GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC
CCN-STIC 821

ESQUEMA NACIONAL DE SEGURIDAD
NORMAS DE SEGURIDAD

FEBRERO 2018

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2018.02.22 16:57:19 +01'00'

Nipo: 785-18-015-2

Fecha de Edición: Febrero de 2018

Carlos Galán ha participado en la realización y modificación del presente documento y sus anexos, que ha sido financiado por Ministerio de Hacienda y Administraciones Públicas.

PRÓLOGO

El uso masivo de las tecnologías de la información y la comunicación (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 (CNI), 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 (CCN) 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.

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), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, 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 la comunicación (STIC) 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.

Febrero de 2018

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 las entidades del ámbito de aplicación del 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), una relación de Normas de Seguridad, recogiendo lo exigido por tal cuerpo legal[1].
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 y, en general, las entidades del Sector Público 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 entidades del Sector Público 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, tal y como se encuentra definido en el artículo 2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP, en adelante).
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**. La calificación de información clasificada (SECRETO, RESERVADO, CONFIDENCIAL y DIFUSIÓN LIMITADA) se hará atendiendo a las regulaciones que le son específicamente de aplicación[2].

[1] Para más información sobre el ámbito de aplicación del ENS puede consultarse la Guía CCN-STIC 830 Ámbito de aplicación del ENS.

[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.

6. Finalmente, todos los preceptos señalados por las Normas contenidas en la presente Guía se contemplan sin perjuicio de la adicional adopción de las previsiones que dimanen de otras regulaciones, tales como las derivadas de la Protección de Datos Personales, etc.

3. REGULACIONES INTERNAS A LAS ENTIDADES DEL SECTOR PÚBLICO

7. Las entidades del Sector Público, en el desarrollo de sus funciones de servicio, policía o fomento, están sometidas a diferentes normativas, de carácter europeo, estatal, autonómico o local. En concreto, la particularidad de la **actuación administrativa realizada por medios electrónicos** viene requiriendo, la existencia de normas asimismo específicas, al objeto de acomodar aquellas funciones originarias a los condicionantes y medios electrónicos.

8. En este sentido, la ya derogada Ley 11/2007 supuso el punto de partida de un extenso compendio de regulaciones que vienen completando nuestro moderno ordenamiento jurídico administrativo-electrónico, entre las que cabe destacar: la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas y la ya mencionada LRJSP, que vuelven a situar al 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 al Real Decreto 4/2010, de de enero, por el que se regula el Esquema Nacional de Interoperabilidad, en el centro de la normativa tecnológica de aplicación.

9. Con el objetivo de profundizar en las medidas de seguridad requeridas por los sistemas de información del ámbito de la LRJSP, el ENS insta a los organismos del Sector Público a desarrollar, publicar y hacer valer normas 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.2], que señala:

> ***1.2 Normativa de seguridad [org.2].***
> *Se dispondrá de una serie de documentos que describan:*
>
> *a) El uso correcto de equipos, servicios e instalaciones.*
> *b) Lo que se considerará uso indebido.*
> *c) La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.*

12. Esta habilitación concedida a las entidades públicas 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

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 Normas de Seguridad que pueden ser usados por las entidades del ámbito de aplicación del ENS, en cumplimiento de lo preceptuado en la anteriormente citada medida del ENS: Normativa de Seguridad [org.2].
15. El conjunto de modelos de normas que contienen los Anexos de esta Guía debe ser tomado como referencia. Cada entidad deberá adaptar las normas a su casuística particular.

5. CONVENCIONES USADAS

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

Término	Significado
<<ENTIDAD>> / <<ORGANISMO>>	Cualquier **entidad u organismo** del ámbito de aplicación del ENS. Puede ser también aplicado a unidades administrativas inferiores, si disponen de la autonomía adecuada y suficiente para decidir sobre su propia normativa interna.
<<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 se complementa con varios Anexos, que se publican separadamente como Apéndices de este documento, y que contienen modelos de normas para propósitos concretos, que se irán actualizando e incrementando a medida que sea necesario.

7. DESARROLLO NORMATIVO DE LA POLÍTICA DE SEGURIDAD

18. Como señala la Guía CCN-STIC 805: Política de Seguridad de la Información, la Política de **Seguridad de la Información** de la <<ENTIDAD>> 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.
19. 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*).
20. Las ***Normas*** uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de **carácter obligatorio**.
21. 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.
22. Los ***Procedimientos*** (operativos) de seguridad afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.
23. Así pues, la Política de Seguridad de la Información de la <<ENTIDAD>> 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.
24. Como regla general, la normativa de seguridad estará disponible en la intranet corporativa de la entidad de que se trate a través de una dirección URL y, en su caso, impresa y accesible en una determinada ubicación física.
25. **La Normativa de Seguridad de cada entidad trae causa y recibe su autoridad ejecutiva de lo preceptuado en el ENS, en primera instancia, y desarrollando normativamente la Política de Seguridad de la entidad en cuestión, en segunda instancia.**

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

8. MÉTRICAS E INDICADORES DE CUMPLIMIENTO

26. 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 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 prestados[4].

27. En relación con la Normativa de Seguridad, pueden utilizarse los siguientes indicadores clásicos:

    - 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.

28. Como acabamos de mencionar, la Normativa de Seguridad podrá ser evaluada atendiendo a dos cualidades:

    a) **Legibilidad de la Normativa**:

    Regularmente se puede preguntar a los usuarios a los que va dirigida la normativa 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.

    b) **Utilidad de la Normativa**:

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

Regularmente se puede preguntar a los usuarios a los que va dirigida la normativa 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.

9. RECONOCIMIENTO

Además de las disposiciones indicadas con anterioridad y las expresamente nombradas en el anexo de Referencias, han inspirado el contenido de los modelos de normas 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.

ANEXO I. REFERENCIAS

- Guía NIST SP 800-100. An introduction to Computer Security: The NIST Handbook. October, 1995.
- Guía CCN-STIC 201. Organización y Gestión para la Seguridad de las TIC.
- Guía CCN-STIC 301. Requisitos STIC.
- Guía CCN-STIC 400. Manual de Seguridad de las Tecnologías de la Información y Comunicaciones.
- Guía CCN-STIC 402. Organización y Gestión para la Seguridad de los Sistemas TIC.
- Guía CCN-STIC 803. Valoración de los Sistemas.
- Guía CCN-STIC 804. ENS-Guía de Implantación.
- Guía CCN-STIC 814. Seguridad en correo electrónico.
- Guía CCN-STIC 815. Métricas e indicadores en el ENS.
- FIPS 200. Minimum Security Requirements for Federal Information and Information Systems.
- Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- 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.
- Real Decreto 1671/2009, de 6 de septiembre, de desarrollo parcial de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
- 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.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad del en ámbito de la administración electrónica.
- Guía NIST SP 800-53. Recommended Security Controls for Federal Information Systems and Organizations.
- Guía NIST SP 800-100. Information Security Handbook: A Guide for Managers.
- UNE - ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la información.
- UNE - ISO/IEC 27001:2007 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.