. Por cada incidente se recopilará la siguiente información que permita un tratamiento posterior.

- ☐ tiempos
- ☐ nivel de severidad
- ☐ consecuencias del incidente
- ☐ causa última que ha provocado el incidente
- ☐ incidencias del incidente

5.2.1. TIEMPOS

tiempos	
REP	reporte fecha y hora en que se reporta el incidente es cuando se abre el proceso de gestión es la referencia temporal que se usa para asignar un incidente a un intervalo temporal, independientemente de cuándo se cierre
FIN	fin cuando se cierra el incidente
procesado	FIN - REP

78. Puede haber incidentes que no se han cerrado, en cuyo caso el tiempo de procesado no está definido, empleándose en su caso el tiempo que lleva abierto (la diferencia entre REP y la fecha actual).

5.2.2. IMPACTO O CONSECUENCIAS DEL INCIDENTE

79. Para cada dimensión, se considera el conjunto de activos esenciales afectados en esa dimensión. Se calcula el impacto con la siguiente tabla

degradación del activo	nivel del activo en la dimensión de seguridad afectada		
	BAJO	MEDIO	ALTO
ALTA afectado gravemente degradación > 50%	BAJO	MEDIO	ALTO
MEDIA afectado apreciablemente degradación ~10%	-	BAJO	MEDIO
BAJA anecdótico degradación ~1%	-	-	BAJO

80. De todos los activos afectados, se considera la valoración en esa dimensión. De todas las valoraciones, nos quedaremos con la máxima.
81. Para el caso de la disponibilidad, se usará la siguiente tabla de degradación

degradación del activo	criterios
ALTA afectado gravemente degradación > 50%	— cuando hay que activar el plan de recuperación — cuando el servicio queda interrumpido más allá del RTO deseado
MEDIA afectado apreciablemente degradación ~10%	— cuando el servicio queda interrumpido del orden de un 10% del RTO deseado — cuando el servicio queda detenido de forma apreciable por los usuarios
BAJA anecdótico degradación ~1%	— cuando el servicio hay que re-arrancarlo

5.2.3. CAUSA DEL INCIDENTE

82. Se investigará la causa o causas que son la razón última (*root cause*) por la cual se ha producido el incidente. Esto significa un análisis forense para determinar en qué punto ha fallado el proceso de seguridad del sistema de información dado pie a que el incidente haya tenido lugar.
83. La siguiente tabla codifica una serie de causas que se podrán extender el futuro o según sea necesario en cada circunstancia. La última columna referencia a la medida de protección que puede estar fallando o estar insuficientemente implantada.

causas del incidente (marcar una o más)		ENS
C.1	incumplimiento o carencia de normativa de seguridad	org.1 org.2
C.2	incumplimiento o carencia de procedimientos de seguridad	org.3
C.3	incumplimiento del proceso de autorización	org.4
C.4	fallo técnico u operativo de identificación o autenticación	op.acc.1 op.acc.5
C.5	fallo técnico u operativo de los controles de acceso	op.acc.2 op.acc.4
C.6	acceso local no autorizado	op.acc.6
C.7	acceso remoto no autorizado	op.acc.7
C.8	ausencia o deficiencia de la segregación de funciones y tareas	op.acc.3
C.9	entrada de datos incorrectos que no han sido detectados a tiempo	
C.10	configuración inadecuada	op.exp.2 op.exp.3
C.11	ausencia o deficiencia de mantenimiento	op.exp.4
C.12	inadecuada ejecución de un cambio	op.exp.5
C.13	falta de concienciación del personal	mp.per.3
C.14	defectos de formación del personal	mp.per.4
C.15	puestos de trabajo no despejados	mp.eq.1
C.16	información remanente no autorizada	mp.si.5
C.17	defectos en la especificación de una aplicación SW	mp.sw
C.18	defectos en la implantación de una aplicación SW	mp.sw.2
C.19	entrada en operación de equipamiento (SW, HW, COMMS) defectuoso	mp.sw.2
C.20	servicio externo: causados por negligencia del proveedor	mp.ext.2
C.21	servicio externo: que no se han comunicado dentro de los plazos y cauces acordados	mp.exp.2
C.22	servicio externo: el proveedor responsable ha incumplido las obligaciones acordadas	mp.exp.2

5.2.4. INCIDENCIAS DEL INCIDENTE

incidencias del incidente (marcar 0 o más)	
II.1	no estaba previsto un procedimiento de actuación (diferente del escalado por defecto)
II.2	el registro de incidencias ha sido insuficiente para analizar las consecuencias

II.3	no se han podido utilizar las registros de actividad por haber desaparecido o haber sido manipulados
II.4	han requerido el sistema de garantía de suministro eléctrico, y éste ha fallado
II.5	han requerido el sistema de protección frente a incendios, y éste ha fallado
II.6	han requerido el sistema de protección frente a inundaciones, y éste ha fallado
II.91	ha sido necesario recurrir a las instalaciones alternativas y estas no han funcionado según el plan previsto
II.92	ha sido necesario recurrir a personal alternativo y esto no ha funcionado según el plan previsto
II.93	ha sido necesario recurrir al equipamiento alternativo y este no ha funcionado según el plan previsto
II.94	ha sido necesario recurrir a canales alternativos y estos no han funcionado según el plan previsto
II.95	ha sido necesario recurrir a servicios alternativos y estos no han funcionado según el plan previsto
II.96	servicio externo: ha sido necesario activar los medios alternativos y estos no han funcionado según el plan previsto

5.3. GESTIÓN DE VULNERABILIDADES

84. Las vulnerabilidades se documentarán como los incidentes, recopilándose los siguientes datos.

- Fechas de reporte y de reparación
- Estimación del impacto como en #ver incidentes#

85. Las vulnerabilidades técnicas pueden venir calificadas siguiendo las escalas CVSS (Ver Anexo C). En este caso:

Metric value (C, I or D)	Para cada activo esencial afectado, nivel del activo en la dimensión de seguridad afectada		
	BAJO	MEDIO	ALTO
C - COMPLETE	BAJO	MEDIO	ALTO
P - PARTIAL	-	BAJO	MEDIO
N - NONE	-	-	-

5.4. AUDITORÍAS

86. Hay auditorías de negocio y auditorías técnicas. De unas y otras, de forma diferenciada, se recopilarán los siguientes datos.

- Fechas de reporte y de reparación

- Estimación del impacto como en #ver incidentes#

5.5. CONTINUIDAD DEL SERVICIO

87. Por cada servicio

Nivel requerido en disponibilidad
<input type="checkbox"/> alto
<input type="checkbox"/> medio
<input type="checkbox"/> bajo
Fechas de realización o actualización de un análisis de impacto.
Fechas de realización de ejercicios
Número de fallos detectados en cada ejercicio, clasificados por severidad y consecuencias como se indicó para los incidentes.

6. MÉTRICAS

88. En esta sección se elaboran algunas métricas que se emplearán para derivar indicadores a partir de los datos o medidas realizadas sobre el sistema.

6.1. PORCENTAJES

89. Son frecuentes los indicadores calculados como la fracción de elementos que cumplen una cierta condición sobre el total de elementos relevantes.
90. A veces un porcentaje es suficiente, como 0%, 33% o 100%.
91. Siempre que sea posible, es preferible presentarlo como fracción, numerador / denominador, siendo ambos valores reales, para poder acumular datos:

Por ejemplo, si la proporción de incidentes de tipo X en un sistema es $n1/d1$ y en otro sistema es $n2/d2$, la proporción combinando ambos sistemas es

$$\text{combinación}(n1/d1, n2/d2) = (n1+n2) / (d1+d2)$$

6.2. CALIDAD DEL SERVICIO

92. Cuando queremos medir la calidad del servicio desde el punto de vista del usuario final, es habitual medir el porcentaje de tiempo que el servicio está disponible (por ejemplo, 99%).
93. Pero esta métrica esconde algunos aspectos importantes
- no es lo mismo estar parado 2s cada minuto (96.7%) que estar parado 1 día al mes (96.7%)
 - no es lo mismo estar parado a las 2 de la madrugada que a las 12 de la mañana
 - no siempre el comportamiento es binario (sí funciona, no funciona); a veces funciona lentamente

- a veces el servicio parece activo pero no se presta servicio efectivo; por ejemplo, cuando los servidores y las líneas están operativos, pero fallan los datos porque están pendientes de una recuperación
- 94. Una percepción más adecuada la podemos obtener midiendo el tiempo de respuesta del sistema a una cierta petición que consideraremos de referencia (puede ser generada regularmente por un usuario virtual, ajustando la frecuencia de muestreo a la carga normal de trabajo durante días, noches y días de la semana, o incluso periodos críticos).
- 95. Disponiendo de la serie de tiempos de respuesta, podemos calcular algunos indicadores útiles

indicador	descripción
Tmin	mínimo: tiempo más breve que se tarda en responder
T(10)	tiempo en el que el 10% de las peticiones están resueltas
T(50)	tiempo en el que el 50% de las peticiones están resueltas
T(90)	tiempo en el que el 90% de las peticiones están resueltas
T(100) Tmax	tiempo en el que el 100% de las peticiones están resueltas; es el tiempo máximo de respuesta

6.3. MADUREZ

96. Los niveles de madurez se describen en muchos lugares (ver referencias en el anexo):

L0 - Inexistente

En el nivel L0 de madurez no hay nada.

L1 - Inicial / ad hoc

En el nivel L1 de madurez, las salvaguardas existen, pero no se gestionan. El éxito depende de buena suerte. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta.

El éxito del nivel L1 depende de tener personal de la alta calidad.

L2 - Reproducible pero intuitivo

En el nivel L2 de madurez, la eficacia de las salvaguardas depende de la buena suerte y de la buena voluntad de las personas. Los éxitos son repetibles, pero no hay plan para los incidentes más allá de la reacción heroica.

Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.

L3 - Proceso definido

Se despliegan y se gestionan las salvaguardas. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular de las protecciones. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado).

El éxito es algo más que buena suerte: se merece.

L4 – Gestionado y medible

Usando medidas de campo, la dirección puede controlar empíricamente la eficacia y la efectividad de las salvaguardas. En particular, la dirección puede fijar metas cuantitativas de la calidad. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza es cuantitativa, mientras que en el nivel L3, la confianza era solamente cualitativa.

L5 - Optimizado

El nivel L5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora de los procesos. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.

6.3.1. MADUREZ DE UNA ACTIVIDAD O PROCESO

97. Se establece un objetivo de madurez que hace de referencia para calcular umbrales.
98. Inspeccionado el sistema, tendremos una estimación del nivel de madurez, sencillo o un rango) para cada actividad.
99. Para cada actividad se estimará el delta entre el nivel de madurez requerido y el actual, tomándose la media cuando se trate de rangos. Se marcará como zona verde si el delta es mayor que -1, como amarilla si está entre -1 y -2, y roja si es menor o igual que -2.

ejemplo			
medido	objetivo	delta	zona
L0	L3	$0-3 = -3$	roja
L1	L3	$1-3 = -2$	roja
L2	L3	$2-3 = -1$	amarilla
L3	L3	$3-3 = 0$	verde
L4	L3	$4-3 = +1$	verde
L5	L3	$5-3 = +2$	verde
L1-L3	L3	$(1+3)/2 - 3 = -1,5$	amarilla

6.3.2. MADUREZ COMPUESTA

100. Para componer un conjunto de medidas, por ejemplo, [mp] o [mp.if], se recogerá
 - el valor mínimo del delta de sus componentes
 - la zona será la peor:
 - roja si hay algún componente en zona roja;
 - amarilla si no hay componentes rojos pero sí hay componentes amarillos
 - verde si no hay componentes rojos ni amarillos

6.4. LEGIBILIDAD DE LA DOCUMENTACIÓN

101. Regularmente se pregunta a los usuarios a los que va dirigida una cierta documentación (en nuestro caso, normativa y procedimientos de seguridad) por la facilidad⁵ con la que se entienden los textos proporcionados.
102. Las respuestas se valorarán en una escala de 1 a 5:
- [5] Está meridianamente claro, expresándose en pocas palabras. Da gusto.
 - [4] Entre [3] y [4].
 - [3] Normal: más o menos creo que se lo que se quiere decir. Lo interpreto con cierta inseguridad. Genera inseguridad.
 - [2] Entre [1] y [3].
 - [1] No se entiende nada. Lo mezcla todo y no se sabe a dónde se quiere ir a parar. Genera confusión.
103. Para calcular la legibilidad de un documento a partir de un conjunto de encuestas, se usarán 2 estadísticos:
- la mediana de las puntuaciones obtenidas
 - la desviación estándar de las puntuaciones obtenidas
104. Si la media o la mediana están por debajo de 3, deberíamos revisar la documentación, reescribiéndola de forma más clara para los lectores previstos.
105. Si la desviación estándar es elevada, deberíamos revisar el colectivo al que va destinada pues puede que sea en sí heterogéneos y la documentación deba fraccionarse en partes o incluso redactarse de varias formas para que llegue a cada colectivo específico.

6.5. UTILIDAD DE LA DOCUMENTACIÓN

106. Regularmente se pregunta a los usuarios a los que va dirigida una cierta documentación (en nuestro caso, normativa y procedimientos de seguridad) por la utilidad que se le saca a los textos proporcionados.
107. Las respuestas se valorarán en una escala de 1 a 5:
- [5] Da gusto: uno encuentra rápidamente respuesta a lo que necesita.
 - [4] Entre [3] y [4].
 - [3] Normal: cuesta trabajo descifrarlo, pero leyéndolo con cuidado al final está explicado.
 - [2] Entre [1] y [3].
 - [1] No vale para nada. No está claro a qué caso se aplica cada cosa y da muchas cosas por sobreentendidas.
108. Para calcular la utilidad de un documento a partir de un conjunto de encuestas, se usarán 2 estadísticos:
- la mediana de las puntuaciones obtenidas

⁵ Realmente no nos interesan métricas sintácticas o semánticas, ni basadas en el empleo del lenguaje en general. Se trata de textos muy específicos para lectores muy determinados y lo que debe inquietarnos es que no sean capaces de leerlo y entenderlo adecuadamente. El lenguaje y las palabras pueden ser propios de la Organización, e incluso críptico para personas de otro ámbito.

la desviación estándar de las puntuaciones obtenidas

109. Si la media o la mediana están por debajo de 3, deberíamos revisar la documentación para ajustarla a los casos de uso previstos.
110. Si la desviación estándar es elevada, deberíamos revisar los escenarios a los que se pretende aplicar pues puede que sean en sí heterogéneos y la documentación deba fraccionarse en partes o incluso redactarse de varias formas para que se adapte a cada caso de aplicación y los lectores sepan cuándo aplica cada cosa que se dice.

7. INDICADORES ESTÁNDAR

7.1. ANEXO II DEL ESQUEMA NACIONAL DE SEGURIDAD

111. El ENS establece una serie de medidas de protección en su Anexo II. En esta sección se plantea cómo medir dos facetas de la implantación de dichas medidas:
112. **Índice de madurez.** Para evaluar la implantación de las medidas en la organización.
113. **Índice de cumplimiento.** Para evaluar la satisfacción de las medidas que se exigen en función de los niveles de seguridad o la categoría del sistema.
114. Se establece un nivel de madurez de referencia para cada medida de protección del Anexo II del ENS. Se sigue una regla simple:

categoría del sistema	nivel de madurez de referencia
BAJA	L2 – reproducible pero intuitivo
MEDIA	L3 – proceso definido
ALTA	L4 – gestionado y medible

7.1.1. ÍNDICE DE MADUREZ DEL ENS

115. Se obtiene aplicando el algoritmo anterior a todas las medidas del Anexo II, excepto aquellas que no apliquen.
116. Las medidas que se considere que no aplican deben estar justificadas a efectos de auditoría.

117. Ejemplo para un sistema de categoría media:

Anexo II - Medidas de protección		2011	plan	objetivo
org	Marco organizativo	L0-L5	L2-L5	L3
op	Marco operacional	L0-L5	L0-L5	L3
op.pl	Planificación	L0-L5	L3-L5	L3
op.acc	Control de acceso	L0-L5	L2-L5	L3
op.exp	Explotación	L0-L5	L0-L5	L3
op.ext	Servicios externos	L1-L5	L4-L5	L3
op.cont	Continuidad del servicio	L0-L3	L2-L4	L3
op.mon	Monitorización del sistema	L0	L3	L3
mp	Medidas de protección	L0-L5	L1-L5	L3
mp.if	Protección de las instalaciones e infraestructuras	L0-L5	L3-L5	L3
mp.per	Gestión del personal	L0-L5	L2-L5	L3
mp.eq	Protección de los equipos	L0-L1	L3-L5	L3
mp.com	Protección de las comunicaciones	L0-L5	L1-L5	L3
mp.si	Protección de los soportes de información	L1	L2	L3
mp.sw	Protección de las aplicaciones informáticas (SW)	L1-L2	L3-L5	L3
mp.info	Protección de la información	L0-L5	L2-L5	L3
mp.s	Protección de los servicios	L0-L2	L2-L5	L3

7.1.2. ÍNDICE DE CUMPLIMIENTO DEL ENS

118. Se obtiene aplicando el algoritmo anterior al conjunto mínimo de medidas que se exigen del Anexo II, en función de los niveles de seguridad y la categoría del sistema evaluado como se indica en el Anexo I, exceptuando aquellas que no apliquen.

119. Las medidas que se considere que no aplican deben estar justificadas a efectos de auditoría.

7.2. RD 1720/2007 DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

120. El RD 1720 establece una serie de medidas de protección en función de una serie de consideraciones sobre la naturaleza de los datos y la finalidad de su tratamiento.

121. Existe amplia jurisprudencia sobre cómo aplicar el decreto en diferentes situaciones. No es esta guía el lugar para recoger qué medidas de protección aplican o no en un caso concreto, remitiéndose al lector al estudio del decreto y la jurisprudencia que sea de aplicación.

122. Una vez determinado qué medidas aplican, en esta sección se plantea cómo medir dos facetas de la implantación de dichas medidas:

123. **Índice de madurez.** Para evaluar la implantación de las medidas en la organización.

124. **Índice de cumplimiento.** Para evaluar la satisfacción de las medidas que se exigen en función de la categoría del sistema.

125. Se establece un nivel de madurez de referencia para cada medida de protección que sea aplicable. Se sigue una regla simple:

categoría del sistema	nivel de madurez de referencia
BAJA	L2 – reproducible pero intuitivo
MEDIA	L3 – proceso definido
ALTA	L4 – gestionado y medible

7.2.1. ÍNDICE DE MADUREZ DEL RD1720

126. Se obtiene aplicando el algoritmo anterior a todas las medidas aplicables.
127. Las medidas que se considere que no aplican deben estar justificadas a efectos de auditoría.

7.2.2. ÍNDICE DE CUMPLIMIENTO DEL RD1720

128. Se obtiene aplicando el algoritmo anterior al conjunto mínimo de medidas que se exigen obligatoriamente en función de la naturaleza de los datos y la finalidad del tratamiento, teniendo en cuenta la jurisprudencia que sea de aplicación.
129. Las medidas que se considere que no aplican deben estar justificadas a efectos de auditoría.

7.3. ORGANIZACIÓN**130. Normativa**

- Proporción de normas implantadas sobre normas previstas
- Número de violaciones graves de la normativa de seguridad reportadas
- Encuesta de legibilidad percibida por los usuarios.
- Encuesta de utilidad percibida por los usuarios.

131. Procedimientos

- Proporción de normas implantadas sobre normas previstas
- Encuesta de legibilidad percibida por los usuarios.
- Encuesta de utilidad percibida por los usuarios.

7.4. GESTIÓN DE INCIDENCIAS

132. Las incidencias miden la inseguridad del sistema. Son una medida indirecta de la inseguridad del sistema. Podemos decir informalmente que en un sistema perfectamente seguro no hay incidencias relevantes, de forma que cuantas más y más graves sean las incidencias, más inseguro es nuestro sistema.
133. Los datos recopilados según la sección “5.2. Incidentes de seguridad” permiten consolidar el número de incidentes por causas y analizar otras incidencias del incidente.
134. El conjunto de incidentes a consolidar depende de lo que necesitemos en cada momento.
135. Una métrica habitual es el número acumulado de incidentes por impacto. Por ejemplo:

impacto	# incidentes	# acumulado
ALTO	12	12
MEDIO	50	62
BAJO	200	262

es el indicador más habitual

136. Otra métrica habitual es analizar la distribución de los tiempos de respuesta o procesado, entendido éste como el lapso de tiempo desde que se reporta el incidente hasta que se cierra.
137. Indicadores sobre un conjunto; típicamente, sobre los incidentes con un impacto I_ALTO:

indicador	descripción
Tmin	mínimo: incidente más rápido en resolver
T(10)	tiempo en el que el 10% de los incidentes están cerrados
T(50)	tiempo en el que el 50% de los incidentes están cerrados; es la mediana
T(90)	tiempo en el que el 90% de los incidentes están cerrados
T(100) Tmax	tiempo en el que el 100% de los incidentes están cerrados; es el tiempo máximo de respuesta

Los indicadores Tmin y Tmax pueden ser más causa de la buena o de la mala fortuna que de la destreza de la organización para resolver los incidentes. Los indicadores sobre un porcentaje eliminan el efecto de los casos extraordinarios. Los más significativos suelen ser

- T(50) como medida del desempeño medio del sistema
- T(90) como medida de deficiencias en el sistema

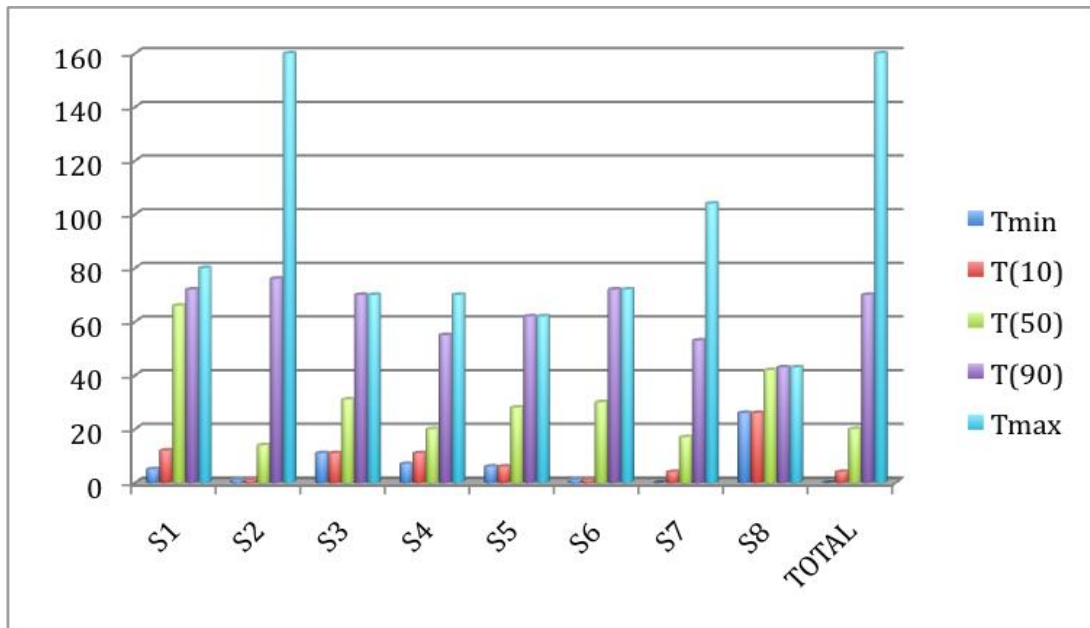
138. Ejemplo

datos	5, 12, 35, 36, 41, 63, 66, 66, 67, 69, 69, 72, 80
Tmin	5
T(10)	12
T(50)	66
T(90)	72
Tmax	80

139. Si tenemos varios sistemas y queremos consolidarlos, podemos calcular los indicadores anteriores para los incidentes de cada sistema y para el conjunto que uno todos los incidentes de todos los sistemas (debe aplicarse la unión de conjuntos, eliminado duplicados: aquellos incidentes que afectan a varios sistemas).

140. Ejemplo. Se marcan en verde aquellos sistemas que están por debajo de la “media” del conjunto de sistemas, y en amarillo los que están por encima. Nótese cómo se amortigua la “mala suerte” de los sistemas S2 y, en menor medida, S7. También se amortigua la “buena suerte” de los sistemas S2, S6 y S7.

sistema	Tmin	T(10)	T(50)	T(90)	Tmax
S1	5	12	66	72	80
S2	1	1	14	76	160
S3	11	11	31	70	70
S4	7	11	20	55	70
S5	6	6	28	62	62
S6	1	1	30	72	72
S7	0	4	17	53	104
S8	26	26	42	43	43
TOTAL	0	4	20	70	160



7.5. DISPONIBILIDAD DE LOS SERVICIOS

141. Porcentaje del tiempo que el servicio está disponible.

142. Sobre un servicio de referencia:

- T(50) - tiempo en el que el 50% de las peticiones están resueltas
- T(90) - tiempo en el que el 90% de las peticiones están resueltas

8. REPORTE ANUAL

143. En este capítulo se fijan los datos que se remitirán anualmente para poder analizar el estado de seguridad de un conjunto de sistemas. Es decir, para ejercer lo prescrito en el Artículo 35 del ENS, arriba citado.

8.1. INVENTARIO

144. Por cada activo esencial, su valoración en cada dimensión de seguridad.

145. Por cada sistema, su valoración en cada dimensión de seguridad (la mayor de las de cada uno de los activos esenciales que le afectan) y la categoría del sistema.

146. Declaración de aplicabilidad de las medidas del Anexo II del ENS.

147. Nivel de madurez de las medidas aplicables de protección del Anexo II del ENS.

148. Tiempo de respuesta a los incidentes de seguridad. Se indicarán T(50) y T(90) para los incidentes del impacto más alto que puede sufrir el sistema (esto es función de la categoría).

8.2. ANÁLISIS DE SITUACIÓN

8.2.1. DOCUMENTACIÓN DE SEGURIDAD

149. Madurez del proceso [org.1].

150. Normativa

- Proporción de normas implantadas.

- Madurez del proceso [org.2].

151. Procedimientos operacionales de seguridad

- Proporción de procedimientos implantados.

- Madurez del proceso [org.3]

8.2.2. ORGANIZACIÓN

152. Análisis de riesgos

- Porcentaje de sistemas que han sido objeto de un análisis de riesgos en el último año.

153. Declaración de aplicabilidad

- Porcentaje de sistemas que disfrutan de una declaración de aplicabilidad de las medidas en el Anexo II del ENS.

154. Plan de adecuación

- Porcentaje de sistemas que disfrutan de un plan de adecuación

8.2.3. PROCESO DE AUTORIZACIÓN

155. Madurez del proceso [org.4].

8.2.4. MEDIDAS DE PROTECCIÓN

- 156. Índice de madurez del Anexo II del ENS.
- 157. Índice de cumplimiento del Anexo II del ENS.

8.2.5. CERTIFICACIONES

- 158. Porcentaje de sistemas que gozan de una certificación de seguridad actualizada al último año. Sólo en sistemas de categoría ALTA:

8.2.6. ANÁLISIS DE INCIDENTES

- 159. Para los incidentes del más alto impacto que pueda sufrir el sistema (depende de la categoría).
 - T(50) de los incidentes
 - T(90) de los incidentes
 - Número de incidentes que llevan más de 30 días pendientes de cerrar

8.2.7. AUDITORÍAS DE NEGOCIO

- 160. Sólo para sistemas de categoría media o alta.
 - Porcentaje de sistemas que han sido objeto de una auditoría de negocio en el último año.
 - Número de defectos de impacto ALTO
 - Número de defectos de impacto MEDIO

8.2.8. AUDITORÍAS TÉCNICAS

- 161. Sólo para sistemas de categoría media o alta.
 - Porcentaje de sistemas que han sido objeto de una auditoría técnica en el último año.
 - Número de defectos de impacto ALTO
 - Número de defectos de impacto MEDIO

9. CUADROS DE MANDO

162. Los cuadros de mando buscan una síntesis de pocos indicadores en pocas áreas que den una visión de muy alto nivel del estado de seguridad del organismo.
163. Los cuadros de mando son muy famosos en escuelas de negocio, sobre todo a partir del artículo de Kaplan y Norton en 1992, en el que buscaban ampliar la perspectiva de una empresa para que se centrara en algo más que en los indicadores económicos. Concretamente identificaron cuatro áreas cuya satisfacción debía estar razonablemente equilibrada:
- **Financial.** To succeed financially, how should we appear to our shareholders?
 - **Customer.** To achieve our vision, how should we appear to our customers?
 - **Internal Business Process.** To satisfy our shareholders and customers, what business processes must we excel at?
 - **Learning and Growth.** To achieve our vision, how will we sustain our ability to change and improve?

9.1. ÁREAS PROPUESTAS E INDICADORES

164. Teniendo en cuenta que el ENS se refiere en todo momento a servicios de la administración electrónica, quizás podemos olvidar los aspectos financieros de los organismos públicos, que se tratan en otros ámbitos. También debemos reemplazar accionistas por ciudadanos que pagan sus impuestos y desean una racionalidad en el gasto; clientes por administrados, que desean unos servicios adecuados y mantener el cuarto punto como sostenibilidad a medio plazo de la calidad de los servicios públicos.

9.1.1. RECURSOS

165. Ver Anexo D.
- Proporción de recursos humanos dedicados a seguridad de los sistemas (ver 10.8.1)
 - Proporción de recursos económicos dedicados a seguridad de los sistemas (ver 10.8.2)

9.1.2. PERCEPCIÓN EXTERNA – CALIDAD DEL SERVICIO PRESTADO

166. Calidad de los servicios. Ver apartado 6.2 de la presente guía.

9.1.3. EXCELENCIA INTERNA

167. Se puede medir como madurez compuesta de ciertos conjuntos de medidas de seguridad:
168. Cumplimiento
- Índices de madurez y cumplimiento del ENS. Ver apartado 7.1 de la presente guía.
 - Índices de madurez y cumplimiento del RD 1720 de protección de datos de carácter personal. Ver apartado 7.2 de la presente guía.
 - Análisis de los resultados de auditoría (ver 8.2.7 y 8.2.8).
169. Identificación, autenticación y control de acceso

- [org.4] Proceso de autorización
- [op.acc] Control de acceso
- [mp.if.2] Identificación de las personas

170. Gestión de incidentes

- [op.exp.7] Gestión de incidencias
- Indicadores del proceso de gestión de incidentes:
 - T(50) de los incidentes del impacto más alto posible en el sistema
 - T(50) de los incidentes del impacto más alto posible en el sistema
 - número de incidentes del impacto más alto posible en el sistema que llevan más de 30 días sin cerrar

171. Servicios externos

- [op.ext.1] Contratación y acuerdos de nivel de servicio
- [op.ext.2] Gestión diaria

172. Continuidad

- [op.cont] Continuidad del servicio
- [op.ext.9] Medios alternativos (proveedores)
- [mp.if.9] Instalaciones alternativas
- [mp.per.9] Personal alternativo
- [mp.eq.9] Medios alternativos (equipos)
- [mp.com.9] Medios alternativos (comunicaciones)
- [mp.info.9] Copias de seguridad (backups)
- [mp.s.9] Medios alternativos (servicios)

9.1.4. ORIENTACIÓN FUTURA

173. Gestión de riesgos y planificación

- [op.exp.1] Inventario de activos
- [op.pl] Planificación
- [mp.if.1] Áreas separadas y con control de acceso

174. Recursos humanos

- [mp.per.3] Concienciación
- [mp.per.4] Formación

10. ORIENTACIONES PRÁCTICAS

175. Todas las guías de métricas e indicadores son prolijas. Esta no parece ser la excepción. Esa prolijidad permite abarcar múltiples situaciones y adelantar métricas e indicadores que puedan ser reutilizados y, sobre todo, que haya un entendimiento común para comparar unos sistemas con otros.
176. Pero si no queremos que la perfección futura nos impida empezar, es decir si somos de los que pensamos que siempre hay algo entre no tener nada y tenerlo todo perfecto, entonces nos conviene tener una perspectiva evolutiva desde un sistema de métricas rudimentario y un sistema de métricas maduro.

10.1. ¿POR DÓNDE EMPEZAR?

177. Probablemente no se puede hacer nada sin haber satisfecho los pasos del Anexo I del ENS:
- identificación de los activos esenciales
 - valoración de los activos esenciales
 - categorización del sistema (o de los sistemas si se prefiere trocear el problema)
178. Una vez tenemos identificado el problema podemos determinar las medidas del Anexo II que son de aplicación y hacer una primera evaluación de su madurez.
179. Con esto podemos pergeñar un cuadro de mando, en la línea de lo propuesto en el capítulo anterior. Este paso es muy importante pues estamos estableciendo el procedimiento de reporte desde los órganos técnicos a los órganos de gobierno, siempre pivotando alrededor del responsable de la seguridad.
180. En este primer cuadro de mando, probablemente
- los datos sean tentativos y poco precisos, pero marcando una tendencia
 - las métricas de disponibilidad y análisis de incidentes estén vacías.
181. Podemos decir que es un cuadro de mando centrado en el cumplimiento.

10.2. ¿CÓMO SEGUIR?

182. El siguiente paso será montar un sistema de gestión de incidentes, automatizado para poder meter en una base de datos la información que recolectemos según se indica en la 5.2. Nótese que estos datos se pueden explotar desde el segundo día; pero empezarán a ser significativos cuando tengamos cubierto 1 año de operación.
183. Con estos datos seremos capaces de disponer de métricas de eficacia y el cuadro de mando se enriquece proporcionalmente.
184. A partir de aquí podemos lanzar actividades estándar, priorizadas en base al valor que soporta el sistema en cada dimensión de seguridad:
- indicadores de disponibilidad
 - indicadores de continuidad
 - realización y análisis de auditorías

10.3. PROYECTOS DE SEGURIDAD

185. Por diversos motivos, la Organización puede verse envuelta en un proyecto de [mejora de la] seguridad. Bien sea por mejorar los indicadores de cumplimiento, bien sea por mejorar los indicadores de eficacia. Si estos proyectos se dilatan en el tiempo (requieren meses o años) es conveniente entrar en medidas coyunturales que pauten el progreso.
186. Si se trata de mejorar los indicadores de eficacia, se puede recurrir a explotar la base de datos de incidentes, buscando reducir el número de incidentes de un cierto tipo o los tiempos de cierre de los mismos.
187. En estos proyectos, esta guía también ayuda a elegir los indicadores apropiados (ver 7) siguiendo bien el método GQM o el método científico para racionalizar lo que vamos a medir y cómo lo vamos a interpretar. También se pueden reutilizar las métricas de la 6.
188. Es habitual encontrar indicadores de este tenor:

Identificación y autenticación:

- Proporción de contraseñas débiles (que son adivinadas)
- Proporción de cuentas autenticadas por contraseña
- Proporción de cuentas autenticadas por medio de token
- Proporción de cuentas autenticadas biométricamente
- Proporción de cuentas que emplean 2 factores de autenticación
- Proporción de cuentas que emplean 3 factores de autenticación
- Proporción de cuentas autenticadas por contraseña con validez limitada
- Proporción de cuentas autenticadas por contraseña que han expirado

Control de la configuración:

- Proporción de equipos (HW y comunicaciones) sujetos a una configuración de seguridad.
- Número de equipos en los que se ha hallado SW instalado sin autorización
- Número de equipos en los que se ha hallado HW instalado sin autorización
- Número de comunicaciones que se han descubierto conectadas a la red sin autorización (incluyendo módems, ADSL, WiFi, gsm, 3g, ...)

Equipos portátiles:

- Proporción de equipos sujetos a una configuración de seguridad
- Proporción de equipos que cifran la información almacenada
- Proporción de equipos que protegen el acceso con contraseña.
- Proporción de equipos que protegen el acceso con token certificado.
- Proporción de equipos que protegen el acceso con biometría.
- Proporción de equipos con protección frente a código dañino.

- Número de portátiles perdidos en el último año

Continuidad de operaciones

- Proporción de servicios que cuentan con un contrato de prestación que incluye un análisis de impacto y un plan de continuidad coordinado.
- Proporción de servicios que disponen de un plan de funcionamiento alternativo en caso de fallo de los medios habituales
- Proporción de servicios en los que se ha realizado o actualizado un análisis de impacto en el último año.
- Proporción de servicios para los que existe un plan de continuidad aprobado.
- Tasa anual de ejercicios
- Proporción de instalaciones con medidas que garanticen la continuidad del suministro eléctrico.
- Proporción de instalaciones con medidas de protección frente a incendios homologadas
- Proporción de instalaciones con medidas de protección frente a inundaciones.
- Proporción de instalaciones para las que hay previstas instalaciones alternativas.
- Proporción de personal para el que se dispone de medios alternativos.
- Proporción de equipos que disponen de medios alternativos.
- Proporción de canales de comunicación que disponen de medios alternativos.
- Porcentaje de los elementos de información que están sujetos a un plan regular de realización de copias de seguridad
- Proporción de servicios que disponen de medios alternativos.

ANEXO A - GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Cuadro de mando

Conjunto de indicadores para resumir el desempeño de un sistema.

Scorecard. (1) A printed program or card enabling a spectator to identify players and record the progress of a game or competition. (2) A small card used to record one's own performance in sports such as golf. [Herrmann:2007]

Datos

Representación de la información usando algún formato que permita su comunicación, interpretación, almacenamiento y procesamiento automático.

Data. (1) Representations of information or objects, in any form. (2) The representation of information in a manner suitable for the communication, interpretation, storage, or processing. [Herrmann:2007].

Datos de carácter personal

Cualquier información concerniente a personas físicas identificadas o identificables. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Indicador

(1) Instrumento que se utiliza para monitorizar la operación de un ingenio, en sentido general. (2) Química. Un elemento que cambia de color o estructura cuando se dan ciertas circunstancias, sirviendo como mecanismo de detección. (3) Economía. Conjunto de estadísticos que sirven para saber cómo está y a dónde se encamina la economía.

Indicator. (1) An instrument used to monitor the operation or condition of an engine, furnace, electrical network, reservoir, or other physical system; a meter or gauge. (2) Chemistry. A chemical compound that changes color and structure when exposed to certain conditions and is therefore useful for chemical tests. (3) Ecology: A plant or animal whose existence in an area is strongly indicative of specific environmental conditions. (4) Any of various statistical values that together provide an indication of the condition or direction of the economy. [Herrmann:2007].

Medición

(1) Proceso consistente en la asignación de números o símbolos a entidades de la realidad de forma que nos permitan describir dichas entidades de acuerdo a unas reglas claramente definidas. (2) Comparación de una propiedad de un objeto con una propiedad similar en otro objeto que se usa de referencia.

Measurement. (1) The process by which numbers or symbols are assigned to entities in the real world in such a way as to describe them according to clearly defined rules. (2) A process that is a repeated application of a test method using a measuring system. (3) The comparison of a property of an object to a similar property of a standard reference. Measurements are effective when they are used either to orient decisions, to define corrective actions, or to get a better understanding of casual relationships between intended expectations and observed facts. [Herrmann:2007].

Medida

El número o símbolo asignado a una entidad como resultado de un proceso de medición. La medida sirve para caracterizar un atributo de la entidad.

Measure. The number or symbol assigned to an entity by the measurement process in order to characterize an attribute. [Herrmann:2007].

Métrica

Por una parte es una unidad de medida (como lo es, por ejemplo, el sistema métrico decimal). Por otra parte, suele tener una finalidad, entendiéndose como una herramienta para entender la realidad y tomar decisiones al respecto.

Metric. (1) A proposed measure or unit of measure. (2) Tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. [Herrmann:2007].

Servicio

Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Seguridad de los sistemas de información

Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. [CNSS-4009].

Sistema de información

Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. ENS.

Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. 44 U.S.C., Sec. 3502; OMB Circular A-130, Appendix III.

Sistema TIC

Sistema de información que emplea tecnologías de la información y de las comunicaciones.

ABREVIATURAS

CCN	Centro Criptológico Nacional
ENS	Esquema Nacional de Seguridad
FIPS	Federal Information Processing Standards
ISO	International Organization for Standardization
STIC	Seguridad TIC
TIC	Tecnologías de la Información y las Comunicaciones

ANEXO B - REFERENCIAS

- ❑ Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. BOE de 29 de enero de 2010.

Guías y normas

- ❑ [CNSS-4009]
Committee on National Security Systems
National Information Assurance (IA) Glossary
CNSS Instruction No. 4009, 26 April 2010
- ❑ ISO/IEC 27004:2009
Information technology – Security techniques – Information security risk management - Measurement
- ❑ NIST SP 800-55
Performance Measurement Guide for Information Security
Rev 1, July 2008
- ❑ ISO/IEC 21827:2002 - Tecnología de información - Ingeniería de seguridad de los sistemas - Modelo de madurez de las capacidades (SSE-CMM®)
- ❑ CMMI – Capability Maturity Model Integration
Software Engineering Institute, Carnegie Mellon
<http://www.sei.cmu.edu/cmmi/start/>

Libros

- ❑ [Brotby:2009]
Brotby, W. Krag, Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement, Auerbach Publications, 2009.
- ❑ [CSI:2008]
CSI Computer Crime & Security Survey de 2008
- ❑ [CSI:2011]
2010 / 2011 - CSI Computer Crime and Security Survey
- ❑ [Hayden:2010]
Hayden, Lance, IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data, McGraw-Hill Osborne Media, 2010.
- ❑ [Herrmann:2007]
Herrmann, Debra S., Complete Guide to Security and Privacy Metrics, Auerbach Publications, 2007.
- ❑ [Jaquith:2007]
Jaquith, Andrew R., Security Metrics – Replacing Fear, Uncertainty and Doubt, Addison-Wesley Professional, 2007.
- ❑ [Kaplan:1992]
Kaplan R.S. and Norton D.P., The Balanced Scorecard: Measures That Drive Performance, Harvard Business Review, January-February 1992, pp 71-79.

Sitios web

- ☐ KPI Library
<http://kpilibrary.com/>
- ☐ Metrics Center
<https://www.metricscenter.org/>
<https://www.metricscenter.net/>
- ☐ Security Metrics
<http://www.securitymetrics.org/>
- ☐ National Vulnerability Database Home
<http://nvd.nist.gov/>

ANNEXO C – CVSS

189. The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS consists of 3 groups: Base, Temporal and Environmental. Each group produces a numeric score ranging from 0 to 10, and a Vector, a compressed textual representation that reflects the values used to derive the score. The Base group represents the intrinsic qualities of a vulnerability. The Temporal group reflects the characteristics of a vulnerability that change over time. The Environmental group represents the characteristics of a vulnerability that are unique to any user's environment. CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit by adopting this common language of scoring IT vulnerabilities.

10.4. CONFIDENTIALITY IMPACT (C)

190. This metric measures the impact on confidentiality of a successfully exploited vulnerability.
191. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized ones. The possible values for this metric are listed in Table 4. Increased confidentiality impact increases the vulnerability score.

Metric Value	Description
None (N)	There is no impact to the confidentiality of the system.
Partial (P)	There is considerable informational disclosure. Access to some system files is possible, but the attacker does not have control over what is obtained, or the scope of the loss is constrained. An example is a vulnerability that divulges only certain tables in a database.
Complete (C)	There is total information disclosure, resulting in all system files being revealed. The attacker is able to read all of the system's data (memory, files, etc.)

10.5. INTEGRITY IMPACT (I)

192. This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and guaranteed veracity of information. The possible values for this metric are listed in Table 5. Increased integrity impact increases the vulnerability score.

Metric Value	Description
None (N)	There is no impact to the integrity of the system.

Partial (P)	Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited. For example, system or application files may be overwritten or modified, but either the attacker has no control over which files are affected or the attacker can modify files within only a limited context or scope.
Complete (C)	There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised. The attacker is able to modify any files on the target system.

10.6. AVAILABILITY IMPACT (A)

193. This metric measures the impact to availability of a successfully exploited vulnerability. Availability refers to the accessibility of information resources. Attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of a system. The possible values for this metric are listed in Table 6. Increased availability impact increases the vulnerability score.

Metric Value	Description
None (N)	There is no impact to the availability of the system.
Partial (P)	There is reduced performance or interruptions in resource availability. An example is a network-based flood attack that permits a limited number of successful connections to an Internet service.
Complete (C)	There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.

ANEXO D – RECURSOS

194. Se trata de calibrar el consumo de recursos dedicados a seguridad de la información.

- humanos: personas, medidas como hombre-año
- económicos: medidos como euros

195. de forma que podamos

- tener una idea a nivel de organismo y agregarlo a nivel de colectivo (CSAE)
- estimar la proporción de recursos en función del tamaño del sistema de información
- estimar la relación entre los recursos dedicados y la eficacia del sistema de protección

196. Mediremos los recursos dedicados a

- TIC – Tecnologías de Información y Comunicaciones; es decir, sistemas de información
- STIC – Seguridad de las TIC; es decir, seguridad de la información

197. Quizás haya que medir también los aspectos de

- seguridad corporativa
- seguridad patrimonial
- seguridad física
- aunque lo dejaremos para más adelante.

10.7. DATOS

10.7.1. RECURSOS HUMANOS

—	dedicados a TIC		dedicados a seguridad TIC	
	año X	recurrentes	año X	recurrentes
personal propio				
personal subcontratado				
TOTAL	RRHH_TIC		RRHH_STIC	

198. Las personas pueden dedicarse a tiempo completo, o una fracción de su tiempo, que se contabilizará como el porcentaje correspondiente.

10.7.2. RECURSOS ECONÓMICOS

	dedicados a TIC		dedicados a seguridad TIC	
	año X	recurrentes	año X	recurrentes
personal propio	(111)	(112)	(211)	(212)
personal subcontratado	(121)	(122)	(221)	(222)

adquisición de productos	(131)	(132)	(231)	(232)
servicios	(141)	(142)	(241)	(242)
TOTAL	EUR_TIC		EUR_STIC	

199. Si los servicios incluyen personas, se imputarán en el capítulo de ‘personal subcontratado’.
200. Hay que determinar qué periodo de depreciación de le aplica a los productos adquiridos. Supongo que 3 años.
201. Quizás sea interesante añadir columnas para “gasto en concienciación y formación”. Parece un componente sustancial.

10.7.3. USUARIOS INTERNOS

202. Número de personas del organismo que usan el sistema como parte de sus actividades laborales.
203. Puede ser una simple medida a título de inventario. En ciertas circunstancias, se pueden relativizar los demás datos teniendo en cuenta el tipo de actividad que realizan dichos usuarios y los cometidos del sistema de información.

10.8. INDICADORES

10.8.1. PROPORCIÓN DE RECURSOS HUMANOS DEDICADOS A SEGURIDAD DE LOS SISTEMAS

$$RRHH_1 = RRHH_STIC / RRHH_TIC$$

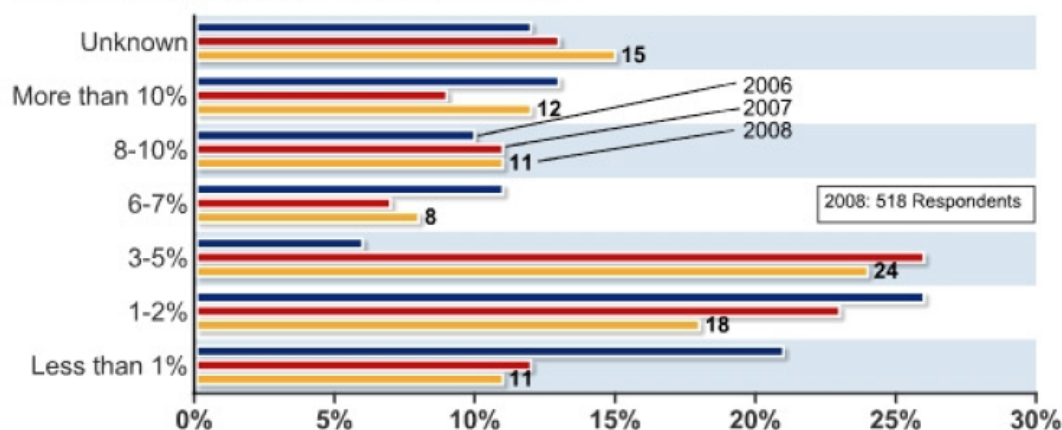
204. relativiza los recursos al tamaño del sistema.

10.8.2. PROPORCIÓN DE RECURSOS ECONÓMICOS DEDICADOS A SEGURIDAD DE LOS SISTEMAS

$$EUR_1 = EUR_STIC / EUR_TIC$$

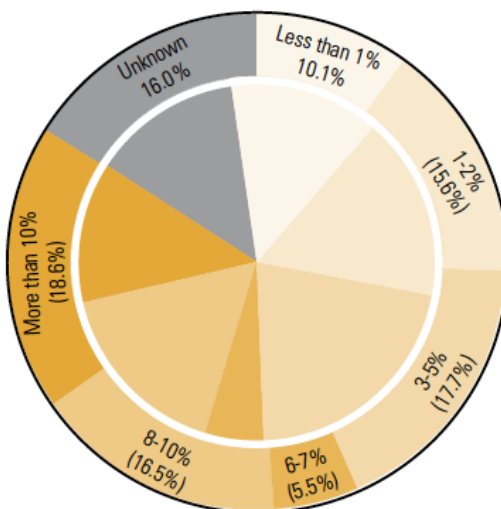
205. relativiza los recursos al tamaño del sistema.

Figure 5: Percentage of IT Budget for Security



Percentage of IT Budget Spent on Security

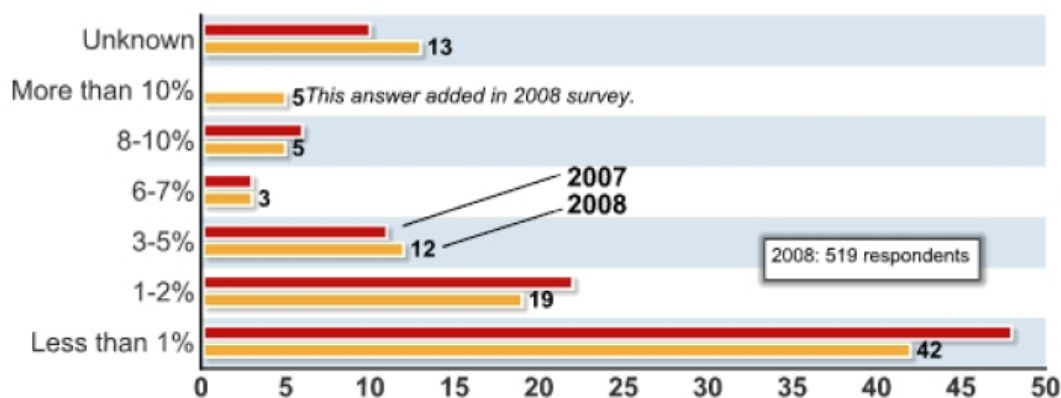
2010 Figures on Outside, 2009 Figures on Inside



2010 CSI Computer Crime and Security Survey

2010 Respondents: 237

Figure 6: Awareness Training as a Percentage of Security Budget



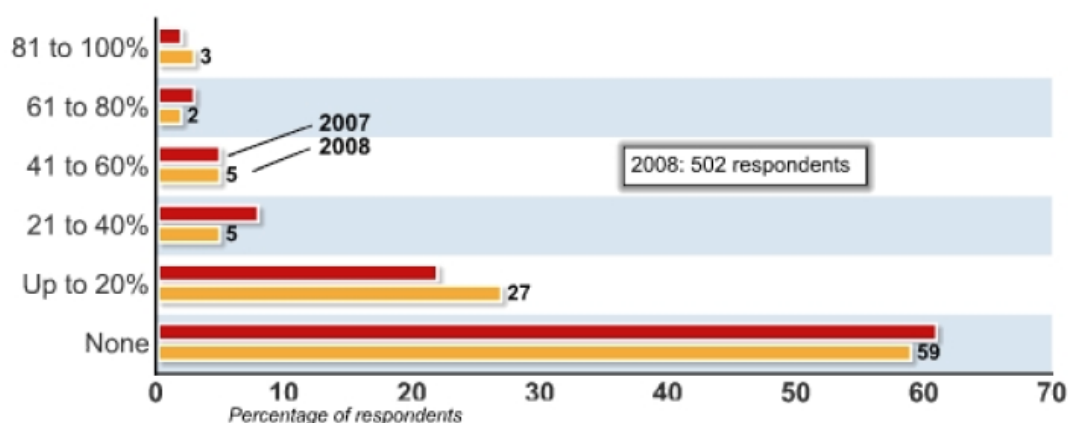
10.8.3. PROPORCIÓN DE RECURSOS TIC EXTERNALIZADOS

$\text{propios} = (111) + (112) + (131)^* + (132)$
 $\text{externos} = (121) + (122) + (141) + (142)$
 $\text{externos} / \text{propios}$

10.8.4. PROPORCIÓN DE RECURSOS STIC EXTERNALIZADOS

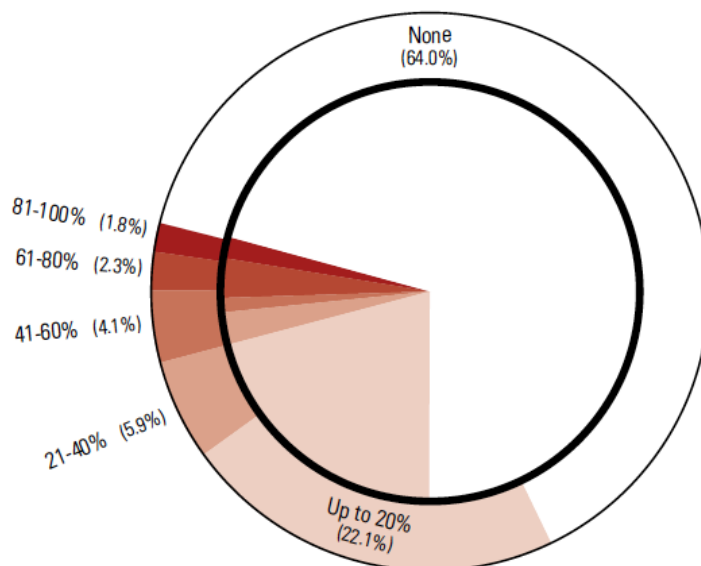
$\text{propios} = (211) + (212) + (231)^* + (232)$
 $\text{externos} = (221) + (222) + (241) + (242)$
 $\text{externos} / \text{propios}$

Figure 8: Percentage of Security Outsourced



Percentage of Security Functions Outsourced

By Percentage of Respondents
2010 Figures on Outside, 2009 Figures on Inside



2010 CSI Computer Crime and Security Survey

2010: 222 Respondents

10.8.5. OTROS INDICADORES

206. Es habitual utilizar otros indicadores financieros que básicamente miran el gasto en seguridad como una inversión y buscan evaluar su rentabilidad. Incluso cuando la rentabilidad es negativa, puede verse la seguridad como “sería peor si no lo hubiéramos hecho”.

ROI – return on investment

retorno de la inversión

Medida de los beneficios más ahorros en costes en proporción al gasto.

ROSI – return on security investment

retorno de la inversión en seguridad

Medida de los beneficios (de seguridad) más ahorros en costes (reducción de pérdidas por incidentes) en proporción al gasto en seguridad

IRR – internal return rate

TIR – tasa interna de retorno

Se calcula sobre unos cuantos años; por ejemplo, 5.

Visto el gasto como una inversión, ¿cuál es la rentabilidad para el organismo?

Sirve para determinar si sería mejor haber puesto el dinero en un activo financiero remunerado.

NPV – net present value

VNP – valor neto presente

Se calcula sobre unos cuantos años; por ejemplo, 5.

Sirve para estimar en valor de la inversión habiendo corregido la depreciación del gasto.

Por ejemplo, corrige el efecto de la inflación.

207. Comentarios

- todos estos indicadores presumen que somos capaces de medir el efecto de la seguridad y el cambio en gastos atribuible a la implantación de las medidas de seguridad; esto es muy discutible u opinable en muchas circunstancias, y especialmente en la administración pública donde muchos impactos son intangibles (incumplimiento de la ley, pérdida de confianza en la administración electrónica; daños a terceros, ciudadanos, que no se cargan a la administración, etc.)
- estos indicadores pueden ser útiles dentro de un organismo, pero no acabo de ver su uso en la CSAE
- es frecuente oír que este tipo de indicadores se usan poco y de forma menguante

Figure 7: Percentage Using ROI, NPV, and IRR Metrics

