GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

CCN
CENTRO CRIPTOLÓGICO NACIONAL

GUÍA DE SEGURIDAD (CCN-STIC-822)

ESQUEMA NACIONAL DE SEGURIDAD PROCEDIMIENTOS DE SEGURIDAD

ens
Esquema Nacional de Seguridad

OCTUBRE 2012

Edita:

NIPO: 002-12-066-9

Tirada: 1000 ejemplares
Fecha de Edición: octubre de 2012

El Sr. Carlos Galán ha elaborado el presente documento y sus anexos.

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.

Octubre de 2012

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

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 específicas. Se espera que cada organización las particularice para adaptarlas a su entorno singular.

2. El objetivo de esta Guía es proponer a los organismos de las Administraciones públicas españolas una relación de Procedimientos de Seguridad, recogiendo lo exigido por el 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 (ENS, en adelante).

3. La publicación y el cumplimiento de las antedichas normas contribuirá a:

   - Facilitar el máximo aprovechamiento de los recursos y sistemas de información en la actuación de las Administraciones públicas.
   - Asegurar la protección de los derechos de los ciudadanos en sus relaciones con las Administraciones públicas y el desenvolvimiento profesional de los empleados públicos y usuarios que tienen acceso a los recursos y sistemas de información de las Administraciones públicas.
   - Mejorar los servicios que las Administraciones públicas prestan a los ciudadanos, propiciando una gestión eficiente y segura de los procesos incluidos en los sistemas de información con los que opera.
   - Proteger a los sistemas de información de las Administraciones públicas y a los datos que tratan de los riesgos que puedan deberse a la acción humana, especialmente en lo referente a conductas incorrectas, inadecuadas o ilegales.

2. ÁMBITO DE APLICACIÓN

4. La normativa contenida en la presente Guía resulta de aplicación a cualquier entidad del sector público del ámbito de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (LAECSP. En adelante): Administración General del Estado, Administración de las Comunidades Autónomas y Administración de las Entidades Locales.

5. Por otro lado, la calificación del nivel de seguridad de la información y de los servicios a los que pudieran afectar las normas comprendidas en la presente Guía, se ha dispuesto atendiendo a las **denominaciones establecidas en el ENS: BAJO, MEDIO o ALTO**[1]. La calificación de información clasificada (SECRETO, RESERVADO, CONFIDENCIAL y DIFUSIÓN LIMITADA) se hará atendiendo a las regulaciones que le son específicamente de aplicación[2].

6. Finalmente, todos los preceptos señalados por los Procedimientos contenidos en la presente Guía se contemplan sin perjuicio de la adicional adopción de las previsiones que

[1] Estas denominaciones son independientes de las establecidas para las medidas de seguridad contempladas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BÁSICO, MEDIO o ALTO), que asimismo resultarán de aplicación cuando se traten datos de carácter personal.

[2] Denominaciones definidas en la Ley 9/1968, de 5 de abril, reguladora de los Secretos Oficiales (LSO, en adelante) y en la Norma NS/04 de la Autoridad Nacional, así como en Políticas de Seguridad de Organizaciones Internacionales y Acuerdos para Protección de la Información Clasificada, y en determinados Departamentos Ministeriales (MINISDEF), como desarrollo de la precitada LSO.

dimanen de otras regulaciones, tales como la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, etc.

3. REGULACIONES INTERNAS A LOS ORGANISMOS DE LAS ADMINISTRACIONES PÚBLICAS

7. Las Administraciones públicas, en el desarrollo de sus funciones de servicio, policía o fomento, están sometidas a diferentes normativas, de carácter estatal, autonómico o local. La particularidad de la actuación administrativa realizada por medios electrónicos viene requiriendo, en los mismos tres niveles, la existencia de normas y procedimientos asimismo específicas, al objeto de acomodar aquellas funciones originarias a los condicionantes y medios electrónicos.

8. En este sentido, la LAECSP ha supuesto el punto de partida de un extenso compendio de regulaciones que vienen completando nuestro moderno ordenamiento jurídico administrativo-electrónico, entre las que cabe destacar: el Real Decreto 1671/2009, de 6 de septiembre, de desarrollo parcial de la LAECSP, el 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 y el Real Decreto 4/2010, de de enero, por el que se regula el Esquema Nacional de Interoperabilidad, entre otras.

9. Con el objetivo de profundizar en las medidas de seguridad requeridas por los sistemas de información del ámbito de la LAECSP, el ENS insta a los organismos de las AA.PP. a desarrollar, publicar y hacer valer Normas y Procedimientos de carácter interno a los propios organismos, tendentes a mejorar el nivel de seguridad de las informaciones que manejan y los servicios que prestan.

10. La necesidad de completar el marco normativo aparece explícitamente en muchos de los preceptos del ENS. Por ejemplo, en los artículos 14 (Gestión del personal), 18 (Adquisición de productos de seguridad), 21 (Protección de información almacenada y en tránsito), 23 (Registro de actividad), 34 (Auditoría de la seguridad), 37 (Prestación de servicios de respuesta a incidentes de seguridad en las Administraciones públicas), Disposición adicional tercera (Comité de Seguridad de la Información de las Administraciones Públicas), etc.

11. En concreto, en el Anexo II del ENS (Medidas de Seguridad), se encuentra la medida [org.3], que señala:

> **3.3 Procedimientos de seguridad [org.3].**
>
> Se dispondrá de una serie de documentos que detallen de forma clara y precisa:
>
> a) Cómo llevar a cabo las tareas habituales.
> b) Quién debe hacer cada tarea.
> c) Cómo identificar y reportar comportamientos anómalos.

12. Esta habilitación a los organismos de las AA.PP. para que promuevan su propia normativa interna y de relación con terceros se alienta en varias medidas de seguridad del ENS: Requisitos de acceso [op.acc.2], Deberes y obligaciones [mp.per.2], Concienciación [mp.per.3], Formación [mp.per.4], Protección del correo electrónico (e-mail) [mp.s.1], etc.

4. LAS GUÍAS CCN-STIC COMO FUENTE DE MODELOS DE NORMAS Y PROCEDIMIENTOS

13. De acuerdo con lo previsto en el artículo 37 del ENS, el CCN-CERT investigará y divulgará las mejores prácticas sobre seguridad de la información entre todos los miembros de las Administraciones públicas. Con esta finalidad, las series de Documentos CCN-STIC, elaboradas por el Centro Criptológico Nacional, ofrecerán normas, instrucciones, guías y recomendaciones para aplicar el Esquema Nacional de Seguridad y para garantizar la seguridad de los sistemas de información en la Administración.

14. Es en base a este mandato por el que se incluyen en la presente Guía algunos Modelos de Procedimientos de Seguridad que pueden ser usados por los organismos de las Administraciones públicas españolas, en cumplimiento de lo preceptuado en la anteriormente citada medida del ENS: Procedimientos de Seguridad [org.3].

15. El conjunto de modelos de procedimientos que contienen los Anexos de esta Guía deben ser tomados como referencia. Cada organismo deberá adaptar las normas a su casuística particular.

5. CONVENCIONES USADAS

16. En el conjunto de modelos de procedimientos contenidos en los Anexos de la presente Guía se han seguido las siguientes convenciones generales:

Término	Significado
<<ORGANISMO>>	Cualquier **organismo** de las Administraciones públicas del ámbito de aplicación del ENS. Puede ser también aplicado a unidades administrativas inferiores, si disponen de la autonomía correspondiente para decidir sobre su propia normativa.
<<U/OC>>	**Unidad / Organismo Colegiado** competente para desarrollar la acción que se menciona. En ocasiones, un mismo párrafo puede contener varias de estas expresiones, que podrán referirse a la misma unidad o a unidades distintas, según corresponda.
<<texto>>	Se incluirá el contenido que se considere adecuado. Por ejemplo *<<señalar periodicidad>>* podría dar lugar a <<mensualmente>>.

6. CONTENIDO

17. Además del cuerpo documental, la presente Guía contiene una serie de Anexos conteniendo Modelos de Procedimientos que desarrollan aspectos concretos.

18. Tales Anexos irán actualizándose y completándose con nuevos procedimientos, a tenor de la evolución tecnológica de los sistemas de información y de los riesgos derivados de su uso.

7. DESARROLLO NORMATIVO Y PROCEDIMENTAL DE LA POLÍTICA DE SEGURIDAD

19. Como señala la Guía CCN-STIC 805: Política de Seguridad de la Información, la Política de Seguridad de la Información del <<ORGANISMO>> es un documento de alto nivel que define lo que significa 'seguridad de la información' en una organización. El documento debe estar accesible por todos los miembros de la organización y redactado de forma sencilla, precisa y comprensible. Conviene que sea breve, dejando los detalles técnicos para otros documentos normativos.

20. Dado que la Política de Seguridad está escrita a un nivel muy amplio, se requiere complementarla con documentos más precisos que ayuden a llevar a cabo lo propuesto. Para ello se utilizan otros instrumentos que reciben diferentes nombres, siendo comunes los siguientes[3]:

    – *Normas* de seguridad (*security standards*).

    – *Guías* de Seguridad (*security guides*).

    – *Procedimientos* de seguridad (*security procedures*).

21. Las Normas uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.

22. Las Guías tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad, proporcionando razonamientos donde no existen procedimientos precisos.

23. Los Procedimientos (operativos) de seguridad afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.

24. Así pues, la Política de Seguridad de la Información del <<ORGANISMO>> se desarrollará, entre otros instrumentos, por medio de la normativa de seguridad, que abordará aspectos generales y específicos y, en general, modelos de comportamiento. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

25. Como regla general, la normativa de seguridad estará disponible en la intranet corporativa del organismo de que se trate a través de una dirección URL y, en su caso, impresa y accesible en una determinada ubicación física.

26. La Normativa de Seguridad de cada organismo trae causa y recibe su autoridad ejecutiva de lo preceptuado en el ENS, en primera instancia, y desarrollando normativamente la Política de Seguridad del organismo en cuestión, en segunda instancia.

[3] Guía NIST SP 800-100. An introduction to Computer Security: The NIST Handbook. October, 1995.

8. PRECEPTOS DEL ENS CONTEMPLADOS EN ESTA GUÍA

27. Las normas incluidas en la presente Guía contemplan, total o parcialmente, los siguientes artículos del ENS:

- ***Artículo 5. La seguridad como un proceso integral.***
  1. La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.
  2. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

- ***Artículo 7. Prevención, reacción y recuperación.***
  1. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.
  2. Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición.
  3. Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo.
  4. Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.
  5. Sin merma de los demás principios básicos y requisitos mínimos establecidos, el sistema garantizará la conservación de los datos e informaciones en soporte electrónico.
  De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

- ***Artículo 8. Líneas de defensa.***
  1. El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:
    a) Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
    b) Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
    c) Minimizar el impacto final sobre el mismo.
  2. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

- ***Artículo 11. Requisitos mínimos de seguridad.***
  1. Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente. Esta política de seguridad, se establecerá en base a los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:
    a) Organización e implantación del proceso de seguridad.
    b) Análisis y gestión de los riesgos.
    c) Gestión de personal.
    d) Profesionalidad.
    e) Autorización y control de los accesos.
    f) Protección de las instalaciones.
    g) Adquisición de productos.
    h) Seguridad por defecto.
    i) Integridad y actualización del sistema.
    j) Protección de la información almacenada y en tránsito.
    k) Prevención ante otros sistemas de información interconectados.
    l) Registro de actividad.
    m) Incidentes de seguridad.
    n) Continuidad de la actividad.
    o) Mejora continua del proceso de seguridad.
  2. A los efectos indicados en el apartado anterior, se considerarán órganos superiores, los responsables directos de la ejecución de la acción del gobierno, central, autonómico o local, en un sector de actividad específico, de acuerdo con lo establecido en la Ley 6/1997, de 14 de abril, de organización y funcionamiento de la Administración General del Estado y Ley 50/1997, de 27 de noviembre, del Gobierno; los estatutos de autonomía correspondientes y normas de desarrollo; y la

Ley 7/1985, de 2 de abril, reguladora de las bases del Régimen Local, respectivamente.
Los municipios podrán disponer de una política de seguridad común elaborada por la Diputación, Cabildo, Consejo Insular u órgano unipersonal correspondiente de aquellas otras corporaciones de carácter representativo a las que corresponda el gobierno y la administración autónoma de la provincia o, en su caso, a la entidad comarcal correspondiente a la que pertenezcan.
3. Todos estos requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, pudiendo algunos no requerirse en sistemas sin riesgos significativos, y se cumplirán de acuerdo con lo establecido en el artículo 27.

- ***Artículo 14. Gestión de personal.***
  1. Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos.
  2. El personal relacionado con la información y los sistemas, ejercitará y aplicará los principios de seguridad en el desempeño de su cometido.
  3. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad.
  4. Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

- ***Artículo 16. Autorización y control de los accesos.***
  El acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

- ***Artículo 17. Protección de las instalaciones.***
  Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas deben estar cerradas y disponer de un control de llaves.

- ***Artículo 19. Seguridad por defecto.***
  Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto:
  a) El sistema proporcionará la mínima funcionalidad requerida para que la organización sólo alcance sus objetivos, y no alcance ninguna otra funcionalidad adicional.
  b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
  c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.
  d) El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

- ***Artículo 21. Protección de información almacenada y en tránsito.***
  1. En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.
  2. Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones públicas en el ámbito de sus competencias.
  3. Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el presente real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.

- ***Artículo 23. Registro de actividad.***
  Con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o

laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

- ***Artículo 24. Incidentes de seguridad.***
  1. Se establecerá un sistema de detección y reacción frente a código dañino.
  2. Se registrarán los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan. Estos registros se emplearán para la mejora continua de la seguridad del sistema.

- ***Artículo 25. Continuidad de la actividad.***
  Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

- ***Artículo 29. Guías de seguridad.***
  Para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, el Centro Criptológico Nacional, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones.

- ***Anexo II: Medidas de Seguridad (****Normativa de seguridad [org.2]).*

9. MÉTRICAS E INDICADORES DE CUMPLIMIENTO

28. Se suele decir que lo que no se mide no puede gobernarse adecuadamente. Este aserto es igualmente predicable de la presencia y grado de cumplimiento de las Normas y Procedimientos de Seguridad en los organismos públicos, razón por la cual conviene determinar qué métricas habrán de proporcionar los indicadores adecuados que permitan a la dirección del organismo gestionar debidamente la influencia de las antedichas normas en la seguridad de la información y de los servicios prestados4.

29. En relación con los Procedimientos de Seguridad, pueden utilizarse los siguientes indicadores clásicos:

- Proporción de procedimientos implantados sobre procedimientos previstos.
- Número de violaciones graves de los procedimientos de seguridad reportadas.
- Encuesta de legibilidad percibida por los usuarios.
- Encuesta de utilidad percibida por los usuarios.

30. Como acabamos de mencionar, las Normas y Procedimientos de Seguridad podrán ser evaluados atendiendo a dos cualidades:

a) **Legibilidad**:

Regularmente se puede preguntar a los usuarios a los que van dirigidos los procedimientos de seguridad por la *facilidad* con la que se entienden los textos proporcionados.

Las respuestas podrán valorarse en una escala de 1 a 5, de la siguiente forma:

- [5] Se interpreta perfectamente.
- [4] Entre [3] y [4].
- [3] Se interpreta con cierta dificultad. Puede generar inseguridad.
- [2] Entre [1] y [3].
- [1] No se entiende nada. Genera confusión.

Para calcular la legibilidad de un documento a partir de un conjunto de encuestas, se usarán dos estadísticos:

- La mediana de las puntuaciones obtenidas.
- La desviación estándar de las puntuaciones obtenidas.

Si la media o la mediana están por debajo de 3, debería revisarse la documentación, reescribiéndola de forma más clara para los lectores previstos.

Si la desviación estándar es elevada, debería revisarse 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.

[4] Véase Guía CCN-STIC 815 Métricas e indicadores en el ENS.

b) **Utilidad**:

Regularmente se puede preguntar a los usuarios a los que van dirigidos los procedimientos de seguridad por la *utilidad* que obtiene de los textos proporcionados.

Las respuestas podrán valorarse en una escala de 1 a 5, de la siguiente forma:

- [5] Se encuentra rápidamente respuesta a lo que se necesita.
- [4] Entre [3] y [4].
- [3] Aunque cuesta trabajo, leyéndolo con cuidado y detenimiento, se consigue.
- [2] Entre [1] y [3].
- [1] No está claro a qué caso se aplica cada cosa y da muchas cosas por sobreentendidas. No sirve.

Para calcular la utilidad de un documento a partir de un conjunto de encuestas, se usarán dos estadísticos:

- La mediana de las puntuaciones obtenidas.

- La desviación estándar de las puntuaciones obtenidas.

Si la media o la mediana están por debajo de 3, debería revisarse la documentación para ajustarla a los casos de uso previstos.

Si la desviación estándar es elevada, deberían revisarse 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.

10. RECONOCIMIENTO

31. Además de las disposiciones indicadas con anterioridad y las expresamente nombradas en cada uno de ellos, han inspirado el contenido de los modelos de procedimientos de la presente Guía, documentos de la Administración en materia de seguridad electrónica, las propias Guías CCN-STIC de Seguridad de los Sistemas de Información y Comunicaciones, la Metodología y herramientas de análisis y gestión de riesgos, el Esquema Nacional de Interoperabilidad, así como una multiplicidad de políticas, criterios y normas internas de distintos organismos públicos, nacionales e internacionales, a los que agradecemos sus aportaciones.