NÚMERO DE EXPEDIENTE: 2022-0941
ID DE CLASIFICACIÓN: 3.2.3

Marco de confianza

para la identificación electrónica sueca (eID)

Versión de 4 de octubre de 2022

1. Antecedentes y finalidad

El marco de confianza para la identificación electrónica sueca tiene como objetivo establecer requisitos comunes para los emisores de identificaciones electrónicas revisadas y aprobadas por la Agencia para la Administración Digital de Suecia (DIGG, por su versión en sueco). Los requisitos se dividen en diferentes niveles de protección, conocidos como niveles de seguridad, que corresponden a diferentes grados de seguridad técnica y operativa por parte del emisor y diferentes grados de verificación de que la persona a la que se expide un documento de identificación electrónica es realmente quien dice ser.

Los requisitos de este marco de confianza se aplican a los niveles de seguridad 2 a 4, correspondiendo el nivel 4 al nivel más alto de protección.

El cumplimiento se interpretará de la siguiente manera:

(a) cuando no se especifique el nivel de seguridad, el requisito deberá cumplirse en todos los niveles; y

(b) cuando se especifique el nivel de seguridad, se garantizará el cumplimiento al menos en el nivel pertinente.

No se tendrán en cuenta los requisitos establecidos para un nivel inferior al pertinente.

2. Organización y gobernanza

Requisitos operativos generales

K2.1 Los emisores de identificaciones electrónicas (eID, por su versión en inglés) suecas que no sean organismos públicos operarán como entidades jurídicas registradas y suscribirán y mantendrán el seguro requerido para la empresa.

K2.2 Los emisores de identificaciones electrónicas suecas deberán tener una empresa establecida, ser plenamente operativos en todas las partes especificadas en este documento y estar bien versados en los requisitos legales que se les imponen como emisores de identificaciones electrónicas suecas.

K2.3 Los emisores de identificaciones electrónicas suecas deberán tener la capacidad de asumir el riesgo de responsabilidad por daños y poseer recursos financieros suficientes para llevar a cabo sus operaciones durante al menos un año.

Seguridad de la información

K2.4 Los emisores de identificaciones electrónicas suecas deberán haber establecido un sistema de gestión de la seguridad de la información para las partes de sus actividades afectadas por el marco de confianza, que se base, cuando proceda, en la norma ISO/IEC 27001 o principios equivalentes para la gestión y el control del trabajo de seguridad de la información, incluidos los siguientes:

(a) todos los procesos administrativos y técnicos críticos para la seguridad deberán documentarse y basarse en una base formal, donde las funciones, responsabilidades y poderes estén claramente definidos;

(b) los emisores de identificaciones electrónicas suecas se asegurarán de que disponen en todo momento de recursos humanos suficientes para cumplir sus obligaciones;

(c) los emisores de identificaciones electrónicas suecas establecerán un proceso de gestión de riesgos que, de manera adecuada, de forma continua o al menos cada doce meses, analice las amenazas y vulnerabilidades en la empresa y que, mediante la introducción de medidas de seguridad, equilibre los riesgos a niveles aceptables;

(d) los emisores de identificaciones electrónicas suecas establecerán un proceso de gestión de incidentes que garantice sistemáticamente la calidad del servicio, las formas de notificación posterior, y que se tomen las medidas reactivas y preventivas adecuadas para mitigar o prevenir los daños resultantes de tales eventos;

(e) los emisores de identificaciones electrónicas suecas establecerán y probarán periódicamente un plan de continuidad que cumpla los requisitos de accesibilidad de la empresa mediante la capacidad de restablecer procesos críticos en caso de crisis o incidentes graves;

(f) los emisores de identificaciones electrónicas suecas evaluarán periódicamente el trabajo de seguridad de la información e introducirán medidas de mejora en el sistema de gestión.

K2.5 Alcance y madurez del sistema de gestión:

Nivel 4: El sistema de gestión de la seguridad de la información cumplirá la norma SS-ISO/IEC 27001:2017 o versiones posteriores o internacionales equivalentes de la norma y, dentro del ámbito de aplicación de esta, incluirá todos los requisitos impuestos a los emisores de identificaciones electrónicas suecas.

Condiciones de subcontratación

K2.6 El emisor de identificaciones electrónicas suecas que haya externalizado la ejecución de uno o más procesos críticos para la seguridad a otra parte definirá mediante contrato de qué procesos críticos es responsable el subcontratista y qué requisitos son aplicables a estos, y aclarará la relación contractual en la declaración del emisor.

Trazabilidad, supresión y almacenamiento de documentos

K2.7 Los emisores de identificaciones electrónicas suecas almacenarán:

(a) documentos de solicitud y documentos relativos a la expedición, recepción o bloqueo de identificaciones electrónicas;

(b) contratos, documentos de política y declaraciones del emisor; y

(c) historial de tratamiento y otra documentación necesaria para demostrar el cumplimiento de los requisitos impuestos a los emisores de identificaciones electrónicas suecas y que permita un seguimiento que demuestre que los procesos y controles críticos para la seguridad están implantados y son eficaces.

K2.8 El período de almacenamiento no será inferior a cinco años y el material podrá ser producido de forma legible durante todo este período, a menos que sea necesario un requisito de eliminación desde el punto de vista de la intimidad y esté respaldado por la ley u otra normativa.

Examen y seguimiento

K2.9 Los emisores de identificaciones electrónicas suecas establecerán una función de auditoría interna que revise periódicamente las actividades de emisión. El auditor interno será independiente en el ejercicio de sus funciones de manera que se garantice una revisión objetiva e imparcial y tendrá la competencia y la experiencia necesarias para el ejercicio de sus funciones. El auditor interno planificará de forma independiente la realización de la auditoría y la documentará en un plan de auditoría que abarque un período de tres años. Los elementos de auditoría se seleccionarán sobre la base de un análisis de riesgos y materialidad y se basarán en las descripciones de las operaciones presentadas por el emisor a la Agencia para la Administración Digital de Suecia.

Niveles 3 y 4: La auditoría interna se llevará a cabo sobre la base de normas de auditoría aceptadas.

3. Seguridad física, administrativa y orientada a las personas

K3.1 Las partes centrales de la operación estarán protegidas físicamente contra daños causados por acontecimientos medioambientales, accesos no autorizados u otras perturbaciones externas. El control de acceso se aplicará de manera que el acceso a las zonas sensibles se limite al personal autorizado, los soportes portadores de información se almacenen y eliminen de forma segura, y el acceso a estas zonas protegidas se supervise continuamente.

K3.2 Antes de que una persona asuma cualquiera de las funciones identificadas de conformidad con el apartado K2.4, letra a), y que sean de particular importancia para la seguridad, el emisor de identificaciones electrónicas suecas deberá haber llevado a cabo verificaciones de antecedentes para garantizar que la persona pueda considerarse confiable y que la persona tenga las calificaciones y la capacitación requeridas para realizar de manera segura las tareas resultantes de la función.

K3.3 Los emisores dispondrán de procedimientos para garantizar que solo el personal específicamente autorizado tenga acceso a los datos recogidos y conservados de conformidad con el apartado K2.7.

K3.4 **Niveles 3 y 4:** Los emisores garantizarán a lo largo de toda la cadena del proceso de expedición que la separación de funciones se aplique de tal manera que ninguna persona pueda obtener una identificación electrónica en nombre de otra persona.

4. Seguridad técnica

K4.1 Los emisores de identificaciones electrónicas suecas velarán por que los controles técnicos establecidos sean suficientes para alcanzar el nivel de protección que se considere necesario con respecto a la naturaleza, el alcance y otras circunstancias de la empresa, y por que dichos controles funcionen y sean eficaces.

K4.2 Los medios electrónicos de comunicación utilizados en la transmisión de datos sensibles estarán protegidos contra la interceptación, manipulación y repetición.

K4.3 El elemento de encriptación sensible utilizado para expedir identificaciones electrónicas, identificar a los titulares y expedir certificados de identidad estará protegido de tal manera que:

(a) el acceso esté limitado, lógica y físicamente, a las funciones y aplicaciones que son estrictamente necesarias;

(b) el elemento de encriptación nunca se almacene en texto plano en soportes de almacenamiento persistentes;

(c) el elemento de encriptación esté protegido mediante el uso de un módulo de *hardware* criptográfico con mecanismos de seguridad activos que contrarresten los intentos físicos y lógicos de comprometer el elemento de encriptación;

(d) los mecanismos de seguridad para la protección del elemento de encriptación sean transparentes y se basen en normas reconocidas y bien establecidas; y

(e) **niveles 3 y 4:** los datos de activación para la protección del elemento de encriptación se gestionan a través del control multipersona.

K4.4 Los emisores dispondrán de procedimientos documentados para garantizar que el nivel de protección requerido en el entorno informático pertinente pueda mantenerse a lo largo del tiempo y en relación con los cambios, incluidas las evaluaciones periódicas de vulnerabilidad y la preparación adecuada para hacer frente a los cambios en los niveles de riesgo y los incidentes que se produzcan.

5. Solicitud, identificación y registro

Información sobre las condiciones

K5.1 Los emisores de identificaciones electrónicas suecas proporcionarán información sobre contratos, términos y condiciones, así como información relacionada y cualquier restricción en el uso del servicio, a usuarios conectados, proveedores de servicios electrónicos y otras personas que puedan confiar en el servicio del emisor.

K5.2 El emisor de identificaciones electrónicas suecas deberá referirse claramente a los términos y las condiciones y diseñar los procedimientos para que los términos y las condiciones se faciliten al solicitante en el proceso de emisión.

K5.3 Los emisores de identificaciones electrónicas suecas deberán presentar una declaración del emisor que incluya:

(a) la identidad y los datos de contacto del emisor;

(b) breves descripciones de los servicios y las soluciones prestados por el emisor, incluidos los métodos aplicados para la solicitud, la emisión y el bloqueo;

(c) condiciones asociadas con el servicio prestado, incluidas las obligaciones del usuario de proteger su identificación electrónica, las obligaciones y responsabilidades del emisor, las garantías dadas y la disponibilidad prometida;

(d) información sobre el tratamiento de datos personales y la forma en que se lleva a cabo; y

(e) disposiciones para modificar los términos u otras condiciones del servicio prestado, incluidas las medidas que deben adoptarse para interrumpir el servicio de manera controlada.

K5.4 **Niveles 3 y 4:** A petición de la Agencia para la Administración Digital de Suecia (DIGG) u otra parte contratante que dependa de los servicios prestados por el emisor, los emisores de identificaciones electrónicas suecas facilitarán información sobre la propiedad y la gestión de la empresa.

K5.5 El emisor de identificaciones electrónicas suecas que cese en sus actividades deberá seguir un plan preestablecido para interrumpir el servicio. El plan incluirá informar a todos los usuarios del servicio y a la Agencia para la Administración Digital de Suecia. El emisor mantendrá además disponible el material archivado de conformidad con los apartados K2.7 y K2.8 después de la interrupción.

Aplicación

K5.6 Una identificación electrónica sueca solo puede expedirse a petición del solicitante o mediante otro procedimiento de aceptación equivalente, y solo después de que el solicitante haya sido informado de las condiciones en las que se expide y de la responsabilidad que recaerá sobre él o ella.

No obstante, la expedición de una identificación electrónica que sustituya o complemente un documento de identificación electrónica válido o bloqueado recientemente, expedido previamente por el mismo emisor, podrá llevarse a cabo sin ningún procedimiento de solicitud previo.

K5.7 La solicitud de una identificación electrónica sueca estará vinculada a un número de identidad personal o un número de coordinación, así como a la información que de otro modo sería necesaria para que el emisor facilite dicha identificación electrónica.

Determinación de la identidad del solicitante

K5.8 Los emisores de identificaciones electrónicas suecas deberán verificar que la información vinculada a la solicitud es completa y corresponde a la información inscrita en un registro oficial.

K5.9 Cuando la información que deba comprobarse en un registro oficial esté marcada como confidencial («identidad protegida»), los controles necesarios podrán llevarse a cabo por otros medios equivalentes.

K5.10 Identificación del solicitante durante una visita presencial:

Los emisores de identificaciones electrónicas suecas podrán verificar la identidad del solicitante durante una visita presencial, de la misma manera que cuando expiden un documento de identidad normalizado.

K5.11 Identificación a distancia del solicitante en la relación existente:

Nivel 3: Los emisores de identificaciones electrónicas suecas que ya hayan identificado al solicitante en una relación que implique transacciones significativas desde el punto de vista económico o jurídico, y en la que el solicitante pueda ser identificado a distancia por otros medios fiables equivalentes a los requisitos de nivel 3 de la marca de calidad de la identificación electrónica sueca, podrán utilizar este método para establecer la identidad del solicitante.

Nivel 4: No se aplica.

K5.12 Identificación mediante la identificación electrónica sueca (eID):

Un emisor de identificaciones electrónicas suecas podrá identificar al solicitante a distancia mediante una identificación electrónica sueca válida existente de al menos el mismo nivel de seguridad que la que vaya a expedirse, si puede, sin obstáculos contractuales, utilizar dicha identificación como base para expedir una nueva identificación electrónica.

Nivel 4: El período de validez de la nueva identificación electrónica expedida se limitará a no extenderse más allá del período de validez de la identificación electrónica existente.

K5.13 Identificación a distancia del solicitante:

Nivel 2: Los emisores de identificaciones electrónicas suecas podrán utilizar grabaciones de imágenes fiables de un documento de identidad normalizado válido y de la imagen facial del solicitante como base para establecer la identidad del solicitante a distancia si la comparación no suscita dudas sobre la verdadera identidad del solicitante.

Nivel 3: Los emisores de identificaciones electrónicas suecas podrán, mediante una lectura segura de un documento de identidad normalizado válido que contenga datos biométricos almacenados electrónicamente, establecer la identidad del solicitante a distancia sobre la base de dichos datos si los datos biométricos correspondientes de la persona que debe identificarse pueden recopilarse de manera suficientemente segura para que pueda realizarse una comparación con una fiabilidad equivalente a la de una visita presencial, y cuando la comparación no suscite dudas sobre la verdadera identidad del solicitante.

Nivel 4: No se aplica.

Registro

K5.14 Los emisores de identificaciones electrónicas suecas, teniendo en cuenta las normas aplicables en materia de protección de datos personales, mantendrán un registro de usuarios conectados y los documentos de identificación electrónica asignados, y mantendrán dicho registro actualizado.

6. Emisión y bloqueo de la identificación electrónica (eID)

Diseño de medios técnicos

K6.1 Medios técnicos:

Niveles 2 y 3: Los medios técnicos para la identificación electrónica a través de la identificación electrónica con la marca de calidad de la identificación electrónica sueca se diseñarán de acuerdo con un principio de dos factores, según el cual una parte consiste en información almacenada electrónicamente que el usuario conservará y la otra parte consiste en lo que el usuario utilizará para activar la identificación electrónica.

Nivel 4: Los medios técnicos para la identificación electrónica a través de la identificación electrónica con la marca de calidad de la identificación electrónica sueca se diseñarán de acuerdo con un principio de dos factores, según el cual una parte consiste en un módulo de seguridad personal que el usuario deberá poseer y la otra parte consiste en lo que el usuario deberá utilizar para activar el módulo de seguridad.

K6.2 El mecanismo de activación y el código personalizado se diseñarán de tal manera que sea poco probable que terceros infrinjan la protección, incluso por medios mecánicos.

Niveles 3 y 4: La protección incluirá mecanismos para evitar la copia y manipulación del documento de identificación electrónica.

K6.3 Los usuarios de la identificación electrónica con la marca de calidad de la identificación electrónica sueca podrán, por iniciativa propia, dentro del período de validez de la identificación electrónica, de forma gratuita y sin inconvenientes significativos, intercambiar o solicitar un nuevo código personal y, mediante orientación o producción automática, recibir ayuda para mantener los requisitos del apartado K6.2.

Si la identificación electrónica está diseñada de tal manera que no pueda intercambiarse un código personalizado, el usuario deberá, en las mismas condiciones, poder obtener rápidamente una nueva identificación electrónica con un nuevo código personalizado que reemplace al anterior a través de un procedimiento de bloqueo.

K6.4 Los emisores de identificaciones electrónicas suecas velarán por que los datos registrados para la identificación electrónica de los titulares representen de forma única al solicitante y se atribuyan a la persona en cuestión al expedir el documento de identificación electrónica.

K6.5 El período de validez de las identificaciones electrónicas expedidas se limitará teniendo en cuenta las características de seguridad del documento de identificación electrónica y los riesgos de uso indebido. El período máximo de validez de la identificación electrónica será de cinco años.

Prestación de un documento de identificación electrónica (eID)

K6.6 Prestación a distancia:

Nivel 2: El emisor de la identificación electrónica sueca facilitará el documento de e-ID de manera que confirme los datos de contacto conservados en el registro oficial o la información registrada en relación con el procedimiento electrónico con arreglo al nivel 2 del apartado K5.13.

Nivel 3: El emisor de identificaciones electrónicas suecas que proporcione una identificación electrónica mediante un procedimiento electrónico conforme a los apartados K5.11 3, K5.12 3 o K5.13 3 se asegurará, en el caso de una nueva emisión, por separado e independientemente de la provisión en términos de seguridad, de que se informe al usuario de que dicho documento de e-ID ha sido entregado o, mediante otras medidas, se garantice un grado equivalente de control para que la persona sea alertada del riesgo de robo de identidad en relación con la provisión.

Nivel 4: El emisor de identificaciones electrónicas suecas que proporcione una identificación electrónica a través de un procedimiento electrónico conforme al nivel 4 del apartado K5.12 se asegurará, en el caso de una nueva emisión, por separado e independientemente de la provisión en términos de seguridad, de que se informe al usuario de que se ha entregado dicho documento de identificación electrónica.

K6.7 Prestación durante una visita presencial:

Durante una visita presencial y tras un control de identidad de conformidad con el apartado K5.10, el emisor de la identificación electrónica sueca facilitará el documento de identificación electrónica contra recibo firmado, así como la parte que el usuario utilizará para activar la identificación electrónica por separado e independientemente de la presentación del documento de identificación electrónica en términos de seguridad, sobre la base de los datos de contacto conservados en un registro oficial u otra información de credibilidad equivalente.

Servicio de bloqueo

K6.8 Los emisores de identificaciones electrónicas suecas proporcionarán un servicio de bloqueo con buena accesibilidad para que el usuario pueda bloquear su identificación electrónica.

K6.9 Los emisores de identificaciones electrónicas suecas tramitarán de forma rápida y segura las solicitudes de bloqueo y adoptarán medidas para evitar el uso indebido sistemático del servicio de bloqueo u otras acciones intencionadas que den lugar al bloqueo generalizado de los documentos de identificación electrónica, garantizando que las identificaciones electrónicas de los usuarios estén disponibles cuando sea necesario

7. Verificación de las identidades electrónicas de los titulares

K7.1 Los emisores de identificaciones electrónicas suecas velarán por que, al verificar la identidad del titular, se lleven a cabo controles fiables de la autenticidad y validez del documento de identificación electrónica.

K7.2 Los emisores de identificaciones electrónicas suecas se asegurarán de que se hayan implementado controles técnicos de seguridad al verificar la identidad electrónica de los titulares, de modo que sea poco probable que terceros, a través de adivinanzas, escuchas, reproducciones o manipulaciones del proceso, puedan infringir los mecanismos de protección.

8. Expedición de certificados de identidad

Los emisores de identificaciones electrónicas suecas que presten un servicio de expedición de certificados de identidad a servicios electrónicos de confianza también cumplirán las disposiciones de la presente sección.

K8.1 Los emisores de identificaciones electrónicas suecas garantizarán que el servicio de expedición de certificados de identidad tenga una buena accesibilidad y que la expedición de certificados de identidad vaya precedida de una identificación fiable de conformidad con las disposiciones de la sección 7.

Nivel 4: Los certificados incluirán una referencia al elemento de encriptación que el emisor haya verificado que está en posesión exclusiva del titular.

K8.2 Los certificados de identidad presentados solo serán válidos durante el tiempo necesario para permitir al usuario el acceso al servicio electrónico solicitado, y estarán protegidos de modo que la información solo pueda ser leída por el destinatario previsto y que la autenticidad de los certificados pueda ser verificada por los destinatarios de los certificados.

K8.3 Los emisores de identificaciones electrónicas suecas, teniendo en cuenta los riesgos de uso indebido del servicio de certificación, limitarán el período de tiempo durante el cual pueden expedirse varios certificados de identidad consecutivos a un titular determinado antes de que el titular sea identificado de nuevo de conformidad con las disposiciones de la sección 7.