GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN Centro Criptológico Nacional

Guía de Seguridad de las TIC
CCN-STIC 821

APÉNDICE VI: ACUERDO DE CONFIDENCIALIDAD PARA TERCEROS NP50

CCN Centro Criptológico Nacional

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
2018.02.23 09:32:42 +01'00'

FEBRERO 2018

ÍNDICE

1. OBJETIVO

1. El objetivo de la presente norma es proporcionar un modelo **de Acuerdo de Confidencialidad para Terceros** de 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 de la <<ENTIDAD>>.

2. ÁMBITO DE APLICACIÓN

3. Cuando resulte de aplicación, el Acuerdo de Confidencialidad resultante es de aplicación con carácter obligatorio 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 aquel personal de la <<ENTIDAD>> que tenga la responsabilidad de formalizar convenios o contratos con terceros proveedores o colaboradores (de empresas, otras entidades, profesionales externos o autónomos).

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. En este caso, es especialmente importante el uso que terceros proveedores o colaboradores (de empresas, otras entidades, profesionales externos o autónomos) puedan hacer de los recursos y sistemas de información de la <<ENTIDAD>>.

7. Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la <<ENTIDAD>>.

8. 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

9. 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.

10. 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>>.
11. 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.
12. Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

5. REFERENCIAS

13. *<<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

14. El presente modelo de "Acuerdo de Confidencialidad para Terceros de la <<ENTIDAD>>" complementa, en sus aspectos específicos, a la "NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DE LA <<ENTIDAD>>"[1], por lo que tal normativa general será de aplicación en los aspectos no señalados en aquella.

[1] 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.

7. LA CONFIDENCIALIDAD DE LA INFORMACIÓN

15. La información es uno de los principales activos de cualquier organización. Con carácter general, el personal de terceras instituciones que preste sus servicios en la <<ENTIDAD>> tiene la obligación de guardar secreto sobre el contenido de aquellos documentos (en papel o electrónicos) a los que pudieran tener acceso. Se hace necesario, por tanto, que la <<ENTIDAD>> posea garantía formal y compromiso de los terceros de que la antedicha información no va a ser divulgada más allá de los usos previstos para ella.

16. El Acuerdo establecido en este documento es de aplicación para todo el personal de terceras instituciones que preste sus servicios en la <<ENTIDAD>>, incluido el personal subcontratado.

17. Los responsables o jefes de proyecto de la <<ENTIDAD>>, bajo la supervisión de la <<U/OC>> controlaran que el personal de terceras instituciones que preste sus servicios o desarrolle proyectos en las instalaciones de la <<ENTIDAD>> suscriban en representación de sus respectivas entidades, el protocolo de firma que se incluye en el Anexo II en este Acuerdo.

8. ÁMBITO DE LA CONFIDENCIALIDAD

8.1. DEBER DE CONFIDENCIALIDAD

18. Es el compromiso de no difundir información a la que se ha tenido acceso a través del desempeño de funciones en la <<ENTIDAD>>, derivado de la ejecución de un proyecto o de una relación de servicios, laboral o profesional con el mismo.

8.2. DIFUSIÓN DE LA INFORMACIÓN

19. Es cualquier forma de transmisión de información: verbal, escrita, o por cualquier otro medio físico o telemático, a cualesquiera personas, empresas, instituciones u organizaciones.

20. También se considerará difusión, permitir o facilitar el acceso de forma dolosa o imprudente a la información a la que se hubiere tenido acceso en virtud de una relación de carácter empresarial, laboral o profesional con la <<ENTIDAD>>.

8.3. INFORMACIÓN COMPRENDIDA EN EL DEBER DE CONFIDENCIALIDAD

21. El deber de confidencialidad atañe a cualquier tipo de información, en cualquier formato, contenida en cualquier documento o soporte, que contenga información de la <<ENTIDAD>>. También es de aplicación a aquella información que la <<ENTIDAD>> pueda mantener sobre entidades colaboradoras y terceros en general.

8.4. PROHIBICIÓN DE DIFUSIÓN DE INFORMACIÓN

- A terceros ajenos a la <<ENTIDAD>>.

- Dentro de la <<ENTIDAD>>, no se difundirá la información a aquellas personas que no deban conocerla, cuando tal conocimiento no se derive de sus funciones profesionales.

8.5. INFORMACIÓN NO COMPRENDIDA EN EL DEBER DE CONFIDENCIALIDAD

- La que la propia <<ENTIDAD>> difunda o haga pública por sí misma, y desde el momento en que lo haga.
- La que sea evidente e irrelevante.
- La que haya sido autorizada expresamente por la <<ENTIDAD>> para su difusión.
- La genérica, aquella que no contenga ni aluda a nombres concretos, operaciones, iniciativas, proyectos o situaciones específicas.
- La que hubiera de difundirse por imperativo legal.
- La puramente anecdótica, que no guarde relación con la actividad, ni pueda afectar al desenvolvimiento de la <<ENTIDAD>> o de terceros.

8.6. INFORMACIÓN QUE NO PUEDE DIFUNDIRSE EN NINGÚN CASO

- Aquella cuya difusión pueda causar cualquier tipo de perjuicio a la <<ENTIDAD>>.
- La que pueda dañar derechos de terceros y, en particular, los relativos a su intimidad, su honor o su imagen.
- Cualquier otra información que se encuentre protegida por la legislación vigente en cualquier materia y hubiere sido conocida con ocasión de la prestación de servicios en la <<ENTIDAD>>.

8.7. COMPORTAMIENTO ANTE EL CONOCIMIENTO DE INFORMACIÓN

22. El comportamiento de los terceros usuarios de los sistemas de información de la <<ENTIDAD>> exige no difundir la información a la que se ha tenido acceso de manera legítima, pero no impide naturalmente su conocimiento, dentro del ámbito de actuación que les haya sido asignado, para la prestación de servicios dentro de la <<ENTIDAD>>.

8.8. DURACIÓN DEL DEBER DE CONFIDENCIALIDAD

23. Es un deber de duración indefinida, exigible tanto durante la vigencia de la relación profesional, laboral o formativa con la <<ENTIDAD>>, como tras su conclusión[2].

[2] Por la propia naturaleza de la obligación, la ruptura del deber de confidencialidad finalizada la relación con la entidad supondría una falta de garantías respecto a la intimidad y los derechos de los que la

8.9. RELACIÓN CON EL DEBER DE NO COMPETENCIA

24. Deber de confidencialidad y deber de no competencia son conceptos diferentes. El deber de no competencia es una obligación que implica la prohibición de desarrollar una actividad profesional en empresas de la competencia, durante un determinado periodo de tiempo.

25. El deber de confidencialidad, que se refiere sólo a la transmisión de información, no limita la futura actividad profesional.

8.10. FUNDAMENTO DEL DEBER DE CONFIDENCIALIDAD

26. Tiene diversos fundamentos, materiales y jurídicos:

- La confianza depositada por la <<ENTIDAD>> en el tercero prestador de los servicios, de que los datos de su actividad administrativa, funcional, económica o del personal a su servicio no van a ser revelados.
- Las pautas de discreción habituales, y cuya ruptura podría acarrear serios perjuicios a la <<ENTIDAD>>.
- La consagración por la Constitución Española, como derechos fundamentales, del derecho al honor, la intimidad y la propia imagen, también predicable de colectivos o instituciones.
- La posibilidad de reclamaciones económicas.
- El art. 279 del Código Penal tipifica como delito la revelación de un secreto por quien tenga la obligación legal o contractual de guardar reserva. Además, en el caso del personal laboral, el Estatuto de los Trabajadores establece el deber de buena fe consustancial al contrato de trabajo, y el poder de dirección de la empresa le faculta para exigir a sus empleados que observen los deberes que la propia empresa asume frente a terceros.

27. Cabe indicar también que la jurisprudencia de los Tribunales Laborales exige el cumplimiento de este deber, entendiendo que su trasgresión constituye causa justa de despido, y que el art. 199 del Código Penal considera delito la revelación de secretos ajenos de los que se tenga conocimiento por razón de una relación laboral.

8.11. COMPROMISO DEL USUARIO CON EL DEBER DE CONFIDENCIALIDAD

28. Se trata de un deber, de carácter vinculante, que el tercero asume desde el primer día en que se inicia la relación profesional, laboral o formativa con la <<ENTIDAD>>. La firma del Acuerdo de Confidencialidad solamente lo ratifica y da mayor seguridad a la <<ENTIDAD>> que, además, podrá exigir su firma a cualquier persona relacionada con los proyectos que acometa, en cualquier momento de la relación establecida o que se establezca.

<<ENTIDAD>> es custodio. Los derechos que se protegen con este deber son también imprescriptibles y de duración ilimitada.

8.12. NEGATIVA A FIRMAR EL ACUERDO DE CONFIDENCIALIDAD

29. La primera consecuencia de la negativa a la firma del Acuerdo de Confidencialidad se presenta como un grave obstáculo para que la <<ENTIDAD>> pueda mantener su confianza en la persona o empresa que presta el servicio, ya que no se puede tener la seguridad de que mantenga la obligada discreción respecto a los datos o la información a la que se pudiera tener acceso.

30. Por lo tanto, esta actitud implicará, con justo derecho, un veto por parte de la <<ENTIDAD>> para que el trabajador o la empresa, pueda desarrollar cualquier actividad dentro del mismo.

9. PROTOCOLO DE FIRMA

31. 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.

Nombre:	
Apellidos:	
Empresa:	
Adscripción:	

Firmado por:

<<En _____, a____ de _____ de 20__>>

El Anexo siguiente muestra un Modelo de Acuerdo de Confidencialidad genérico, caso de que la <<ENTIDAD>> deseara particularizar cada Acuerdo de Confidencialidad suscrito con terceros.

ANEXO. MODELO DE ACUERDO DE CONFIDENCIALIDAD

ACUERDO DE CONFIDENCIALIDAD PERSONAL

De una parte, la <<ENTIDAD>> (en adelante, ORGANISMO), en virtud de las facultades que le son atribuidas por <<*precisar habilitación normativa general y/o específica*>>.

Y, de otra parte, D/Dª <<*Nombre y apellidos del receptor de la información y firmante del acuerdo*>>, con NIF <<*DNI del receptor de la información*>>, en calidad de <<*Puesto desempeñado por el firmante en su organización*>>, de <<*Organización a la que pertenece el receptor de la información*>>, en adelante "receptor de la información".

Ambas partes se reconocen recíprocamente la capacidad legal necesaria para la firma del presente Acuerdo de Confidencialidad, y a tal efecto:

EXPONEN

Único. - Que con objeto de dar cumplimiento a los requerimientos del ORGANISMO para tener acceso a la información que pueda solicitar o puede tener acceso el receptor de la información, ambas partes optan por la firma de un Acuerdo de Confidencialidad, lo que llevan a efecto en base a las siguientes,

CLÁUSULAS

Primera. - Objeto

El objeto del presente Acuerdo de Confidencialidad es fijar los términos y condiciones bajo las cuales la parte receptora mantendrá la confidencialidad de la información que le suministre el ORGANISMO, con independencia del medio o soporte en el que se haya efectuado (verbal, escrito, electrónico, o de cualquier otro tipo).

Segunda. - Confidencialidad

La parte receptora de la información la custodiará y dará el tratamiento adecuado al grado de calificación de la información recibida, mediante la aplicación de las garantías y medidas establecidas en…

<<Posibilidades no excluyentes:

- *…la siguiente normativa: [enunciar la normativa que resulta de aplicación al caso, por ejemplo: el ENS, regulación sobre información clasificada, etc.]*
- *La enunciación explícita de las condiciones de confidencialidad y la tipología de la información a la que se aplica. Por ejemplo, cláusulas del tipo:*

[El receptor de la información se compromete a adoptar las medidas oportunas, para asegurar el tratamiento confidencial la información suministrada por la <<ENTIDAD>> o la que hubiere tendido acceso, asumiendo las siguientes

obligaciones:

1. *Usar la información solamente para el uso propio al que sea destinada de acuerdo con el objeto del presente Acuerdo.*
2. *Permitir el acceso a la información únicamente a aquellas personas físicas o jurídicas que necesiten la información para el desarrollo de tareas para las que el uso de esta información sea estrictamente necesario.*
   A este respecto, el receptor de la información advertirá a dichas personas físicas o jurídicas de sus obligaciones respecto a la confidencialidad, velando por el cumplimiento de las mismas.
3. *Comunicar a la <<ENTIDAD>> toda filtración de información de la que tengan o lleguen a tener conocimiento, producida por la vulneración del Acuerdo de confidencialidad o infidelidad de las personas que hayan accedido a la información, bien entendido que tal comunicación no exime al receptor de la información de su responsabilidad, pero si la incumple dará lugar a cuantas responsabilidades se deriven de dicha omisión en particular.*
4. *Limitar el uso de la información al estrictamente necesario para el cumplimiento del objeto de este Acuerdo, asumiendo el receptor de la información la responsabilidad por todo uso distinto al mismo, realizado por ella o por las personas físicas o jurídicas a las que haya permitido el acceso a la información. El presente acuerdo no supondrá, en ningún caso, la concesión de permiso o derecho expreso o implícito para el uso de licencias o derechos de autor, propiedad de la parte que revele la información. El receptor de la información se compromete a no copiar, reproducir, ni por cualquier otro procedimiento, ceder información o material facilitado por la <<ENTIDAD>> o al que hubiere tenido acceso, así como a no permitir a ninguna otra persona, empresa o institución la copia, reproducción o divulgación, sea total, parcial o de cualquier forma, de información o materiales facilitados por la <<ENTIDAD>> o a los que se hubieren tenido acceso en cualquier momento y que obren en poder del receptor de la información, sin la autorización previa de la <<ENTIDAD>>, manifestada expresamente y por escrito*
5. *No desvelar ni revelar la información de la otra parte a terceras personas salvo autorización previa y escrita de dicha otra parte.]>>*

El acceso de terceros a la información a la que se refiere el presente acuerdo, se efectuará en los términos indicados en las disposiciones legales señaladas en el apartado anterior y, en todo caso, previa autorización expresa y escrita del ORGANISMO.

Tercera. - Duración

La información obtenida por aplicación del presente Acuerdo, con independencia del soporte en que esté, y aunque los de naturaleza material hayan sido devueltos al ORGANISMO, será protegida por la parte receptora por tiempo indefinido.

En cualquier momento durante el cumplimiento del presente Acuerdo, el ORGANISMO, sin necesidad de explicar las razones, podrá cesar de suministrar información al receptor y requerirle para la devolución de la ya entregada, que habrá de ser remitida, juntos con todas las copias que pudieran haberse realizado, en el plazo

máximo de un mes.

Cuarta. - Derechos de Propiedad

La información suministrada por el ORGANISMO a la parte receptora es propiedad del mismo, y no supone cesión de ningún derecho, especialmente sobre las patentes, marcas, derechos de autor o cualquier otro derecho de propiedad intelectual o industrial sobre la misma.

Quinta. - Modificación

El presente Acuerdo podrá ser modificado durante su vigencia por mutuo acuerdo expreso y escrito de ambas partes. También podrá ser modificado por decisión unilateral del ORGANISMO, comunicada por escrito a la otra parte.

Sexta. - Resolución

Serán causas de resolución del presente Acuerdo:

a) El incumplimiento de lo establecido en el mismo.

b) La no aceptación por la parte receptora de la información, de la modificación unilateral propuesta por el ORGANISMO.

c) Las demás causas establecidas en Derecho.

Séptima. - Jurisdicción

Las diferencias que puedan surgir sobre la interpretación, modificación, resolución y efectos de la aplicación del presente Acuerdo de Confidencialidad, se resolverán mediante acuerdo entre las partes logrado en los tres meses siguientes a la fecha que surjan.

A falta de acuerdo, ambas partes se someten expresamente a los Juzgados y Tribunales de <<*localización propuesta por el ORGANISMO*>>.

En prueba de conformidad con cuanto antecede, las partes firman el presente acuerdo, en el lugar y fecha indicados *ut supra.*

Por el Receptor de la Información	**Por el ORGANISMO**