Proceso de acreditación delegada para sistemas TIC

Abstract: el presente documento describe las acciones necesarias que se han de acometer por parte de una entidad del ámbito privado en el proceso de acreditación delegada de un sistema TIC para la obtención de una acreditación de seguridad de grado DIFUSIÓN LIMITADA o equivalente.

Contenido:

1. ALCANCE

Todo Sistema de las Tecnologías de la Información y la Comunicación (Sistema TIC) que vaya a manejar información clasificada de cualquier grado tiene que estar previamente acreditado. Para el grado de ***DIFUSIÓN LIMITADA o equivalente*** esta acreditación puede ser llevada a cabo por la empresa o entidad del sector privado (en adelante "entidad de ámbito privado") que vaya a manejar información clasificada, siempre bajo su responsabilidad.

Este proceso establece el conjunto de acciones necesarias que se deben acometer en un sistema TIC de cara a obtener una acreditación de seguridad de grado ***DIFUSIÓN LIMITADA o equivalente*** a través de este proceso de acreditación delegada, en los ámbitos de competencia de la *Oficina Nacional de Seguridad (ONS)*.

Con anterioridad al inicio de la acreditación, el *Jefe del Servicio de Protección de Información Clasificada* (*JSPIC*) de la entidad de ámbito privado, propietaria del futuro sistema TIC a acreditar, deberá leer en detalle la Norma NS/05 de las Normas de la *Autoridad Nacional de Seguridad* y la normativa adicional del *Centro Criptológico Nacional* que en ella se menciona, para familiarizarse con todos los procesos que se van a ejecutar.

Los aspectos generales y específicos del manejo de información clasificada, establecidos en el resto de la normativa de la *Autoridad Nacional de Seguridad*, serán igualmente de aplicación.

2. OBJETO

Establecer los criterios y las referencias para que una entidad de ámbito privado pueda acogerse al procedimiento de acreditación delegada para sistemas TIC que vayan a manejar información clasificada de grado ***DIFUSIÓN LIMITADA o equivalente***.

3. RESPONSABILIDADES

El *JSPIC* responsable del sistema TIC que vaya a manejar información clasificada que se acoja a implementar el proceso de acreditación delegada, tendrá la responsabilidad de asegurar la protección de dicha información de conformidad con la normativa aplicable.

El *JSPIC* también actuará como único punto de contacto con la *Oficina Nacional de Seguridad*.

La *Oficina Nacional de Seguridad* y el *Centro Criptológico Nacional* mantendrán la responsabilidad de la protección de la información manejada por la entidad de ámbito privado y tendrán el derecho de inspeccionar las medidas de seguridad implementadas durante toda la vida del sistema TIC.

4. SEGURIDAD DEL PERSONAL Y FORMACIÓN

Para acceder a información clasificada de grado ***DIFUSIÓN LIMITADA o equivalente*** no hace falta estar en posesión de ninguna *Habilitación Personal de Seguridad* (HPS). Solamente es necesario tener "necesidad de conocer" ("need-to-know"), haber sido formado sobre el manejo de dicha información y dar conocimiento de haber entendido completamente sus responsabilidades.

El *JSPIC* de la entidad de ámbito privado deberá de establecer los requisitos que deben de ser entendidos por el personal que va a manejar información clasificada. Los requisitos deben de estar documentados en la documentación de seguridad del sistema acreditado.

Se formará de manera periódica a todo el personal que vaya a manejar información clasificada, insistiendo especialmente:

- En la normativa de seguridad del sistema.
- En la detección y reacción ante incidentes de seguridad o comprometimiento de la información clasificada.
- El manejo y custodia de la información clasificada.

El personal que vaya a utilizar el sistema acreditado para el manejo de información clasificada de grado ***DIFUSIÓN LIMITADA o equivalente*** deberá leer y firmar los *Procedimientos Operativos de Seguridad* (POS) específicos del sistema. Este reconocimiento de sus responsabilidades deberá ser custodiado por el *JSPIC*.

La norma NS/02 de las Normas de la *Autoridad Nacional de Seguridad* detalla la concienciación e instrucción de seguridad del personal.

5. SEGURIDAD FÍSICA

La información clasificada de grado ***DIFUSIÓN LIMITADA o equivalente*** debe ser manejada en una *Zona Administrativa de Protección* (ZAP) o bien contemplar escenarios alternativos que, a través de la implementación de medidas compensatorias de seguridad y complementarias de vigilancia, pueda reducirse al mínimo el riesgo de pérdida o compromiso de este tipo de información clasificada.

El *JSPIC* será responsable de establecer las *Zonas Administrativas de Protección* precisas para el manejo de la información clasificada en sus propias instalaciones o bien establecer el conjunto de medidas compensatorias de seguridad y complementarias de vigilancia, conforme a los procedimientos y criterios de la *Oficina Nacional de Seguridad* y del *Centro Criptológico Nacional*.

Para establecer una *Zona Administrativa de Protección*, se debe utilizar como referencia el documento "*OR-ASIP-04-01.05 - Orientaciones para el manejo de información DIFUSIÓN LIMITADA*" (disponible en la página Web de la *Oficina Nacional de Seguridad*). A la vez que se establecen las medidas de seguridad indicadas en esta orientación, el *JSPIC* deberá redactar un Plan de Protección que detalle la ubicación, describa las medidas físicas que dispone y desarrolle los procedimientos de gestión de personal y documentos dentro de esa *Zona Administrativa de Protección*. Además, deberá incluir un plano de planta señalando la situación y perímetro exactos.

Por otra parte, si se establece un escenario alternativo a la *Zona Administrativa de Protección*, el personal debe cumplir todas las medidas compensatorias de seguridad y complementarias de vigilancia definidas en la Documentación de Seguridad del Sistema. Se deberán definir adecuadamente las medidas compensatorias de seguridad y complementarias de vigilancia con el objetivo de reducir al mínimo el riesgo de pérdida o comprometimiento de la información clasificada cuando el sistema es utilizado fuera de las Zonas de Seguridad de la organización (POS particulares).

6. SEGURIDAD DE LAS TIC

Todo sistema de las TIC que maneje información clasificada deberá de disponer de un conjunto equilibrado de servicios y requisitos de seguridad que permita alcanzar los objetivos de seguridad requeridos, que deberá ser completado con los requisitos de seguridad obtenidos en el análisis de riesgos preceptivo.

Todos los requisitos de seguridad del sistema TIC tendrán que estar recogidos en su documentación de seguridad, debiendo actualizarse cada vez que se produzca una modificación.

Servicios y requisitos de seguridad deberán de seguir lo expuesto en la guía "*CCN-STIC 301 - Medidas de Seguridad de las TIC a Implementar en Sistema Clasificados*", en particular, lo recogido en su ANEXO B, así como cualquier otra norma o procedimiento que dictamine el *Centro Criptológico Nacional* dentro de su ámbito de competencia.

Por otro lado, cuando se lleve a cabo una interconexión entre sistemas TIC, será también de aplicación la guía "*CCN-STIC 302 - Interconexión de Sistemas*".

Fijado el propósito de la acreditación delegada, la entidad de ámbito privado deberá obtener la Declaración de Conformidad STIC del sistema TIC propósito de la acreditación por parte del *Centro Criptológico Nacional*. Dicha conformidad se podrá obtener tras la realización de una Inspección STIC que, o bien realizará el *Centro Criptológico Nacional* o bien podrán realizarlas entidades auditoras certificadas[1] de acuerdo con la guía "*CCN-STIC 120 - Procedimiento de certificación de empresas para la realización de auditorías DL*"[2].

Para cualquier consulta o información se puede visitar la página Web del *Centro Criptológico Nacional*: *www.ccn.cni.es*.

7. DOCUMENTACIÓN DE SEGURIDAD

Todo sistema de las TIC que maneje información clasificada de grado DIFUSIÓN LIMITADA o equivalente deberá incluir dentro de su marco normativo aquellos aspectos de seguridad especificados en las normas de aplicación (Serie CCN-STIC 200).

La implementación de las medidas incluidas en dicho marco normativo se podrá estructurar mediante una hoja de ruta de vigilancia y supervisión (*suite de vigilancia*) materializada a través de Soluciones de Seguridad del *Centro Criptológico Nacional* que permitan una gestión de la ciberseguridad adecuada.

8. DECLARACIÓN RESPONSABLE

El *JSPIC* deberá proporcionar, firmado por él, una declaración de cumplimiento en la que se certifique que el sistema TIC cumple con las políticas y normas de seguridad aprobadas por la *Oficina Nacional de Seguridad* y el *Centro Criptológico Nacional* o las establecidas por el propietario de la información manejada en el sistema TIC.

[1] Enlace relacionado: https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/entidades-de-certificacion

[2] Véase: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3119-ccn-stic-120-procedimiento-acreditacion-empresas-dl/file.html

Para poder presentar esta declaración responsable, el sistema TIC deberá contar inexcusablemente con la pertinente Declaración de Conformidad STIC emitida por el *Centro Criptológico Nacional*, tal como se ha detallado en el apartado de Seguridad de las TIC.

Una vez emitida esta declaración, se deberán mantener las condiciones de seguridad iniciales durante toda la vida del sistema.

9. VALIDEZ DE LA ACREDITACIÓN

Se establece un periodo de validez de 36 meses (3 años). Una vez concluido este período, se deberá iniciar un proceso de renovación. También son motivo de renovación los cambios en el sistema TIC que afecten a las condiciones de seguridad del mismo.

10. DOCUMENTACIÓN A PRESENTAR

Una copia de la siguiente documentación deberá ser entregada a la *Oficina Nacional de Seguridad* para su estudio y custodia:

- La Documentación de seguridad STIC generada para el sistema TIC (apartado DOCUMENTACIÓN DE SEGURIDAD).
- Declaración de constitución de la Zona Administrativa de Protección (apartado SEGURIDAD FÍSICA).
- Declaración de Conformidad STIC emitida por el *Centro Criptológico Nacional* (apartado SEGURIDAD DE LAS TIC).
- Declaraciones individuales de haber leído los POS firmadas por todos los usuarios (apartado SEGURIDAD DEL PERSONAL Y FORMACIÓN).
- Declaración responsable firmada por el *JSPIC* (apartado DECLARACIÓN RESPONSABLE).

11.DOCUMENTACIÓN DE REFERENCIA

- Normas de la Autoridad Nacional para la protección de la Información Clasificada (*www.cni.es/es/ons*).
- Serie CCN-STIC 100.
- Serie CCN-STIC 200.
- CCN-STIC 301 - Medidas de Seguridad de las TIC a Implementar en Sistema Clasificados.
    - ANEXO B - Requisitos de Seguridad TIC específicos para Sistemas que manejan Información Clasificada hasta DIFUSIÓN LIMITADA.

- CCN-STIC 302 - Interconexión de Sistemas.
- Directive on Classified Project and Industrial Security (AC/35-D/2003-REV5).
  - APPENDIX 4 - Contract Security Clause for Inclusion in Tenders and Contracts involving NATO RESTRICTED infomation.
  - APPENDIX 5 - Security Aspects Letter (SAL).
- COMMISSION DECISION (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information.
- COMMISSION DECISION (EU, Euratom) 2019/1963 of 17 October 2019 laying down implementing rules on industrial security with regard to classified procurement contracts.

12.CONTACTO

Para consultas sobre acreditación de sistemas TIC en la *Oficina Nacional de Seguridad*:

- cis.ons@areatec.com
- www.cni.es/es/ons

Para consultas sobre seguridad de los sistemas TIC en el *Centro Criptológico Nacional*:

- acreditacion@ccn.cni.es
- www.ccn.cni.es

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.02.22 02:57:35 +01'00'