13. PROCEDIMIENTO PARA LA ACREDITACIÓN DE LOS SISTEMAS CIS.

Para el manejo y custodia de Información clasificada en un Sistema de Información y Comunicaciones, el contratista deberá tener concedida en primer lugar una HSEM y una HSES del grado correspondiente a la información a tratar en los sistemas y deberá solicitar, además, la Acreditación del Sistema de Información y Comunicaciones y el nombramiento de un Administrador de Seguridad de los Sistemas de Información (ASSI).

La acreditación será concedida en base a unas determinadas condiciones de seguridad de la Información clasificada, tanto en lo referente a la Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC), como a la Seguridad en el Personal, la Seguridad Física de las instalaciones y la Seguridad de la Información, que deberán ser previamente acreditadas, y de las que el solicitante deberá aportar las evidencias documentales necesarias para su valoración y aprobación, en todo caso se ajustará a lo establecido en la normativa sobre seguridad de la información en los sistemas de información y telecomunicaciones que esté en vigor en el Ministerio de Defensa.

La acreditación tiene un carácter temporal, por lo que deberá renovarse siempre que transcurra su plazo de validez o que se produzcan cambios que supongan una modificación apreciable de las condiciones de seguridad.

Serán objeto de Acreditación específica, por un lado, los Sistemas dedicados al manejo de Información clasificada (típicamente estaciones aisladas, redes de área local y redes de área extensa), y por otro, las interconexiones entre dos o más de estos Sistemas.

Para cada Sistema e interconexión de Sistemas se emitirá, una vez aprobadas sus condiciones seguridad (Seguridad de la Información – documental -, Seguridad en el Personal, Seguridad Física - de las instalaciones - y Seguridad en los Sistemas), el correspondiente Certificado de Acreditación.

Todo proceso de Acreditación de Sistemas se regirá por las siguientes fases:

Fase 1.- Inicio del proceso de Acreditación:

La empresa que desee acreditar sus sistemas CIS, presentará por escrito solicitud a la DGAM (SDGINSERT)—acompañado de la documentación acreditativa de estar en posesión de HSEM y HSES. Además, deberá incluir una descripción del Sistema a acreditar, que se ajustará al formato de Concepto de Operación definido en el anexo XVIII.

Una vez aprobada la documentación aportada, se comunicará este hecho a la empresa.

Fase 2.- Elaboración y aprobación de la documentación de seguridad:

La empresa, una vez aprobado el Concepto de Operación, elaborará el resto de documentación de seguridad exigida en cada caso.

Dicha documentación, junto con aquella complementaria que en su caso se pueda solicitar para acreditar la certificación con que cuente el personal y los locales del Sistema, deberá ser enviada igualmente para su aprobación.

Fase 3.- Implementación del Sistema y de su entorno de seguridad:

Una vez aprobada la documentación de seguridad del Sistema, la empresa podrá ponerlo en funcionamiento, de acuerdo a dicha documentación y a las condiciones de seguridad especificadas en ella.

La empresa comunicará a la DGAM (SDGINSERT), con antelación suficiente, la fecha a partir de la cual el Sistema y su entorno de seguridad (entornos de seguridad local, global y electrónico) estarán listos para su inspección, a fin de que esta última pueda comunicarlo al Organismo que ha de efectuarla.

Fase 4.- Inspección del Sistema y de su entorno de seguridad:

El Sistema a autorizar será inspeccionado por el Órgano competente a fin de verificar su correcta implementación, de acuerdo a la documentación de seguridad aprobada.

El resultado de dicha inspección será comunicado oficialmente a la empresa. Aun resultando positiva la evaluación realizada, ésta no constituye en sí una autorización al Sistema para operar, la cual será comunicada oficialmente por escrito, una vez verificado el resto de condicionantes (seguridad física, seguridad en el personal y seguridad documental).

Fase 5.- Acreditación:

Tras la verificación positiva de las condiciones de seguridad del Sistema (seguridad documental, seguridad física, seguridad en el personal y seguridad técnica), se emitirá del correspondiente Certificado de Acreditación, el cual constituye, a todos los efectos, la única autorización para que el Sistema maneje Información clasificada.

Fase 6.- Explotación del Sistema

Una vez obtenido el Certificado de Acreditación, se deberán mantener las condiciones de seguridad iniciales que dieron lugar a dicha autorización. En caso contrario, este Certificado de Acreditación pierde automáticamente toda validez, siendo imprescindible la superación de un proceso de reacreditación, destinado a la obtención de un nuevo Certificado de Acreditación del Sistema.

Con el fin de verificar que los Sistemas autorizados para el manejo de Información clasificada mantienen las condiciones de seguridad que dieron lugar a la Acreditación, éstos se someterán a un proceso de inspecciones de seguridad periódicas.

Fase 7.- Reacreditación

Transcurrido el periodo de validez del Certificado de Acreditación, el Sistema pierde su autorización para manejar Información clasificada. Es responsabilidad de la empresa el iniciar, con la antelación suficiente, los trámites para la reacreditación del mismo.

También son motivo de reacreditación del Sistema los cambios que afecten a sus condiciones de seguridad. Antes de realizar dichos cambios, éstos deben

ser aprobados por el Órgano competente, que verificará el impacto de dichos cambios en las condiciones de seguridad exigidas al sistema.

Fase 8.- Baja del Sistema

Cuando acaba la vida útil de un Sistema autorizado para el manejo de Información clasificada, es responsabilidad de la empresa garantizar la correcta desclasificación de sus activos y la destrucción de la Información clasificada almacenada en él.

Los procedimientos a seguir en este caso estarán recogidos en el Documento de Requisitos de Seguridad del Sistema o interconexión, tal y como se indica en la guía CCN STIC 202.