

## ÍNDICE

|                                     |          |
|-------------------------------------|----------|
| <b>1. OBJETIVO:</b> .....           | <b>2</b> |
| <b>2. ALCANCE:</b> .....            | <b>2</b> |
| <b>3. DEFINICIONES:</b> .....       | <b>2</b> |
| <b>4. DESARROLLO:</b> .....         | <b>3</b> |
| <b>5. ANEXO:</b> .....              | <b>8</b> |
| <b>6. CONTROL DE CAMBIOS:</b> ..... | <b>8</b> |
| <b>7. APROBACIÓN:</b> .....         | <b>9</b> |

|   |  |  |
|---|--|--|
|  | <b>INSTRUCTIVO</b>   | <b>ME-VAR-RPSC-IN-02</b><br>Versión 01 |
|   | <b>IDENTIFICACIÓN VIRTUAL PARA LA EMISIÓN DE CERTIFICADOS DIGITALES DE FIRMAS ELECTRÓNICAS AVANZADAS</b> | <b>Página 2 de 9</b>                   |

**1. OBJETIVO:**

Detalla las condiciones y requisitos mínimos aplicables a la verificación de la identidad de la persona solicitante para la emisión de un certificado digital de firma electrónica avanzada, mediante métodos de identificación virtual, que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, de conformidad ACUERDO GUBERNATIVO No. 110-2020, REFORMAS AL REGLAMENTO DE LA LEY PARA EL RECONOCIMIENTO DE LAS COMUNICACIONES Y FIRMAS ELECTRÓNICAS , ACUERDO GUBERNATIVO No. 135-2009.

**2. ALCANCE:**

Aplica a los Prestadores de Servicios de Certificación Autorizados, que opten por la modalidad de identificación virtual en la emisión de certificados digitales de firmas electrónicas avanzadas.

**3. DEFINICIONES:**

- 3.1. Fondo numismático:** Impresión de muchas líneas onduladas entrelazadas en un fondo uniforme, para ayudar a detectar si la impresión del texto variable ha sido alterada.
- 3.2. Fraude:** Suministro de declaraciones falsas a otra parte con el fin de obtener algo que no se habría proporcionado sin el engaño.
- 3.3. Identificación Virtual Asistida:** Proceso de verificación de la identidad de una persona a través de medios digitales, con el acompañamiento de un agente humano. Este tipo de identificación se utiliza para la creación de firma electrónica avanzada y otro tipo de trámites.
- 3.4. Identificación Virtual No Asistida:** Proceso de verificación de la identidad de una persona a través de medios digitales, sin el acompañamiento de un agente humano. Este tipo de identificación se utiliza para la creación de firma electrónica avanzada y otro tipo de trámites.
- 3.5. Imagen Fantasma:** Fotografía secundaria del titular del documento de identificación, impresa a colores atenuados contigua a la fotografía principal.
- 3.6. Micro Línea Offset:** Texto muy pequeño (150um) el cual puede ser leído únicamente con lentes de aumento y es imposible de reproducir con las técnicas estándares de impresión.
- 3.7. OCR:** Siglas en inglés correspondientes a “Optical Character Recognition” cuyo significado en español es “Reconocimiento óptico de caracteres”.
- 3.8. OTP:** Siglas en inglés correspondientes a “One Time Password”, cuyo significado en español es “Contraseña de un solo uso”.

|   |  |  |
|---|--|--|
|  | <b>INSTRUCTIVO</b>   | <b>ME-VAR-RPSC-IN-02</b><br>Versión 01 |
|   | <b>IDENTIFICACIÓN VIRTUAL PARA LA EMISIÓN DE CERTIFICADOS DIGITALES DE FIRMAS ELECTRÓNICAS AVANZADAS</b> | <b>Página 3 de 9</b>                   |

**3.9. PSC:** Siglas correspondientes a: Prestador de Servicios de Certificación.

**3.10. Suplantación de Identidad:** Uso no autorizado y malintencionado de los datos personales por parte de alguien con el fin de actuar en el nombre de otra persona.

**3.11. Código de la guía:** Consiste en la identificación alfanumérica que se debe consignar en la parte superior derecha de cada página de la guía técnica, relacionada con los órganos dependencias establecidas en la estructura orgánica interna del Ministerio, propietarias de las guías.

#### **4. DESARROLLO:**

##### **4.1. GENERALIDADES**

###### **4.1.1. Modalidades de la identificación virtual**

El proceso de identificación se podrá realizar de las siguientes formas:

4.1.1.1. Asistida, con la intervención sincrónica de un operador del prestador de servicios de certificación (operadores u operadores del prestador de servicios de certificación, indistintamente).

4.1.1.2. No asistida, con la intervención asincrónica del mencionado operador.

###### **4.1.2. Validez del proceso de identificación**

El proceso de identificación no se considerará válido cuando ocurra alguna de las circunstancias siguientes:

4.1.2.1. Existan indicios de falsedad o manipulación del documento de identificación.

4.1.2.2. La integridad física del documento este comprometida.

4.1.2.3. Existan indicios de uso de archivos pregrabados.

**Nota:** En cualquiera de los casos de identificación asistida y no asistida, el operador deberá basar su decisión de aprobación o denegación de la solicitud de emisión del certificado en la verificación de todas las evidencias recabadas en el proceso de identificación.

|   |  |  |
|---|--|--|
|  | <b>INSTRUCTIVO</b>   | <b>ME-VAR-RPSC-IN-02</b><br>Versión 01 |
|   | <b>IDENTIFICACIÓN VIRTUAL PARA LA EMISIÓN DE CERTIFICADOS DIGITALES DE FIRMAS ELECTRÓNICAS AVANZADAS</b> | <b>Página 4 de 9</b>                   |

## **4.2. EVALUACIÓN**

### **4.2.1. Evaluación de la conformidad**

- 4.2.1.1. El cumplimiento de los requisitos deberá ser confirmado por el Registro de Prestadores de Servicios de Certificación durante el proceso de auditoría.
- 4.2.1.2. El prestador de servicios de certificación deberá haber sido auditado, con carácter previo a ofrecer el servicio de identificación virtual al público.
- 4.2.1.3. El Registro de Prestadores de Servicios de Certificación podrá requerir al prestador, documentación e información adicional sobre cualquier aspecto de la solución de identificación virtual, con carácter previo o posterior a su implementación.

### **4.2.2. Requisitos generales de seguridad**

- 4.2.2.1. El prestador de servicios de certificación debe:
  - 4.2.2.1.1. Disponer y realizar análisis de riesgos específicos a la identificación virtual que se revisará al menos una vez al año, y en particular cuando se produzca un cambio en la prestación del servicio, que pudiera influir en el perfil de riesgo del procedimiento de identificación.
  - 4.2.2.1.2. Adoptar medidas técnicas y organizativas adicionales a las indicadas en este documento cuando el resultado del análisis de riesgos efectuado así lo requiera.
  - 4.2.2.1.3. Validar los datos de identidad, número de documento de identificación, fotografía del documento a través de servicios de consulta del Registro Nacional de las Personas RENAP; en caso el servicio de consulta no esté disponible, se deberá guardar el registro de por lo menos 3 intentos de la consulta efectuada y adjuntar evidencia de otros servicios de consulta con registros fiables.
  - 4.2.2.1.4. Evaluar y documentar las características de seguridad del conjunto del sistema, incluyendo todos los elementos sustantivos de la plataforma de identificación, los canales de comunicación y la generación y conservación de evidencias producidas durante el proceso de identificación.

|   |  |  |
|---|--|--|
|  | <b>INSTRUCTIVO</b>   | <b>ME-VAR-RPSC-IN-02</b><br>Versión 01 |
|   | <b>IDENTIFICACIÓN VIRTUAL PARA LA EMISIÓN DE CERTIFICADOS DIGITALES DE FIRMAS ELECTRÓNICAS AVANZADAS</b> | <b>Página 5 de 9</b>                   |

- 4.2.2.1.5. Notificar inmediatamente al Registro de Prestadores de Servicios de Certificación cualquier violación de la seguridad o pérdida de integridad que tenga impacto en el servicio.
- 4.2.2.1.6. Tomar medidas para reducir el riesgo de suplantación de identidad.
- 4.2.2.1.7. Basado en el grado de fiabilidad aportado por el sistema implementado y el correspondiente análisis de riesgos, deberá valorar el nivel de exposición a fallos y ataques que corresponda, estableciendo el procedimiento y criterios que debe seguir el operador para decidir sobre la aprobación de la solicitud de emisión del certificado.

#### **4.2.3. Requisitos del personal y plan de formación.**

El personal encargado de la verificación virtual de la identidad del solicitante de un certificado de firma electrónica avanzada debe:

- 4.2.3.1. Contar con formación específica sobre las características del método de identificación, sus procedimientos, métodos de prueba y métodos comunes de falsificación, con el fin de asegurar que dispone de la capacitación suficiente para detectar potenciales fraudes en el proceso de identificación.
- 4.2.3.2. Tener conocimiento sobre la legislación vigente en materia de servicios de certificación.
- 4.2.3.3. Evidenciar que existe una mejora continua en la formación relacionada a su perfil de puesto como mínimo una vez a año.

#### **4.2.4. Requisitos del proceso de identificación.**

- 4.2.4.1. La identidad del solicitante se acreditará únicamente mediante el Documento Personal de Identificación o pasaporte.
- 4.2.4.2. Informar al solicitante, de manera clara y comprensible, de los términos y condiciones del proceso de identificación virtual, así como de las recomendaciones de seguridad aplicables.
- 4.2.4.3. Requerir el consentimiento expreso del solicitante para la grabación del proceso de identificación y la recopilación de datos.
- 4.2.4.4. Si el proceso de identificación se realiza de forma asistida, el prestador dispondrá de un procedimiento para llevar a cabo la entrevista de identificación del solicitante del

|   |  |  |
|---|--|--|
|  | <b>INSTRUCTIVO</b>   | <b>ME-VAR-RPSC-IN-02</b><br>Versión 01 |
|   | <b>IDENTIFICACIÓN VIRTUAL PARA LA EMISIÓN DE CERTIFICADOS DIGITALES DE FIRMAS ELECTRÓNICAS AVANZADAS</b> | <b>Página 6 de 9</b>                   |

certificado y una guía de diálogo para los operadores, que incluya preguntas aleatorias y dinámicas.

4.2.4.5. Si el proceso de identificación se realiza de forma no asistida, el operador del prestador de servicios de certificación supervisará posteriormente el proceso de identificación y comprobará las evidencias e imágenes generadas por el sistema para aceptar o rechazar la validez del proceso de identificación.

4.2.4.6. Se enviará al solicitante un código único, aleatorio e impredecible, de un solo uso generado para el efecto. El código constará de un mínimo de 6 caracteres (OTP) o sistema de tecnología equivalente. El solicitante deberá introducirlo durante el proceso de identificación o de emisión del certificado digital.

4.2.4.7. Se tomarán las medidas adecuadas para detectar una posible manipulación de la imagen de video, del documento de identificación o del solicitante. Para ello se implementarán las medidas siguientes:

4.2.4.7.1. En el caso de la identificación virtual asistida: Medidas que evidencien la manipulación a través de la interacción con el documento de identificación utilizado y con el solicitante, según las indicaciones del operador, a través de interacciones y actuaciones físicas que figurarán en un protocolo que incluirá acciones tanto comunes como aleatorias y diferenciadas.

4.2.4.7.2. En el caso de la identificación virtual no asistida: El sistema requerirá al solicitante la realización activa de interacciones y actuaciones físicas.

4.2.4.8. Comprobación de los atributos de identificación de las calidades con que se acredita el solicitante, de acuerdo con las prácticas de certificación del prestador de servicios de certificación conforme la legislación aplicable.

#### **4.2.5. Requisitos de evidencias y de su conservación**

4.2.5.1. Se conservará una copia de la grabación en video de la información correspondiente a la identificación, y en particular el reconocimiento óptico de caracteres (OCR), Documento de identificación, prueba de vida y biometría facial.

4.2.5.2. Se conservarán fotos y toda la información del solicitante, incluyendo el documento de identificación utilizado en su anverso y reverso.

|   |  |  |
|---|--|--|
|  | <b>INSTRUCTIVO</b>   | <b>ME-VAR-RPSC-IN-02</b><br>Versión 01 |
|   | <b>IDENTIFICACIÓN VIRTUAL PARA LA EMISIÓN DE CERTIFICADOS DIGITALES DE FIRMAS ELECTRÓNICAS AVANZADAS</b> | <b>Página 7 de 9</b>                   |

4.2.5.3. La grabación en video y las imágenes obtenidas durante el procedimiento de identificación reunirán las condiciones de calidad y nitidez suficientes para garantizar su uso en investigaciones o análisis posteriores.

4.2.5.4. La evidencia deberá conservarse por un periodo mínimo de diez años.

#### **4.2.6. Requisitos mínimos de seguridad del sistema de identificación virtual**

4.2.6.1. La captura del video debe de realizarse en tiempo real.

4.2.6.2. Garantizar que se realiza desde un único dispositivo.

4.2.6.3. Comprobación del documento de identificación con el solicitante:

4.2.6.3.1. Si es asistido, el sistema permitirá al operador comparar las características biométricas del solicitante y la equivalencia de la información incluida en el documento de identificación con la foto del solicitante.

4.2.6.3.2. Si es no asistido, el sistema biométrico deberá realizar una comparación entre la imagen capturada y el documento de identidad, proveyendo automáticamente una puntuación sobre el grado de similitud entre los mismos.

#### **4.2.7. Prueba de vida**

4.2.7.1. Si es asistido, el sistema permitirá al operador comprobar que la persona está viva utilizando un procedimiento para llevar a cabo la entrevista de identificación del solicitante del certificado y una guía de diálogo para los operadores, que incluya preguntas aleatorias y dinámicas.

4.2.7.2. Si es no asistido, la solución debe establecer medidas técnicas para detectar que la persona está viva a través de los movimientos de los rasgos faciales y el movimiento del solicitante.

#### **4.2.8. Validación de los documentos de identificación**

El sistema debe ser capaz de validar la información siguiente:

4.2.8.1. Autenticidad:

4.2.8.1.1. Características del documento: tamaño, patrón, diseño, espaciado entre caracteres y tipografía del documento.

|   |  |  |
|---|--|--|
|  | <b>INSTRUCTIVO</b>   | <b>ME-VAR-RPSC-IN-02</b><br>Versión 01 |
|   | <b>IDENTIFICACIÓN VIRTUAL PARA LA EMISIÓN DE CERTIFICADOS DIGITALES DE FIRMAS ELECTRÓNICAS AVANZADAS</b> | <b>Página 8 de 9</b>                   |

- 4.2.8.1.2. Verificación de las medidas de seguridad, como imagen fantasma, fondo numismático, micro línea offset u otras, cuando sea posible.
- 4.2.8.2. Vigencia: Fecha de expiración.
- 4.2.8.3. Integridad: Validación de los datos con la zona de lectura mecánica (MRZ).
- 4.2.8.4. Que el anverso y reverso corresponden al mismo documento.
- 4.2.8.5. Si es asistido, los procesos y herramientas utilizados permitirán verificar al operador visualmente que las imágenes del documento de identidad y fondos de seguridad corresponden con el tipo y versión del documento esperado.
- 4.2.8.6. Si es no asistido, el sistema permitirá a un operador supervisar posteriormente el proceso de identificación grabado y comprobar las evidencias e imágenes generadas del documento de acuerdo con lo especificado en el numeral 4.2.8.5.

**4.2.9. Requisitos de auditoría.**

El sistema debe capturar registros (logs) y almacenarlos para permitir la trazabilidad de cada proceso de identificación. Deberá disponer de los registros siguientes:

- 4.2.9.1. Fecha y hora en la que se produce el registro.
- 4.2.9.2. Identificación del operador que ha realizado el registro.

**4.2.10. Requisitos de administración del servicio.**

- 4.2.10.1. El servicio deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones administrativas.
- 4.2.10.2. El servicio tendrá la capacidad de definir al menos los tipos de roles de administrador y auditor.

**5. ANEXO:**

No Aplica.

**6. CONTROL DE CAMBIOS:**

No Aplica.

|   |  |  |
|---|--|--|
|  | <b>INSTRUCTIVO</b>   | <b>ME-VAR-RPSC-IN-02</b><br>Versión 01 |
|   | <b>IDENTIFICACIÓN VIRTUAL PARA LA EMISIÓN DE CERTIFICADOS DIGITALES DE FIRMAS ELECTRÓNICAS AVANZADAS</b> | <b>Página 9 de 9</b>                   |

**7. APROBACIÓN:**

| Aprobado por                              | Cargo               | Fecha      | Firma y sello |
|---|---------------------|------------|---------------|
| Licda. Mariela Skarlette Anthonne Andrade | Directora Ejecutiva | 30/05/2024 |               |