



## Guía de Seguridad de las TIC CCN-STIC 821

### APÉNDICE VII: MODELO DE CONTENIDO DE BUENAS PRÁCTICAS PARA TERCEROS NP60



CENTRO CRIPTOLOGICO NACIONAL  
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,  
ou=sello electrónico, serialNumber=52800155J,  
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO  
CRIPTOLOGICO NACIONAL, c=ES  
2018.02.23 09:33:40 +01'00'

FEBRERO 2018

## ÍNDICE

|                                                              |          |
|--------------------------------------------------------------|----------|
| <b>1. OBJETIVO .....</b>                                     | <b>1</b> |
| <b>2. ÁMBITO DE APLICACIÓN.....</b>                          | <b>1</b> |
| <b>3. VIGENCIA .....</b>                                     | <b>1</b> |
| <b>4. REVISIÓN Y EVALUACIÓN .....</b>                        | <b>1</b> |
| <b>5. REFERENCIAS.....</b>                                   | <b>2</b> |
| <b>6. NORMAS PREVIAS .....</b>                               | <b>2</b> |
| <b>7. ACTORES Y RESPONSABILIDADES.....</b>                   | <b>2</b> |
| <b>8. IDENTIFICACIÓN DE RIESGOS POR TERCEROS.....</b>        | <b>3</b> |
| <b>9. MEDIDAS DE SEGURIDAD CON RESPECTO A TERCEROS .....</b> | <b>3</b> |
| <b>10. RETIRADA DE MATERIAL POR TERCEROS.....</b>            | <b>4</b> |
| <b>11. INTERCAMBIO DE INFORMACIÓN .....</b>                  | <b>5</b> |
| <b>12. SUPERVISIÓN Y REVISIÓN DE ACUERDOS .....</b>          | <b>5</b> |
| <b>13. REGISTROS E INDICADORES .....</b>                     | <b>5</b> |
| 13.1. TABLA DE REGISTROS.....                                | 5        |
| 13.2. TABLA DE INDICADORES .....                             | 6        |
| <b>14. SOPORTE Y MODELOS.....</b>                            | <b>6</b> |
| 14.1. SOPORTE .....                                          | 6        |
| 14.2. MODELO DE REGISTRO DE SALIDA DE MATERIAL .....         | 6        |
| 14.3. MODELO DE REGISTRO DE INTERCAMBIO DE INFORMACIÓN ..... | 6        |
| <b>15. PROTOCOLO DE FIRMA .....</b>                          | <b>7</b> |

## 1. OBJETIVO

1. El objetivo de la presente norma es presentar un **Modelo Contenido de Buenas Prácticas para Terceros**, que presten servicios en la <<ENTIDAD>>.

La presente Normativa deberá ser complementada, en su caso y en la medida oportuna, con la aplicación de las medidas de seguridad previstas en el Anexo II 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).

2. Este documento se considera de uso interno de la <<ENTIDAD>> y, por tanto, no podrá ser divulgado salvo autorización del <<U/OC>>.

## 2. ÁMBITO DE APLICACIÓN

3. Esta normativa es de aplicación a todo el ámbito de actuación de la <<ENTIDAD>>, y sus contenidos se ubican bajo las directrices de carácter más general definidas en la Política de Seguridad de la Información de la <<ENTIDAD>>.
4. En este sentido, su alcance comprende toda la información utilizada para el desarrollo de las funciones y competencias atribuidas a la <<ENTIDAD>>, así como los sistemas de información que la gestionan, y **será de obligado cumplimiento para todo el personal de terceras instituciones que preste sus servicios en la <<ENTIDAD>>**. Por tanto, su alcance incluye a todos los usuarios de entidades externas a la <<ENTIDAD>> que requieran, en el marco de un acuerdo de colaboración o relación contractual, de acceso a los activos de información de la <<ENTIDAD>>.

## 3. VIGENCIA

5. La presente Norma ha sido aprobada por la <<U/OC>> de la <<ENTIDAD>>, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la <<ENTIDAD>> pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.
6. Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la <<ENTIDAD>>.
7. Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta Normativa.

## 4. REVISIÓN Y EVALUACIÓN

8. La gestión de esta Normativa corresponde a la <<U/OC>>, que es competente para:
  - Interpretar las dudas que puedan surgir en su aplicación.
  - Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.

- Verificar su efectividad.
- 9. Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), la <<U/OC>> revisará la presente Normativa, que se someterá, de haber modificaciones, a la aprobación de la <<U/OC>> de la <<ENTIDAD>>.
- 10. La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.
- 11. Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

## 5. REFERENCIAS

12. <<En este epígrafe se deben incluir aquellas referencias documentales que vengan a apoyar o completar esta Norma o que hubieren sido consideradas en su redacción.

### **Internas:**

- ----
- ----
- 

### **Externas:**

(Por ejemplo:

- 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.
- 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.
- ISO/IEC 9001:2000 Sistemas de gestión de la calidad.
- Documentos y Guías CCN-STIC.
- Etc.>>

## 6. NORMAS PREVIAS

13. El presente “Modelo de Buenas Prácticas para Terceros” complementa, en sus aspectos específicos, a la “NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DE LA <<ENTIDAD>>”<sup>1</sup>, por lo que tal normativa general será de aplicación en los aspectos no señalados en aquella.

## 7. ACTORES Y RESPONSABILIDADES

14. Las responsabilidades definidas por la metodología y actividades descritas en la presente Norma son las siguientes.

---

<sup>1</sup> Se recomienda que el organismo disponga de una Normativa General de Utilización de los Recursos y Sistemas de Información de la <<ENTIDAD>>, del tipo descrito en el documento CCN STIC – 821 - NG00.

| Actores  | Responsabilidades                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Usuarios | Cumplir con las directrices establecidas en la <b>Normativa de Buenas Prácticas para Terceros</b> , haciendo un uso responsable de los canales de intercambio de información de la <<ENTIDAD>>, así como de la información intercambiada.                                                                                                                                                                                                                                                                                                                                                                           |
| <<U/OC>> | <ul style="list-style-type: none"> <li>– Comprobar que los usuarios de las entidades prestando servicios para la &lt;&lt;ENTIDAD&gt;&gt; firman la <b>Normativa de Buenas Prácticas para Terceros</b> de la &lt;&lt;ENTIDAD&gt;&gt;.</li> <li>– Definir y actualizar las líneas maestras en las que se debe basar el intercambio de información con entidades externas.</li> <li>– Coordinar las actuaciones de auditoría para garantizar el cumplimiento por parte de las entidades prestando servicios para la &lt;&lt;ENTIDAD&gt;&gt; de las medidas de seguridad definidas en la presente normativa.</li> </ul> |

## 8. IDENTIFICACIÓN DE RIESGOS POR TERCEROS

15. La <<ENTIDAD>> es consciente de los riesgos que genera el acceso por terceros a su información y, en consecuencia, ha definido un conjunto de **medidas de seguridad** aplicables y exigibles a este colectivo.
16. La <<ENTIDAD>> se reserva el derecho de verificar, **mediante auditorías periódicas**, el cumplimiento de toda medida de seguridad adicional no recogida en la presente normativa e incluida en las cláusulas particulares de los contratos suscritos con terceros.
17. Adicionalmente, los análisis de riesgos periódicos realizados por la <<ENTIDAD>>, recogerán las amenazas detectadas en servicios prestados por terceros.

## 9. MEDIDAS DE SEGURIDAD CON RESPECTO A TERCEROS

18. A continuación, se relacionan las medidas de seguridad que conforman la base normativa que regirá en la relación con terceros prestando servicios para la <<ENTIDAD>>, y que podrá completarse con medidas más restrictivas en el caso de servicios que así lo requieran.
  - Los contratos firmados con las entidades que prestarán servicios para la <<ENTIDAD>> deberán recoger en su clausulado la **obligación de confidencialidad** en el marco de la relación contractual (por ejemplo, suscribiendo el correspondiente **Acuerdo de Confidencialidad con Terceros** de la <<ENTIDAD>><sup>2</sup>)

<sup>2</sup> Véase Guía: Modelo de Acuerdo de Confidencialidad para Terceros – NP50, en esta misma Guía.

- Los usuarios de terceras empresas prestando servicios para la <<ENTIDAD>> deberán firmar la **Normativa de Buenas Prácticas para Terceros** de la <<ENTIDAD>><sup>3</sup>.
- Las empresas prestando servicios para la <<ENTIDAD>> que requieran de acceso a sus sistemas de información deberán seguir las directrices establecidas en el **Procedimiento de Gestión y Configuración de Redes** de la <<ENTIDAD>>.
- Se prohíbe el empleo de soportes de información extraíbles (CD's, DVD's, memorias USB, etc.), por parte del personal de terceros prestando servicios para la <<ENTIDAD>> para el almacenamiento de información de la <<ENTIDAD>>, sin autorización previa.
- El personal de terceros prestando servicios para el <ORGANISMO>> en sus dependencias deberá seguir las directrices establecidas en la **Normativa General de Utilización de los Recursos y Sistemas de Información**<sup>4</sup> correspondiente de la <<ENTIDAD>>.
- La <<ENTIDAD>> podrá exigir, en aplicación del clausulado de los contratos de prestación de servicios firmados con terceros, cualesquiera evidencias de cumplimiento de la legislación y/o normativa vigente.
- El personal de terceros prestando servicios para la <<ENTIDAD>> será informado y concienciado en buenas prácticas, uso responsable de los sistemas de intercambio de información y en los mecanismos existentes en la <<ENTIDAD>> para la apertura de incidencias de seguridad relacionadas con dichos sistemas.

## 10. RETIRADA DE MATERIAL POR TERCEROS

19. Los desplazamientos de activos hardware, software o información fuera de las instalaciones de la <<ENTIDAD>> deberán ser previamente autorizados por la <<U/OC>>.
20. La autorización deberá solicitarse a través del **gestor de incidencias** de la <<ENTIDAD>> y toda salida deberá ser consignada en un registro de salida de material, del que se presenta un modelo en el apartado Soporte y Modelos de la presente Normativa.
21. [El registro de salida de material se almacenará en el **gestor documental** de la <<ENTIDAD>> y se comprobará periódicamente para garantizar el retorno de los activos, especialmente a la finalización de la relación contractual con terceros prestando servicios para la <<ENTIDAD>>.

<sup>3</sup> En general, esta Normativa será un subconjunto ad hoc de la Normativa General de Utilización de los Recursos y Sistemas de Información de la <<ENTIDAD>>. Véase NG00 de la presente Guía.

<sup>4</sup> Se recomienda que el organismo disponga de una Normativa General de Utilización de los Recursos y Sistemas de Información de la <<ENTIDAD>>, del tipo descrito en el documento CCN STIC – 821 - NG00.

## 11. INTERCAMBIO DE INFORMACIÓN

22. La <<ENTIDAD>> intercambiará información en el ámbito de la prestación de servicios por parte de terceros, a través de los canales debidamente configurados, protegidos y controlados, que la <<ENTIDAD>> determine para cada proyecto.
23. Excepcionalmente, podrá considerarse conveniente por motivos de confidencialidad y especial trascendencia, aplicar medidas de seguridad adicionales sobre la información recogida en el registro de intercambio de información que se encuentra disponible a través del gestor documental de la <<ENTIDAD>>.

## 12. SUPERVISIÓN Y REVISIÓN DE ACUERDOS

24. El<<ORGANISMO>> podrá requerir la firma de **Acuerdos de Nivel de Servicio (SLA)**, para aquellos servicios que presenten especiales condicionantes en cuanto a confidencialidad, disponibilidad, integridad, autenticidad o trazabilidad de la información manejada o los servicios prestados. Dichos acuerdos serán supervisados y auditados de manera periódica para garantizar el adecuado cumplimiento de las condiciones contractuales pactadas.
25. La <<ENTIDAD>> se reserva el derecho de realizar un seguimiento de los servicios contratados mediante las correspondientes **auditorías**, con objeto de verificar el cumplimiento de los acuerdos firmados. Este derecho se plasmará tanto en los pliegos de las licitaciones como en los contratos firmados con terceros.

## 13. REGISTROS E INDICADORES

### 13.1. TABLA DE REGISTROS

(Ejemplo)

| Identificador | Nombre                                      | Frecuencia | Archivo           | Unidad que Genera | Unidad que Custodia |
|---------------|---------------------------------------------|------------|-------------------|-------------------|---------------------|
| XXX           | Informes de Auditoría de Terceros           | Anual      | Gestor Documental | Unidad 1          | Unidad 2            |
| YYY           | Normativa de Buenas Prácticas para Terceros | N/A        | Archivo Físico    | Unidad 1          | Unidad 2            |
| ZZZ           | Registro de Salida de material              | N/A        | Gestor Documental | Unidad 1          | Unidad 2            |
| AAA           | Registro de Intercambio de Información      | N/A        | Gestor Documental | Unidad 1          | Unidad 2            |

## 13.2. TABLA DE INDICADORES

(Ejemplo)

| Identificador | Rango | Frecuencia | Métrica                                     | Objetivo | Descripción |
|---------------|-------|------------|---------------------------------------------|----------|-------------|
| XXX           | %     | Anual      | Normativa de Buenas Prácticas para Terceros | 100%     | --          |
| YYY           | %     | Anual      | Salidas no autorizadas de material          | 0%       | --          |

## 14. SOPORTE Y MODELOS

### 14.1. SOPORTE

26. Los elementos de soporte necesarios para la implantación de a presente normativa son:
- Gestor Documental.
  - Gestor de Incidencias.

### 14.2. MODELO DE REGISTRO DE SALIDA DE MATERIAL

27. Modelo de control de los activos de la <<ENTIDAD>> que hubieren de salir fuera de sus dependencias.

(Ejemplo)

| Fecha      | Empresa | Nombre empleado | Firma | Tipo             | Descripción | Comentarios |
|------------|---------|-----------------|-------|------------------|-------------|-------------|
| dd/mm/aaaa |         |                 |       | HW<br>SW<br>INFO |             |             |

### 14.3. MODELO DE REGISTRO DE INTERCAMBIO DE INFORMACIÓN

(Ejemplo)

| Información | Área funcional | Entidad de Intercambio | Medida Adicional |
|-------------|----------------|------------------------|------------------|
|             |                |                        |                  |

## 15. PROTOCOLO DE FIRMA

5. Podrá usarse un formulario como el mostrado seguidamente, si la conformidad con la Política de Confidencialidad de la Información de la <<ENTIDAD>> está expresada en un documento, que habrá de ser suscrito por todos los terceros que tengan acceso a información de la <<ENTIDAD>>.

He leído y comprendido el Acuerdo de Confidencialidad de la <<ENTIDAD>> (versión) y, por medio del presente documento, acepto su contenido íntegramente, en los términos expresados en el citado Acuerdo de Confidencialidad, asumiendo las obligaciones que en él se contienen.

|                     |  |
|---------------------|--|
| <b>Nombre:</b>      |  |
| <b>Apellidos:</b>   |  |
| <b>Empresa:</b>     |  |
| <b>Adscripción:</b> |  |

Firmado por:

<<En \_\_\_\_\_, a \_\_\_\_ de \_\_\_\_ de 20\_\_>>