INSTRUCCIÓN TECNICA
AUDITORIA Y CERTIFICACIÓN ENS (DISTRIBUCIÓN EXTERNA)
ENS-IT01 / 231110

ELABORADO POR: DIRECCIÓN TECNICA – DIRECCIÓN DE PRODUCTO

APROBADO POR: DIRECCIÓN TECNICA

FECHA DE APROBACIÓN: 10-11-2023

OBJETO Y ALCANCE

La presente instrucción tiene por objeto resumir el proceso y criterios empleados por ADOK CERTIFICACIÓN, S.L. (en adelante, ADOK) en sus servicios de auditoría y certificación del Esquema Nacional de Seguridad (en adelante, ENS). La finalidad del documento es disponer de una documentación para su disposición pública externa.

DESARROLLO

1. PROCESO COMERCIAL

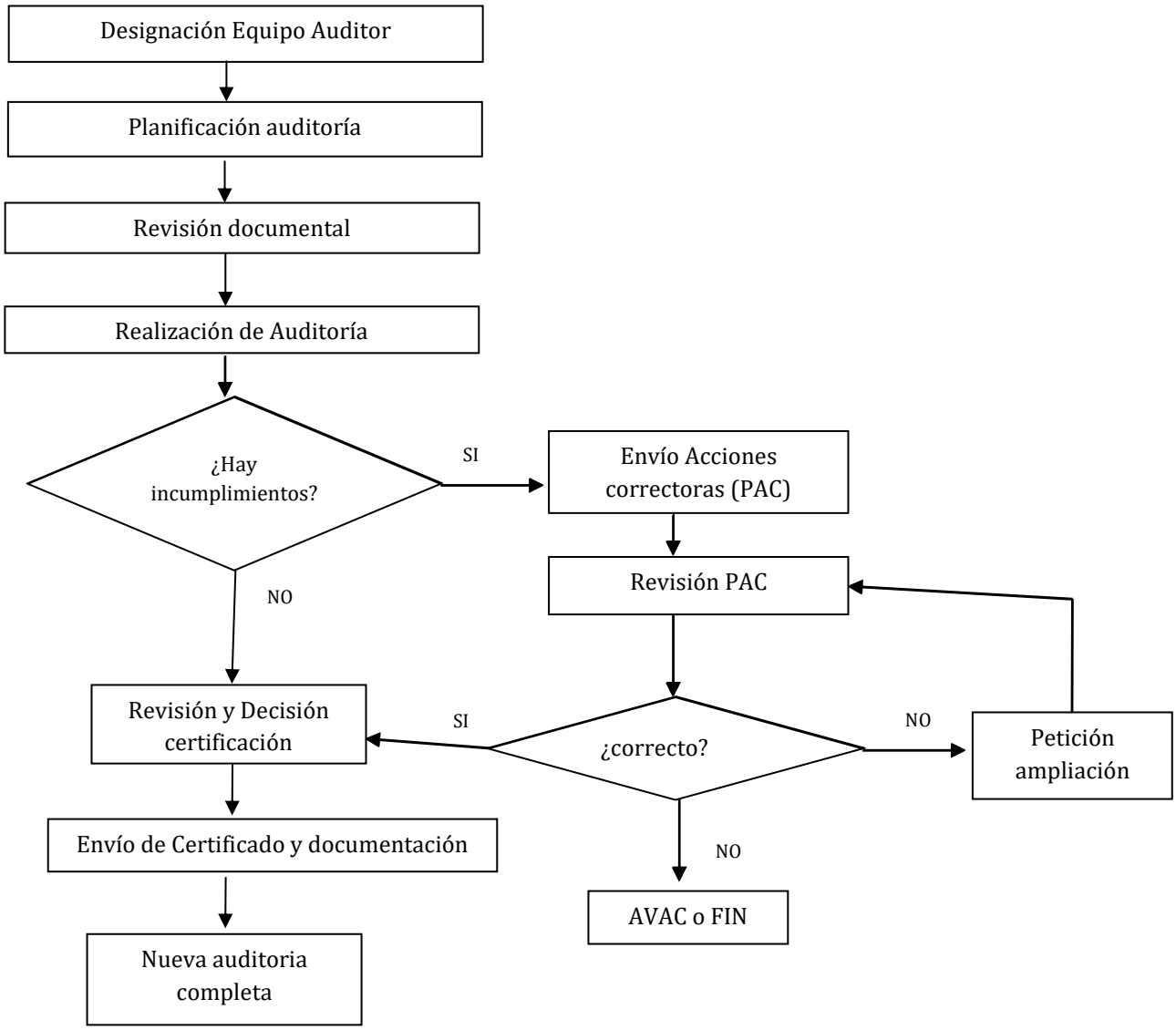
Previamente al inicio del proceso de auditoria con la planificación, se realiza el proceso comercial que comprende las siguientes fases:

- ADOK recaba del cliente todos los datos necesarios para presentar una oferta de certificación. Esto se realiza a través del documento de solicitud de oferta de certificación.
- Con los datos aportados, el departamento técnico de ADOK realiza una revisión técnica obteniendo la información necesaria para realizar la auditoria y en consecuencia, emitir la oferta.
- ADOK emite una oferta vinculante en la que se incluyen los servicios ofertados y las características
- El cliente debe aceptar y firmar la oferta convirtiéndose esta en contrato y así para poder iniciar el proceso de auditoría.

Existe la posibilidad de la realización de presupuestos previos, individuales o grupales, los cuales no son vinculantes, ya que posteriormente en todos los casos debe ser emitida la oferta-contrato individual definitiva.

2.- PROCESO GENERAL DE AUDITORIA Y CERTIFICACION

El proceso general de auditoría de sistemas de gestión bajo acreditación se describe a continuación:


Designación Equipo Auditor
Planificación auditoría
Revisión documental
Realización de Auditoría
¿Hay incumplimientos?
SI
Envío Acciones correctoras (PAC)
Revisión PAC
NO
Revisión y Decisión certificación
SI
¿correcto?
NO
Petición ampliación
Envío de Certificado y documentación
NO
AVAC o FIN
Nueva auditoria completa

3.- PROGRAMACIÓN DE LA AUDITORIA

Una vez aprobado por el cliente el contrato, ADOK procede a realizar la planificación de la auditoria inicial (o las siguientes ordinarias completas, según corresponda).

El departamento de programación de ADOK contacta con el cliente con antelación suficiente para acordar las fechas y condiciones de cada una de las auditorias. Una vez acordadas las fechas, el departamento de programación junto con el departamento técnico realiza la asignación del equipo auditor.

La auditoría puede ser desarrollada in situ o remoto (total o parcialmente).

4.- PLANIFICACIÓN DE LA AUDITORIA

Objetivos de las auditorias

La Auditoría de la Seguridad es un proceso sistemático, independiente y documentado, para la obtención de evidencias y su evaluación objetiva, con el fin de determinar el grado de conformidad con el ENS del sistema de información auditado. Debe permitir a sus responsables adoptar las medidas oportunas para subsanar las deficiencias y atender a las observaciones o recomendaciones que pudiera haber identificado el Equipo Auditor y, en su caso, posibilitar la obtención de la correspondiente Certificación de Conformidad, tal y como dispone la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad, regulada por Resolución de 13 de octubre de 2016, del secretario de Estado de Administraciones Públicas.

Concretamente, los objetivos son:

- El objetivo de esta auditoría es determinar la conformidad del Sistema de información de la organización auditada, dentro del alcance, con las disposiciones del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Verificar el cumplimiento de los requisitos establecidos en los capítulos II, III, IV, V, VI y en los Anexos I, II y III del ENS. Todo ello de acuerdo con el Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Evaluar y verificar la existencia y la eficacia del sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección, tomando como base la Declaración de Aplicabilidad regulada en el artículo 28 del RD 311/2022, en su totalidad de acuerdo con la categoría de aplicación.
- Dictaminar sobre el grado de cumplimiento del RD 311/2022, identificar sus deficiencias y sugerir las posibles medidas correctoras o complementarias necesarias, así como las recomendaciones que se consideren oportunas.

Determinación del alcance

El alcance de la auditoría debe estar claramente definido, documentado y consensuado entre ADOK y la organización a certificar. Se deberá haber determinado en la fase comercial pero este alcance deberá ser corroborado (y modificado, si fuera el caso) por el equipo auditor.

Para definir el alcance hay que tener en cuenta:

- Para una correcta definición del alcance se debe tener en cuenta la naturaleza de las distintas medidas de seguridad a auditar, así como las conexiones de los sistemas de la administración pública con entidades públicas y privadas.

- Tanto los sistemas de información como los servicios sustentados en dichos sistemas deberán aparecer explícitamente mencionados en el Certificado de Conformidad con el ENS que, en su caso, se expida, y que se ajustará a lo dispuesto en la Resolución, de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Asimismo, con el objetivo de ofrecer la debida transparencia en el cumplimiento del ENS y del resto de regulaciones concordantes, los certificados de conformidad con el ENS de aquellos sistemas de información que ofrezcan servicios en la nube, expresarán, dentro de la mención a los servicios comprendidos en el alcance, la ubicación (ciudad, región y país) de los CPD en los que se soportan dichos servicios, junto con una mención sobre los que hayan sido objeto de evaluación directa por parte de ADOK en la auditoría.
- En tanto los Servicios Compartidos ofrecidos por la Administración General del Estado (AGE) o, en su caso, por las Administraciones Territoriales competentes, que pudieran estar comprendidos en el alcance de la auditoría no dispongan de la preceptiva Certificación de Conformidad con el ENS, la Auditoría de Conformidad con el ENS deberá concentrarse solo en los servicios que puedan satisfacerse a través de los propios sistemas de información de la organización auditada (o en sistemas de información externos que posean la Certificación de Conformidad con el ENS o puedan ser auditados y certificados en tal sentido).
- De no ser posible lo anterior, y cuando se trate de la utilización de Servicios Compartidos suministrados por la AGE o, en su caso, por las Administraciones Territoriales competentes, el alcance de la Certificación de Conformidad (y la subsiguiente Certificación de Conformidad) habrá de señalar la parte que ha sido auditada, mencionando, expresamente, que la porción no auditada (ACCEDA o GEISER, por ejemplo) no se encuentra comprendida en tal alcance.
- Cuando el alcance de la Certificación de Conformidad con el ENS comprenda sistemas de información utilizados para la prestación de servicios comercializados bajo signos distintivos (marcas y nombres comerciales), la denominación de tales signos deberá figurar, explícitamente, en la Certificación de Conformidad.

Planificación de la auditoria

De manera previa a la realización de la auditoria in situ, y según se indica en la guía CCN-STIC 802 "Guía de auditoría", el auditor jefe solicitará a la organización la siguiente documentación mínima:

- Documentos firmados por el órgano superior correspondiente que muestren el conocimiento y la aprobación formal de las decisiones en materia de política de seguridad.
- Documentos descriptivos de los Sistemas operativos utilizados en equipos y servidores, tipos de ordenadores (sobremesa, portátiles, etc.…), redes, dispositivos portátiles, móviles, elementos de seguridad física, etc.
- Organigrama de los servicios o áreas afectadas, con descripción de funciones y responsabilidades.
- Identificación de los responsables: de la información, de los servicios, de la seguridad y del sistema.
- Descripción detallada del sistema de información a auditar (ubicaciones, redes, líneas de defensa, comunicaciones, software, hardware, comunicaciones, equipamiento auxiliar, ubicaciones y similares).
- Guías de bastionado o descripción de la configuración de los componentes (hardware, software, comunicaciones, etc.…) que intervienen en el sistema de gestión del ENS.
- Inventario de hardware y software utilizados (con indicación de los fabricantes y sus versiones), incluidos antivirus, firewalls, etc.…

- Inventario de componentes certificados u homologados por el CCN u otros criterios de adquisición de nuevos componentes.
- Procedimientos operativos documentados (Adquisición de nuevos componentes, gestión de cambios, gestión de capacidad, gestión de incidentes de seguridad de la información, gestión de riesgos de seguridad de la información, gestión documental, auditorías internas, gestión de autorizaciones, etc.…).
- Categoría del sistema según el Anexo I del ENS, incluyendo los criterios de identificación y valor de los niveles de las dimensiones de seguridad que serán de aplicación al sistema.
- La Política de Seguridad.
- La Política de Firma Electrónica y Certificados (si se emplean estas tecnologías).
- La Normativa de Seguridad (que se entrega al personal de la organización).
- Descripción detallada del sistema de gestión de la seguridad y la documentación que lo sustancia.
- Informes con el desarrollo y resultado de la apreciación del riesgo, incluyendo la identificación de escenarios de riesgo, su análisis y evaluación.
- La Declaración de Aplicabilidad.
- Decisiones adoptadas para tratar los riesgos.
- Relación de las medidas de seguridad implantadas por requisitos legales o como resultado de la apreciación del riesgo.
- Relación de registros de actividad en lo relativo a las medidas de seguridad implantadas y estado de implantación.
- Informes de otras auditorías previas de seguridad relacionados con los sistemas y servicios incluidos en el alcance de la auditoría, como podría ser el informe de auditorías relativas a la protección de datos de carácter personal, o de auditorías previas con el mismo objetivo y alcance que la auditoría a comenzar.
- Informes de seguimiento de deficiencias detectadas en auditorías previas de seguridad, y relacionadas con el sistema a auditar.
- Lista de proveedores externos cuyos servicios se ven afectados o entran dentro del alcance de la auditoría, y evidencias del control realizado sobre estos servicios.
- Sistemas de métricas con referencia a las guías CCN-STIC-815 “Sistema de Métricas e Indicadores”, CCN-STIC -824 “Informe Nacional del Estado de la Seguridad, teniendo en consideración lo indicado en la Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad”
- Cualquier otra información que se considere necesaria.

Plan de auditoria

En base a esta información, el auditor jefe prepara el plan de auditoría, que envía con antelación suficiente a la organización y al resto del equipo auditor.

En el plan se establece, entre otra información, el calendario, horarios, procesos y/o requisitos a auditar. El cliente puede recursar al equipo auditor.

5.- REALIZACIÓN DE LA AUDITORIA

Reunión inicial

Al inicio de la auditoría, se llevará a cabo una reunión inicial en la que el auditor jefe expondrá los siguientes aspectos:

- presentación de equipo auditor, incluyendo breve descripción de sus funciones
- confirmación del plan de auditoría (incluyendo el tipo y el alcance, los objetivos y los criterios), de posibles cambios, y ajustes horarios según disponibilidades incluyendo reunión de cierre y reuniones intermedias
- presentación de los canales de comunicación entre la organización y el equipo auditor
- confirmación de la disponibilidad de recursos y logística necesaria para poder realizar la auditoria
- explicación del compromiso de confidencialidad
- confirmación de los procedimientos de protección, emergencia y seguridad en el trabajo pertinentes para el equipo auditor
- confirmación de la disponibilidad, de las funciones y de la identidad de los interlocutores
- explicación del método de presentación de la información, incluyendo la clasificación de los incumplimientos
- información sobre las condiciones bajo las cuales la auditoría puede darse por terminada prematuramente
- confirmación de que el auditor jefe y el resto de los miembros del equipo auditor, como representantes del organismo de certificación, son los responsables de la auditoría controlando la ejecución del plan, incluyendo las actividades y las líneas de investigación de la auditoría
- explicación de sistemática y métodos a emplear para realizar una auditoría basada en muestreo
- confirmación del idioma de la auditoría
- confirmación de que durante la auditoría se mantendrá informado a la organización auditada sobre el progreso de la auditoria y cualquier problema
- información sobre el derecho del cliente a presentar reclamación por cualquier aspecto del servicio prestado
- información del derecho del cliente a formular preguntas, a alegar el resultado del informe y a apelar la decisión de la entidad

Criterios de auditoría

Los documentos de referencia, que actúan como criterios de auditoría son:

- Marco de control: ENS - Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad
- Guías CCN-STIC de aplicación: estas deben considerarse como “mejores prácticas”.
- Análisis de Riesgos – Alcance de la Auditoria
- Documentación referente al SGSI
- Declaración de Aplicabilidad
- Presente procedimiento de ADOK

Metodología para la realización de la auditoria

El equipo auditor, bajo la coordinación del auditor jefe, realizará la auditoría obteniendo evidencias de cumplimiento de todas las disposiciones del ENS que sean de aplicación, en función de la categoría del sistema que se certifica, a fin de determinar si el nivel de cumplimiento alcanzado por el auditado es correcto y suficiente como para obtener el certificado de conformidad correspondiente.
Para ello emplearán las técnicas de auditoría que consideren necesarias.

Las evidencias se obtendrán mediante:
- la revisión de los registros aplicables
- la observación in situ de la realización de las actividades y de las instalaciones, materiales y equipamientos
- entrevista con los responsables y el personal implicado en cada caso

Es necesario auditar específicamente las 73 medidas de seguridad que determina el anexo II del RD 311/2022, siempre que sean de aplicación en función de la categorización del sistema, junto a otros requisitos en el cuerpo del propio RD 311/2022. Todo ello siguiendo lo dispuesto en la Guía "CCN-STIC 802. ENS Guía de Auditoría" que desarrolla la Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información. Así mismo, el equipo auditor deberá tener en cuenta lo definido en la Guía CCN-STIC 808 "Verificación del cumplimiento del ENS".

El equipo auditor, en su caso, puede utilizar tecnologías de auditoría en remoto, tales como teleconferencias, reuniones vía web, comunicaciones interactivas por web, acceso electrónico remoto a documentación, etc.

En el caso de auditorías de organizaciones que engloban varias razones sociales en el mismo sistema de gestión, el sistema debe cumplir lo siguiente:
- su diseño, operación y resultados responden a una Dirección concreta (fijar políticas y asignar presupuestos y proporcionar recursos).
- la documentación del sistema debe ser única y su control debe estar unificado
- los registros generados que respondan a requisitos generales del sistema deben ser comunes.
- las instalaciones que afectan al ENS serán las mismas o idénticas
- el organigrama y funciones y responsabilidades, aunque en algunos casos puedan ser diferentes, al menos deberá existir dentro del sistema un único responsable de la gestión del sistema y una única dirección con la autoridad suficiente.
- el responsable de la gestión del sistema debe ser una única persona y con capacitación para responder a cuestiones de las diferentes empresas
- los alcances de cada razón social deben ser iguales

Reclamaciones de tercera parte
En el caso de que ADOK haya recibido una reclamación de un tercero sobre el sistema de gestión a auditar, se sigue lo definido en el procedimiento correspondiente. Si en la auditoria se requiere una investigación sobre la reclamación, junto con la asignación estará toda la información sobre la misma. El auditor deberá reflejar en las notas y en el informe de auditoría de manera clara la información obtenida y las conclusiones a las que ha llegado. Las conclusiones pueden implicar la apertura de incidencias o no conformidades.

Hallazgos de auditoria
Los hallazgos se clasifican de la siguiente manera:
- No conformidades menores: Se documentará una "No Conformidad Menor" ante la ausencia o el fallo en la implantación o mantenimiento de uno o más de los requisitos del ENS, incluyendo cualquier situación que pudiese, en base a una evidencia objetiva, sustentar una duda significativa sobre la conformidad del sistema de información con uno o más de tales requisitos.

- No conformidades mayores: Se documentará una "No Conformidad Mayor" cuando se detecten "No Conformidades Menores" en relación con cualquiera de los preceptos contenidos en el RD 311/2022, o en el Marco organizativo, o en alguno de los subgrupos que integran el Marco operacional o las Medidas de protección (Planificación, Control de Accesos, Explotación, Servicios Externos, Continuidad del Servicio, Monitorización del Sistema, Protección de las Infraestructuras, Gestión del Personal, Protección de Equipos, Comunicaciones, Soportes de Información, Aplicaciones Informáticas, Información o Servicios) que, evaluadas en su conjunto, puedan implicar el incumplimiento del objetivo del Grupo o Subgrupo considerados.
- Observación: Se documentará una Observación cuando se encuentren evidencias de una debilidad, una vulnerabilidad o una situación que, sin comprometer cualquier área del sistema de gestión definida en el ENS o por la organización, pueda, en la actualidad o en el futuro, derivar en un problema.

Más concretamente, y tal y como se define en CCN-IC-01-19:
Se considera la existencia de una no conformidad mayor:

- Ante el incumplimiento de un artículo del RD311/2022 y/o el incumplimiento total de un conjunto de medidas/controles pertenecientes a un dominio del Anexo II en función de la categorización del sistema.
- Cuando existen incumplimientos de carácter legal relacionados con la seguridad de la información.
- Cuando la desviación afecta a la capacidad del sistema de información para atender sus funciones esenciales.
- Cuando exista una duda razonable de que se haya implementado un control eficaz del proceso, o de que las medidas de seguridad cumplan los requisitos especificados.
- Cuando se evidencie un número significativo de no conformidades menores asociadas al mismo requisito.
- Cuando el número de no conformidades menores detectadas impidan deducir la adecuación del sistema a los principios básicos y requisitos mínimos del Esquema Nacional de Seguridad.
- Cuando se detecte un incumplimiento del deber de adecuada exhibición de los Distintivos de Conformidad según marca el art.41 del ENS detectado durante una auditoría (no en auditorias iniciales).

Se considera la existencia de una no conformidad menor:

- Ante el incumplimiento parcial de algún artículo del RD311/2022 y/o el incumplimiento parcial de alguna medida/control (o algún requisito de alguna medida/control) del Anexo II en función de la categorización del sistema.
- Cuando, sin afectar a la capacidad del sistema de protección para lograr los resultados previstos; los requisitos se cumplen de forma manifiestamente mejorable, o se aprecian incoherencias entre requisitos que deberían estar alineados.

Por otra parte, hay que tener en cuenta que la inadecuación total o parcial del sistema de información evaluado a lo dispuesto en la Guía CCN-STIC que resultare de aplicación en cada caso, podría identificado también como un hallazgo de auditoría (Observación, No Conformidad Menor o No Conformidad Mayor), atendiendo al impacto que su incumplimiento pudiera tener en la seguridad de dicho sistema de información.

Respecto a la posible agrupación de hallazgos, se tendrá en cuenta lo siguiente:

- Será posible agrupar varias No Conformidades menores en una sola no conformidad menor, si dichos hallazgos están referidos a una única medida.
- Cuando las no conformidades menores estén referidas a varias medidas dentro de un mismo grupo de medidas (por ejemplo: [op.pl.*], [op.acc.*], [op.exp.*], [mp.if.*], [mp.eq.*], etc.), su posible agrupación estará calificada como no conformidad mayor.
- No podrán agruparse no conformidades menores que se refieran a distintos grupos de medidas, como tampoco podrán agruparse no conformidades mayores.

Reunión final

Se debe realizar una reunión final con el cliente con el objetivo de presentar las conclusiones de la auditoria, incluyendo las recomendaciones relativas a la certificación.

6.- INFORME DE AUDITORIA

Al finalizar la auditoria, el equipo auditor se reúne y el auditor jefe elabora el informe de auditoría en un formato establecido y lo entregará al cliente en formato electrónico y con firma digital del equipo auditor.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas exigidas por el RD 311/2022. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados.

Atendiendo a la categoría del sistema auditado (BÁSICA, MEDIA o ALTA) el informe de auditoría se basará en el cumplimiento alcanzado de lo prescrito en el ENS y en concreto en las medidas de seguridad del Anexo II que resulten de aplicación, así como de aquellos requisitos específicos que pudieran documentarse en guías CCN-STIC en función del contexto interno o externo del sistema de información, identificando, en su caso, los hallazgos de conformidad, no conformidad y observaciones que se detecten, así como los registros, declaraciones de hechos o cualquier otra información pertinente y verificable en que se basen las conclusiones alcanzadas.

En base al resultado el auditor jefe incluye en el informe una recomendación que puede ser:

- El certificado puede ser concedido o renovado: en el caso de no detectarse ninguna no conformidad mayor o menor
- El certificado puede ser concedido o renovado tras el envío en plazo de un plan de acciones adecuado, ya que se han detectado no conformidades mayores y/o menores.
- Se estima que el certificado no podrá ser concedido o renovado ya que se detecta un número significativo de no conformidades cuya resolución no puede evidenciarse a través de un plan de acciones y por ello se requerirá de una auditoría extraordinaria.

7.- PLAZOS Y VALORACIÓN DEL PLAN DE ACCION (PAC)

Contenido del PAC

Para cada incumplimiento, la organización deberá presentar un plan de acciones correctivas (PAC) que incluya como mínimo para cada incumplimiento:

- Identificación de la no conformidad
- Análisis profundo de las causas que a juicio de la organización han motivado la no conformidad
- Si es aplicable, acciones de reparación que anule o minimice los efectos del incumplimiento, indicando plazos y responsables.
- Acciones correctivas dirigidas a eliminar o minimizar las causas identificadas para evitar su reaparición, indicando plazos y responsables.
- Acciones de seguimiento de las acciones de reparación y las correctivas.
- Definición de un método, plazo y responsable para la verificación de la eficacia de las acciones correctivas de manera que la organización se asegure que las causas que han motivado el incumplimiento han desaparecido.
- Evidencias de la ejecución de las acciones de reparación y de las acciones correctivas.

Deberá presentarlo en el formato que su sistema establezca para el registro de las no conformidades y acciones correctivas.

Plazo:

- La organización cliente dispone de 1 mes para presentar el plan de acciones a contar desde la fecha de envío del informe de auditoría por parte del equipo auditor.
- Este plazo puede ser menor en los casos de las auditorias no iniciales.
- Este plazo máximo incluye las posibles peticiones de ampliación de documentación que pueda hacer el auditor jefe.
- Si el plazo de implantación de las acciones correctivas fuera superior a 1 mes, la organización deberá aportar evidencias de acciones de remedio o contención suficientes hasta que las acciones correctivas se implanten. En cualquier caso, el PAC debe contener una planificación concreta de las acciones correctivas precisas que, en el tiempo adecuado y razonable en función de las no conformidades detectadas y su tipificación, traten y resuelvan las causas de los problemas detectados.
- Una vez superado el plazo máximo, el auditor jefe deberá enviar a ADOK el expediente completo incluyendo una recomendación de certificación.

Responsable:

El auditor jefe evalúa el PAC. En los casos en los que la valoración requiera de conocimientos específicos que el auditor jefe no tiene, este contará con el apoyo del equipo auditor que ha participado en la auditoria.

Si considera que el PAC no es incorrecto o es incompleto o insuficiente, pedirá a la organización auditada las ampliaciones oportunas.

Recomendación del auditor jefe

Una vez evaluado el PAC o transcurrido el plazo máximo el auditor jefe emite una recomendación (favorable / desfavorable) en un formato establecido.

En el caso de recomendación desfavorable, el auditor jefe deberá explicar con detalle los motivos y la recomendación de los pasos a seguir, entre los cuales, podemos encontrar:

- la no recomendación dando por finalizado el proceso.
- Recomendación de realización de auditoria extraordinaria para la valoración de las acciones correctivas. En ese caso, el auditor jefe debe detallar qué aspectos deben ser evaluados en esa auditoría y por qué.

Auditoría extraordinaria de verificación de acciones correctivas (AVAC)

El objetivo de esta auditoría es la verificación in situ de la implantación efectiva de todo o parte del PAC derivado de una auditoria ordinaria. La AVAC es una extensión de la auditoría ordinaria, un método de obtener evidencias suficientes de la implantación efectiva de las acciones.

Para poder hacer la recomendación y decisión, el auditor jefe previamente debe haber evaluado el PAC enviado por la organización y haberlo considerado válido, ya que el objetivo de la AVAC es verificar la implantación efectiva del PAC.

Deberá ser realizada en un plazo máximo de 6 meses desde la emisión del informe de la auditoría anterior.

8.- REVISIÓN Y DECISIÓN DE LA CERTIFICACIÓN

Revisión

Una vez emitida la recomendación por el auditor jefe, todos los expedientes pasan a un proceso de revisión previo a la decisión sobre la certificación.

La revisión es realizada por un revisor técnico cualificado como tal para el ENS, según el perfil definido, y que no haya participado en el proceso de auditoría, con el fin de garantizar la imparcialidad.

El revisor o revisores realiza una revisión completa del expediente desde la fase comercial (solicitud de oferta, evaluación técnica de oferta, contrato) hasta la programación, la ejecución de la auditoría y la valoración del PAC. También deberá valorar que se salvaguarda la imparcialidad en el proceso o que se han valorado las reclamaciones de terceras partes, en caso de haberlas.

El objetivo es garantizar que todo el proceso se ha realizado siguiendo los requisitos de acreditación y, por tanto, se puede adoptar una decisión (favorable o desfavorable) informada, justificada y justa.

El revisor registra sus conclusiones y la recomendación de las acciones a realizar, que pueden ser:

- Decisión favorable a la certificación sin requerir acciones adicionales
- Solicitud de documentación adicional al cliente: modificaciones o ampliaciones en el plan de acciones o evidencias enviadas, u otro tipo de documentación.
- Solicitud de documentación adicional al equipo auditor o a ADOK: modificaciones o ampliaciones de registros o aclaraciones a los registros presentados.
- Realización de auditoría de verificación de acciones correctoras (AVAC): En ese caso, indicará claramente los conceptos a revisar y las recomendaciones (tiempo de dedicación, etc.) para su realización, tal y como se ha explicado con anterioridad.
- Otras: explicará con detalle

9.- COMUNICACIÓN DE LA DECISIÓN Y EMISIÓN DEL CERTIFICADO

La decisión adoptada se comunica a la organización por escrito. En caso favorable, se emite un certificado.

El certificado tiene una validez de 2 años y es emitido en castellano. Si la organización lo solicitara también en alguna de las lenguas cooficiales, se emitirá un certificado bilingüe (castellano y la otra lengua solicitada), utilizando el mismo formato en un único documento con igual tipo de letra y rango.

Junto con el certificado tendrá derecho a usar los distintivos de conformidad establecidos por el CCN siguiendo las directrices definidas en el documento "CCN-STIC-809 Declaración y certificación de la conformidad con el ENS".

10.- COMUNICACIÓN AL CCN

Una vez emitido el certificado, ADOK lo comunicará al Centro Criptológico Nacional dentro de los quince días siguientes a la expedición a través de la solución AMPARO (o la que CCN pueda establecer).

Cualquier cambio en el certificado emitido (modificación, suspensión, retirada), también se comunicarán al CCN usando la misma vía.

Así mismo, ADOK comunicará al CCN la información sobre los hallazgos detectados (no conformidades mayores, no conformidades menores y observaciones) y su ubicación, ya sea en los artículos del ENS o en las medidas de su Anexo II.

11.- APROBACIÓN PROVISIONAL DE CONFORMIDAD (APC)

El CCN podrá expedir excepcionalmente una Aprobación Provisional de Conformidad (APC) si se concurren simultáneamente los siguientes requisitos:

- Certificación inicial ENS
- El Plan de Acciones Correctivas, por razones adecuadas y razonables, requiere un período de ejecución superior a tres (3) meses.
- No se han detectado No Conformidades Mayores en la auditoría de certificación inicial
- El sistema de información es de categorías BÁSICA o MEDIA.

Esta APC tendrá una vigencia de seis (6) meses, que podrá ser ampliado por otros seis (6) meses, cuando concurran circunstancias de seguridad que así lo aconsejen.

Para ello, ADOK, una vez verificado que se cumplen las condiciones anteriores, trasladará la petición de emisión de la APC al CCN.

La organización debe subsanar las no conformidades menores durante el período de validez de la APC. El equipo auditor valorará el plan de acciones correctivas y evidencias recibidos, indicando si se considera satisfactorio o no, en el propio informe de recomendación, justificando dicha decisión.

En caso de que se subsanen adecuadamente, se expedirá el Certificado de Conformidad en el ENS, según lo indicado anteriormente.

Sin embargo, si no se subsanan, ADOK se lo comunicará al CCN para que se retire la APC concedida. En caso de querer optar a la certificación, deberá iniciar un proceso nuevo.

12.- ACTIVIDADES DE VIGILANCIA

Una vez concedida la certificación y con carácter al menos semestral, ADOK realizará vigilancia del cumplimiento del uso de la marca (distintivos de conformidad) por parte de la organización certificada. Se verificará que el uso de la certificación y distintivos de conformidad con el ENS es adecuado y cumple con lo indicado en la guía CCN-STIC-809.

En caso de detectar algún uso incorrecto, tanto de la organización certificada como de un proveedor de ésta, se contactará por escrito con la misma para su inmediata corrección, concediéndole un plazo máximo de 1 mes. En caso de no resolverse satisfactoriamente o en tiempo, se informará al CCN al respecto.

En el documento ENS-FR06 se registrarán todas las actividades de vigilancia, junto el resultado, las acciones y la conclusión adoptada al respecto por ADOK y/o por el CCN.

13.- AUDITORIA NUEVA COMPLETA ORDINARIA

Es imprescindible realizar una auditoría completa ordinaria cada 2 años.

Con antelación suficiente, la responsable de programación y/o dirección de producto contacta con la organización para informarle de la necesidad de realizar la auditoría, recabar información de posibles cambios, etc.

El proceso de programación y realización de auditoría sigue la sistemática anteriormente definida con la siguiente particularidad:

- Si en una auditoría ordinaria se detectan no conformidades mayores, durante el período de resolución de las no conformidades mayores, el certificado quedará suspendido. En caso de no cerrar las no conformidades mayores en un plazo máximo de seis meses el certificado se cancelará. La organización auditada deberá dejar de hacer uso de la marca durante el periodo de suspensión.

14.- VALORACIÓN DE CAMBIOS SIGNIFICATIVOS

Durante el periodo de 2 años entre 2 auditorías, el sistema de información de una organización puede sufrir cambios significativos con respecto a lo que está certificado. La organización certificada tiene la obligación de informar a ADOK por escrito puntualmente de cualquiera de estos cambios. La no realización de esta comunicación puede conllevar la retirada del certificado.

Pueden ser cambios significativos:

- Ampliación o reducción del alcance identificado en el certificado (actividades, servicios o proceso aplicables al ENS)
- Ampliación o reducción de los controles
- Cambio de categoría del sistema
- Ampliación o cambios en los centros de trabajo incluidos en la certificación

ADOK realiza una valoración de dichos cambios, debiendo decidir las acciones a adoptar. Para ello, tiene en cuenta la trascendencia y envergadura de los cambios y el momento del ciclo que se encuentra (cercanía a la auditoría completa ordinaria bienal). La decisión puede ser:

- Realizar una auditoría extraordinaria para valorar la correcta implantación de los cambios.
- Adelantar la auditoria de completa ordinaria bienal, realizando por tanto una auditoría completa. En este caso, se emite un nuevo certificado con una validez de 2 años más.

15.- TRANSFERENCIA DE CERTIFICADOS

Si una organización está certificada con otra entidad acreditada y solicita la transferencia de su certificado, se le requerirá copia de dicho certificado en vigor y toda la documentación relativa a la última auditoria. Se verificará en la página web del CCN el estado del certificado. Con dicha información se programará la auditoria completa ordinaria en la fecha que le corresponda.

En caso de que no aporte dicha documentación o no fuera correcta, se realizará un proceso de certificación inicial.

16.- SUSPENSIÓN Y RETIRADA DE LA CERTIFICACIÓN

- La suspensión del certificado implica que, mientras dure la misma, no puede hacer uso de su condición de certificado ni usar, por tanto, las marcas y logotipos de certificación.

- La suspensión queda anulada cuando se puede verificar que los motivos que motivaron la suspensión ya no existen y el problema ha sido solucionado
- Al anular la suspensión, la organización recobra su condición de certificado y, con ella, todos sus derechos. A partir de ese momento el ciclo y las fechas de auditorías previstas son las mismas que antes de la suspensión
- El periodo de suspensión se decide en cada caso siendo el máximo de 6 meses
- La comunicación de la suspensión a la organización certificada, así como su revocación se realiza por los medios descritos anteriormente en este mismo procedimiento.
- Básicamente, se podrá suspender temporalmente la certificación ENS por los siguientes motivos:
    - Por detectarse no conformidades mayores en el transcurso de una auditoría completa ordinaria, no inicial.
    - Derivadas de actividades de vigilancia por un uso no adecuado de la certificación y distintivos de conformidad.
    - Por solicitud voluntaria de la empresa certificada, quien también podrá finalizar la certificación directamente

En caso de no solucionarse en el plazo indicado los problemas que han motivado la suspensión, se procederá a la cancelación del certificado, lo que implica la pérdida de todos los derechos como organización certificada, debiendo comenzar un nuevo proceso de certificación inicial en caso de querer certificarse. La cancelación del certificado se comunicará por escrito tal y como se ha descrito anteriormente.

15.- CAMBIOS QUE AFECTAN A LA CERTIFICACIÓN

En caso de modificaciones del Esquema Nacional de Seguridad (nuevos requisitos, revisión de los requisitos) o de los requisitos de acreditación que afecten a las organizaciones certificadas, ADOK analizará dichos cambios y comunicará por escrito la implicación de los mismos a las organizaciones certificadas.

16.- APELACIONES, QUEJAS Y RECLAMACIONES, DENUNCIAS O RECLAMACIONES DE TERCERA PARTE

ADOK dispone de los medios necesarios para recibir, canalizar y tratar las reclamaciones, apelaciones y recursos recibidos. A continuación, se resume la sistemática de gestión en función de la naturaleza de la misma.

Con carácter general, cualquier persona u organización involucrada en alguno de los procesos a continuación descritos, en caso de no estar de acuerdo con las decisiones adoptadas, podrá dirigirse a la entidad de acreditación o los organismos que considere oportuno.

Recusación del personal que participa en el proceso de certificación

Si durante el proceso de certificación, dentro de la sistemática establecida en los planes de auditoría, el cliente hace uso de su derecho a recusar al equipo auditor, ADOK analizará los motivos de dicha recusación. Si los motivos son fundados y la recusación es asumible, se cambia el equipo auditor. En caso contrario, se informa a la organización de que la modificación no procede, pudiendo esta seguir con el proceso o anular la ejecución del servicio, según lo definido en las condiciones contractuales.

Apelaciones a la decisión de certificación

Las organizaciones certificadas o en proceso de certificación tienen el derecho de apelar a las decisiones de certificación adoptadas por ADOK. En tal caso, deben presentar formalmente y por escrito la apelación a ADOK, quien asigna su evaluación a una o varias personas técnicamente

competentes y que no hayan intervenido en el proceso de certificación. Se emite una decisión que es avalada por dirección técnica y dirigida al apelante.

En caso de que el apelante no esté de acuerdo con la decisión, ADOK nombra un árbitro externo. El apelante puede presentar formalmente su apelación ante el árbitro, quien evalúa la apelación y emite una decisión, que es remitida al apelante. Con esta decisión ADOK comunica al apelante que el proceso ha terminado.

Reclamaciones de terceras partes

Se entiende por reclamación de tercera parte las quejas o reclamaciones recibidas en ADOK en relación con los productos, procesos o servicios amparados por el sistema certificado.

Las reclamaciones de terceras partes deberán ser realizadas por escrito. ADOK realiza acuse de recibo de la misma y realiza el siguiente análisis con el fin de decidir si la reclamación se admite y se puede gestionar:

- se asegura que la organización contra la que se realiza la reclamación dispone de un certificado en vigor
- se asegura que la actividad que ha originado la reclamación está cubierta por el sistema de gestión y el alcance certificado.
- se dispone de documentación y evidencias suficientes.

Con ello, adopta una decisión e informa al reclamante si se admite o no, aportando los motivos en tal caso. En caso de duda, y, en cualquier caso, para poder continuar con la gestión de la reclamación, solicita más información o aclaraciones.

En caso de considerar que se debe realizar una investigación de la reclamación, ADOK recopila y analiza toda la información A la vista de toda la información, en función de la gravedad de la reclamación y de la proximidad de auditorías a la organización certificada, se deciden los siguientes pasos a dar, que pueden ser:

- Investigar la reclamación durante la siguiente auditoría.
- Realizar una investigación mediante una auditoría extraordinaria dirigida a investigar el hecho en concreto. En esos casos se realiza una auditoría de notificación a corto plazo.
- Analizar la reclamación documentalmente. Posteriormente, se puede requerir la realización de una auditoría.

Finalmente se adopta una decisión y en consecuencia de ella unas acciones a realizar. En la decisión se tiene en cuenta la gravedad de la reclamación y sus consecuencias, las posibilidades de repetición, la responsabilidad y el historial de reclamaciones.

El resultado de la investigación y la decisión deben ser comunicados a la organización certificada y al reclamante.

En cualquier caso, en la siguiente auditoría, se debe investigar el estado de cierre de las no conformidades y acciones derivadas de la reclamación, con el fin de ver la eficacia continuada y corroborar si las causas que motivaron la reclamación han sido eliminadas o minimizadas

Reclamaciones de clientes sobre el servicio ofrecido por ADOK

Las reclamaciones deberán ser comunicadas a ADOK por escrito, quien las evaluará analizando las causas y adoptando si procede, acciones tanto reparadoras como correctivas. ADOK comunicará siempre al reclamante las decisiones adoptadas y los avances en la gestión de la reclamación.