



Esquema de evaluación y certificación de la seguridad de las tecnologías de información

Evaluación de Biometría Facial.
Herramientas de videoidentificación

01/06/2022

Versión 2

IT-014

© Centro Criptológico Nacional, 2022

Fecha de Edición: Mayo de 2022

La Universidad Carlos III de Madrid (UC3M) ha participado en la realización y modificación del presente documento.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Documento del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de Información.

Copia no controlada en soporte papel.

Índice

1	INTRODUCCIÓN Y ALCANCE	5
2	METODOLOGÍA DE EJECUCIÓN DE LAS PRUEBAS DE EVALUACIÓN BIOMÉTRICA	6
2.1	TIPOS DE PRUEBAS A REALIZAR	6
2.1.1	FASE 1: PRUEBAS DE RENDIMIENTO DEL TOE	6
2.1.2	FASE 2: PRUEBAS DE ROBUSTEZ FIDEDIGNA	6
2.1.3	FASE 3: PRUEBAS DE DETECCIÓN DE ATAQUES DE PRESENTACIÓN	6
2.2	TÉRMINOS UTILIZADOS Y PARÁMETROS DE EVALUACIÓN	6
2.3	FLUJO DE EJECUCIÓN DE LAS PRUEBAS EN LAS FASES 1 Y 2.....	9
2.4	FLUJO DE EJECUCIÓN DE LAS PRUEBAS EN LA FASE 3	13
3	RECURSOS NECESARIOS PARA LA EVALUACIÓN.....	17
3.1	ELECCIÓN DEL TIPO DE CÁMARA	21
4	PRUEBAS DE FUNCIONALIDAD DEL TOE	22
4.1	P1.2M: COMPROBAR VERIFICACIÓN CORRECTA BAJO DISTINTOS ENTORNOS	22
4.1.1	DESCRIPCIÓN	22
4.1.2	ESCENARIOS.....	22
4.1.3	MATERIALES.....	22
4.1.4	SUJETOS	23
4.1.5	ENSAYOS	23
4.1.6	INTENTOS.....	24
4.1.7	PARÁMETROS	24
4.1.8	CRITERIOS DE DECISIÓN Y UMBRAL DE ACEPTACIÓN.....	24
4.1.9	ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN	25
4.2	P1.6: COMPROBAR QUE EL PRODUCTO VERIFICA LA PRUEBA DE VIDA	26
4.2.1	DESCRIPCIÓN	26
4.2.2	ESCENARIOS.....	27
4.2.3	MATERIALES.....	27
4.2.4	SUJETOS	27
4.2.5	ENSAYOS	27
4.2.6	INTENTOS.....	28
4.2.7	PARÁMETROS	28
4.2.8	CRITERIOS DE DECISIÓN Y UMBRAL DE ACEPTACIÓN.....	29
4.2.9	ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN	29
5	PRUEBAS DE DETECCIÓN DE ATAQUES DE PRESENTACIÓN	31
5.1	CARACTERÍSTICAS COMUNES A LAS PRUEBAS	31
5.1.1	ESCENARIOS.....	31
5.1.2	MATERIALES.....	31
5.1.3	INTENTOS.....	32
5.1.4	PARÁMETROS	32
5.1.5	CRITERIOS DE DECISIÓN Y UMBRAL DE ACEPTACIÓN.....	32

5.1.6	ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN	33
5.2	P3.1: ATAQUES DE PRESENTACIÓN DE IMPOSTOR	34
5.2.1	DESCRIPCIÓN	34
5.2.2	MATERIALES	34
5.2.3	SUJETOS	35
5.2.4	ENSAYOS	35
5.2.5	PARÁMETROS	35
5.2.6	ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN	36
5.3	P3.3.2: ATAQUES DE PRESENTACIÓN USANDO VÍDEOS	36
5.3.1	DESCRIPCIÓN	36
5.3.2	MATERIALES	36
5.3.3	SUJETOS	36
5.3.4	ENSAYOS	36
5.3.5	INTENTOS	37
5.3.6	PARÁMETROS	37
5.3.7	ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN	38
5.4	P3.3.3: ATAQUES DE PRESENTACIÓN USANDO MÁSCARAS DE MUY BAJO COSTE	38
5.4.1	DESCRIPCIÓN	38
5.4.2	MATERIALES	38
5.4.3	SUJETOS	38
5.4.4	ENSAYOS	38
5.4.5	PARÁMETROS	39
5.4.6	ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN	39
5.5	P3.3.4: ATAQUES DE PRESENTACIÓN USANDO MÁSCARAS AVANZADAS	40
5.5.1	DESCRIPCIÓN	40
5.5.2	MATERIALES	40
5.5.3	SUJETOS	40
5.5.4	ENSAYOS	40
5.5.5	PARÁMETROS	41
5.5.6	ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN	41
5.6	P3.3.5: ATAQUES DE PRESENTACIÓN USANDO MAQUILLAJE	41
5.6.1	DESCRIPCIÓN	41
5.6.2	MATERIALES	42
5.6.3	SUJETOS	42
5.6.4	ENSAYOS	42
5.6.5	PARÁMETROS	43
5.6.6	ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN	43
5.7	P3.3.6: ATAQUES USANDO HERRAMIENTAS INFORMÁTICAS DE DEEPFAKE	43
5.7.1	DESCRIPCIÓN	43
5.7.2	MATERIALES	44
5.7.3	SUJETOS	44
5.7.4	ENSAYOS	44
5.7.5	PARÁMETROS	45
5.7.6	ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN	45
6	LISTADO DE ACRÓNIMOS	46

1 INTRODUCCIÓN Y ALCANCE

1. El presente documento especifica cómo realizar la evaluación de la funcionalidad de reconocimiento biométrico para la solución descrita en el Anexo F.11 "*Herramientas de Videoidentificación*" dentro de la Guía de Seguridad de las TIC CCN-STIC-140 (en adelante STIC-140-F11).
2. Desde un punto de vista formal, el presente documento es una de las instrucciones técnicas a las que se hace referencia en el Módulo de Evaluación Biométrica (MEB) de la metodología para la certificación LINCE [CCN-STIC-2002]. En caso de que el alcance del TOE descrito en la Declaración de Seguridad incluya diversos documentos de identidad, las pruebas descritas en el presente documento deberán repetirse en su totalidad para cada uno de ellos.

2 METODOLOGÍA DE EJECUCIÓN DE LAS PRUEBAS DE EVALUACIÓN BIOMÉTRICA

2.1 TIPOS DE PRUEBAS A REALIZAR

3. Dentro del alcance del Módulo MEB se realizan tres (3) tipos de PRUEBAS, ejecutadas en tres (3) fases secuenciales.

2.1.1 FASE 1: PRUEBAS DE RENDIMIENTO DEL TOE

4. El objetivo de estas PRUEBAS es verificar que el rendimiento declarado por el fabricante se mantiene en el ESCENARIO de uso previsto para el producto en cuestión. Es decir, el objetivo principal es comprobar si en un uso normal del TOE, éste tiene un comportamiento funcionalmente correcto.
5. Las PRUEBAS de FASE 1 consideradas para este tipo de producto se describen en la sección 4.

2.1.2 FASE 2: PRUEBAS DE ROBUSTEZ FIDEDIGNA

6. El objeto de estas PRUEBAS es localizar los puntos límite de funcionamiento con USUARIOS fidedignos para conocer el sistema y descubrir estrategias de ataque para la fase 3. Los resultados obtenidos se comprobarán con el manual del TOE, para verificar si los casos problemáticos están claramente excluidos del uso.
7. La presente instrucción técnica no se ocupa de la descripción de este tipo de pruebas ya que se prevé que no se realicen pruebas de este tipo.

2.1.3 FASE 3: PRUEBAS DE DETECCIÓN DE ATAQUES DE PRESENTACIÓN

8. El objeto de estas PRUEBAS es comprobar si el sistema es susceptible de ser atacado en el proceso de presentación de la muestra biométrica. Los ataques realizados en esta fase podrán ser tanto de suplantación como de ofuscación. Por normal general, salvo que sea justificado a lo largo de la evaluación, un ataque exitoso contra el TOE (siempre considerando que no supera el máximo potencial de ataque) hará fallar la evaluación de seguridad.
9. Las PRUEBAS de FASE 3 consideradas para este tipo de producto se describen en la sección 5.

2.2 TÉRMINOS UTILIZADOS Y PARÁMETROS DE EVALUACIÓN

10. La gran mayoría de las PRUEBAS biométricas siguen una secuencia de ejecución muy similar, que se describe en los apartados 2.3 y 2.4. Esta descripción genérica del flujo de la prueba permitirá simplificar la descripción detallada de cada una de las pruebas que se presenta en los capítulos 4 y 5 del presente documento. En la descripción detallada de cada una de las pruebas se hará referencia a este flujo genérico, evitando así la necesidad de repetirlo en cada una de ellas.

11. Para la correcta comprensión de esta metodología, es necesario describir los siguientes términos:

- **ARTEFACTO:** Objeto artificial o representación que presenta una copia de características biométricas o patrones biométricos sintéticos.
- **ATACANTE:** Individuo que ataca el sistema. Puede ser un impostor o emplear un artefacto para ataques de presentación.
- **DISTINTO:** Resultado negativo de la comparación biométrica en un ENSAYO. Por ejemplo, un rechazo a la identificación de un SUJETO fidedigno en una PRUEBA funcional. En el caso de una PRUEBA de PAD, un DISTINTO es el resultado deseable, puesto que no ha permitido hacer una verificación correcta con el artefacto utilizado.
- **ENSAYO:** Cada una de las acciones de un SUJETO frente al TOE, con el objetivo de pasar la PRUEBA. Dependiendo del TOE, cada ENSAYO puede permitir varios INTENTOS (por ejemplo, el TOE puede mandar repetir la presentación de la muestra por errores en la captura, constituyendo dicha nueva presentación un nuevo INTENTO).
- **EQUIVALENTE:** Resultado positivo de la comparación biométrica en un ENSAYO. Por ejemplo, una identificación correcta de un SUJETO fidedigno en una PRUEBA funcional. En el caso de una PRUEBA de PAD, un EQUIVALENTE sería el resultado no esperado, puesto que implicaría que un artefacto ha sido verificado correctamente.
- **ERROR:** Situación en la que el TOE no es capaz de realizar correctamente su función, y por tanto no puede terminar la ejecución de la comparación. Un ejemplo podría ser el que el subsistema de captura no permitiese obtener la muestra biométrica de un SUJETO fidedigno. En el caso de una PRUEBA de PAD, un ERROR (una vez superado el límite máximo de INTENTOS) puede ser considerado como DISTINTO, al no capturar (es decir, rechazar) la muestra biométrica obtenida a partir del artefacto.
- **ERROR_PRUEBA:** Situación en la que, dentro de una PRUEBA, los ENSAYOS correspondientes a un SUJETO superan un límite máximo de ERRORES_SUJETO permitidos para ese SUJETO.
- **ESCENARIO:** Contexto de ejecución de un ENSAYO de la PRUEBA. El ESCENARIO puede ser la descripción de los equipos a utilizar, de la forma de interacción, de las condiciones de entorno, de los artefactos a presentar, etc. Para cada PRUEBA habrá que definir el/los ESCENARIO/S a considerar.
- **FALLA:** Para las pruebas de las fases 1 y 2, resultado final de una PRUEBA que indica que el comportamiento del TOE no es el adecuado. Por el contrario, para las pruebas de penetración de la fase 3 un resultado FALLA implica que la prueba de penetración no ha tenido éxito y, por lo tanto, el comportamiento del TOE es el adecuado.
- **INTENTO:** Cada una de las interacciones individuales que hace el SUJETO con el TOE para ejecutar el ENSAYO.

- **OPERADOR:** Persona que, partiendo de los datos capturados por el TOE durante el proceso de reconocimiento, toma la decisión de si la operación es válida o no.
- **PASA:** Para las pruebas de las fases 1 y 2, resultado final de una PRUEBA que indica que el comportamiento del TOE es el adecuado. Por el contrario, para las pruebas de penetración de la fase 3 un resultado PASA implica que la prueba de penetración ha tenido éxito y, por lo tanto, el comportamiento del TOE no es el adecuado.
- **PRUEBA:** Acción de evaluar el comportamiento del sistema biométrico para determinar ciertas características. Una PRUEBA estará compuesta por múltiples ENSAYOS, que involucrarán a varios SUJETOS y, probablemente, varios ESCENARIOS.
- **SERVIDOR:** Equipo informático en el que el TOE almacena los datos capturados durante el proceso de reconocimiento, para que posteriormente sean analizados por el OPERADOR.
- **SUJETO:** Conjunto de USUARIO y documento, que se utilizará para interactuar con el TOE, durante un ENSAYO. Toda PRUEBA biométrica contará con la participación de varios SUJETOS. En caso de pruebas PAD será el conjunto de USUARIO, documento y artefacto.
- **USUARIO:** Individuo que forma parte de un ENSAYO. Dependiendo de la PRUEBA, el USUARIO podrá ser fidedigno, ATACANTE, o contar con dos USUARIOS, uno de ellos actuando como fidedigno y otro como atacante.

12. También es importante tener en cuenta las siguientes constantes:

- **MAX_DISTINTOS_ESCENARIO:** (Fases 1 y 2) número máximo de ENSAYOS, de todos los exigidos dentro de un ESCENARIO de una PRUEBA, que pueden dar resultado DISTINTO, antes de que pueda considerarse que la PRUEBA FALLA para ese ESCENARIO.
- **MAX_DISTINTOS_PRUEBA:** (Fases 1 y 2) número máximo de ENSAYOS, de todos los exigidos en una PRUEBA, que den resultado DISTINTO, antes de considerar que la PRUEBA FALLA.
- **MAX_DISTINTOS_SUJETO:** (Fases 1 y 2) número máximo de ENSAYOS con resultado DISTINTO que se permiten para un mismo SUJETO, en un ESCENARIO.
- **MAX_EQUIVALENTES_ESCENARIO:** (Fase 3) número máximo de ENSAYOS, de todos los exigidos dentro de un ESCENARIO de una PRUEBA, que pueden dar resultado EQUIVALENTE, antes de que pueda considerarse que la PRUEBA PASA para ese ESCENARIO.
- **MAX_EQUIVALENTES_PRUEBA:** (Fase 3) número máximo de ENSAYOS, de todos los exigidos en una PRUEBA, que den resultado EQUIVALENTE, antes de considerar que la PRUEBA PASA.

- **MAX_EQUIVALENTES_SUJETO:** (Fase 3) número máximo de ENSAYOS con resultado EQUIVALENTE, que se permiten para un mismo SUJETO, en un ESCENARIO.
 - **MAX_ERRORES_PRUEBA:** (Fases 1 y 2) número máximo de SUJETOS para los que, dentro de una PRUEBA, sus ENSAYOS han superado un número de errores dado por MAX_ERRORES_SUJETO.
 - **MAX_ERRORES_SUJETO:** (Fases 1 y 2) número máximo de ERRORES_SUJETO permitidos en los ENSAYOS realizados para un mismo SUJETO, dentro de un mismo ESCENARIO y PRUEBA.
 - **MAX_FALLA_SUJETOS:** (Fases 1 y 2) número máximo de SUJETOS, para los que los ENSAYOS dentro de una PRUEBA y ESCENARIO, han superado el número de DISTINTOS, dado por MAX_DISTINTOS_SUJETO.
 - **MAX_PASA_SUJETOS:** (Fase 3) número máximo de SUJETOS, para los que los ENSAYOS dentro de una PRUEBA y ESCENARIO, han superado el número de EQUIVALENTES dado por MAX_EQUIVALENTES_SUJETO.
 - **MAX_INTENTOS:** número máximo de INTENTOS que de superarse dará lugar a un ERROR en el ENSAYO.
 - **MIN_ENSAYOS:** número mínimo de ENSAYOS definidos.
 - **MIN_ESCENARIOS:** número mínimo de ESCENARIOS definidos
 - **MIN_SUJETOS:** número mínimo de SUJETOS definidos.
13. Como se puede ver, los parámetros MIN_ENSAYOS, MIN_ESCENARIOS y MIN_SUJETOS, indican un número mínimo especificado en cada una de las PRUEBAS. Ese será el número que deberá utilizar el laboratorio. Sin embargo, si el laboratorio, en los ENSAYOS realizados detecta resultados ERROR, incrementará ese valor (ya sea el número de ENSAYOS, de ESCENARIOS, o de SUJETOS) hasta que obtenga el número de resultados conclusos igual al producto de MIN_ENSAYOS por MIN_ESCENARIOS y por MIN_SUJETOS o alcance un máximo número de intentos ERROR igual a MAX_ERRORES_PRUEBA. Estas desviaciones deben ser plenamente justificadas y reflejadas en el Informe Técnico de Evaluación.

2.3 FLUJO DE EJECUCIÓN DE LAS PRUEBAS EN LAS FASES 1 Y 2

14. Cada una de las PRUEBAS a realizar va a contar con una serie de ESCENARIOS, un conjunto de SUJETOS, y para cada una de esas combinaciones, se llevarán a cabo una serie de ENSAYOS, los cuales pueden contar con varios INTENTOS. La siguiente figura representa la relación entre estos elementos.

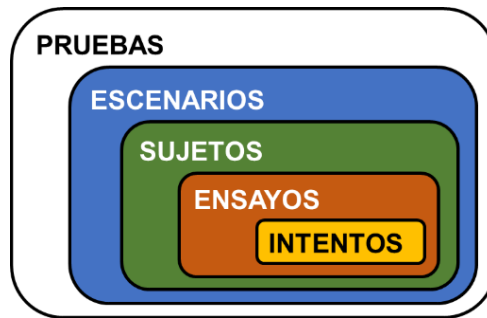


Figura 1: Figura relacional

15. La ejecución de cada PRUEBA se resume en la ejecución de una serie de ESCENARIOS, hasta llegar a un mínimo marcado por MIN_ESCENARIOS. El laboratorio deberá ampliar el número de escenarios en caso de resultados de ERROR como se ha visto en el párrafo 13, hasta un número no superior a MAX_ESCENARIOS. Una vez finaliza la ejecución de todos los ESCENARIOS, se analizan los resultados obtenidos para todos los SUJETOS y ENSAYOS, para determinar el resultado final de dicha PRUEBA basándose en los criterios dados.

16. El siguiente diagrama de flujo muestra el proceso de ESCENARIOS:

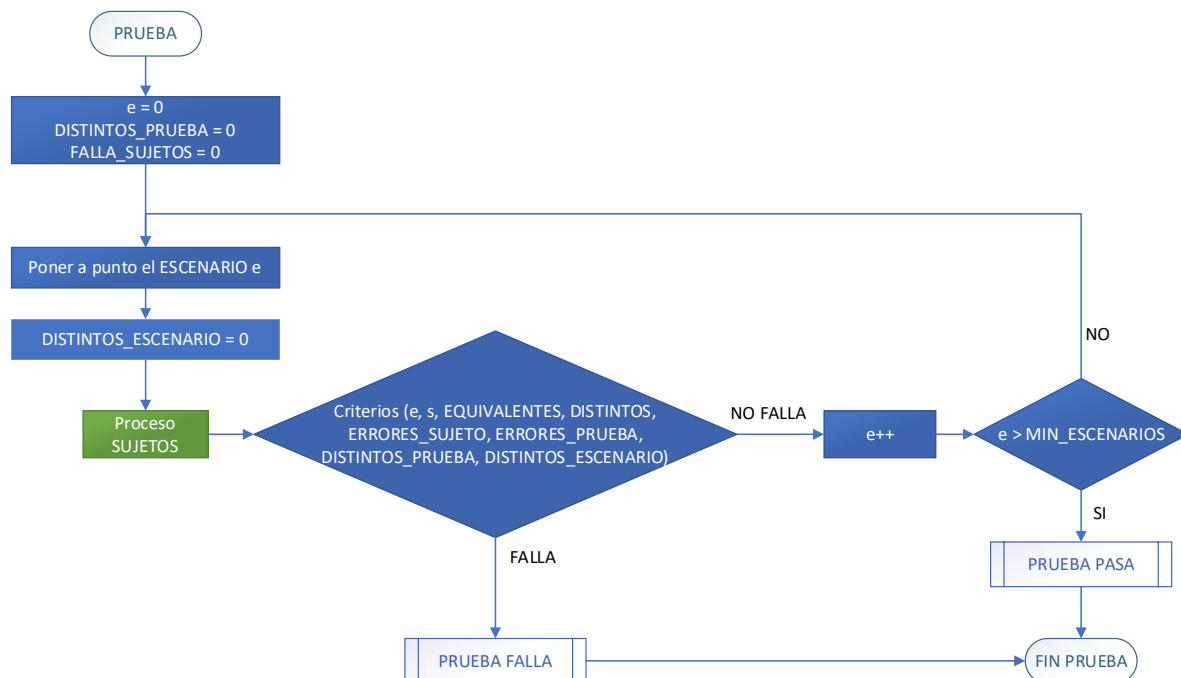


Figura 2: Diagrama de flujo – Proceso ESCENARIOS (Fases 1 y 2)

17. En la ejecución de cada ESCENARIO, participarán diversos SUJETOS hasta cumplir un mínimo de MIN_SUJETOS. El laboratorio deberá ampliar el número de SUJETOS en caso de resultados de ERROR como se ha visto en el párrafo 13, hasta un número no superior a MAX_SUJETOS. Una vez finalizada la ejecución de todos los ENSAYOS para cada SUJETO, se analizan los resultados obtenidos, atendiendo al número de ERRORES_SUJETO, EQUIVALENTES y DISTINTOS obtenidos para ese SUJETO. Finalizados todos los SUJETOS, se analizarán los resultados para saber si la PRUEBA PASA o FALLA, caso de que no hubiese dado un FALLO antes.

18. El siguiente diagrama de flujo muestra el proceso de SUJETOS:

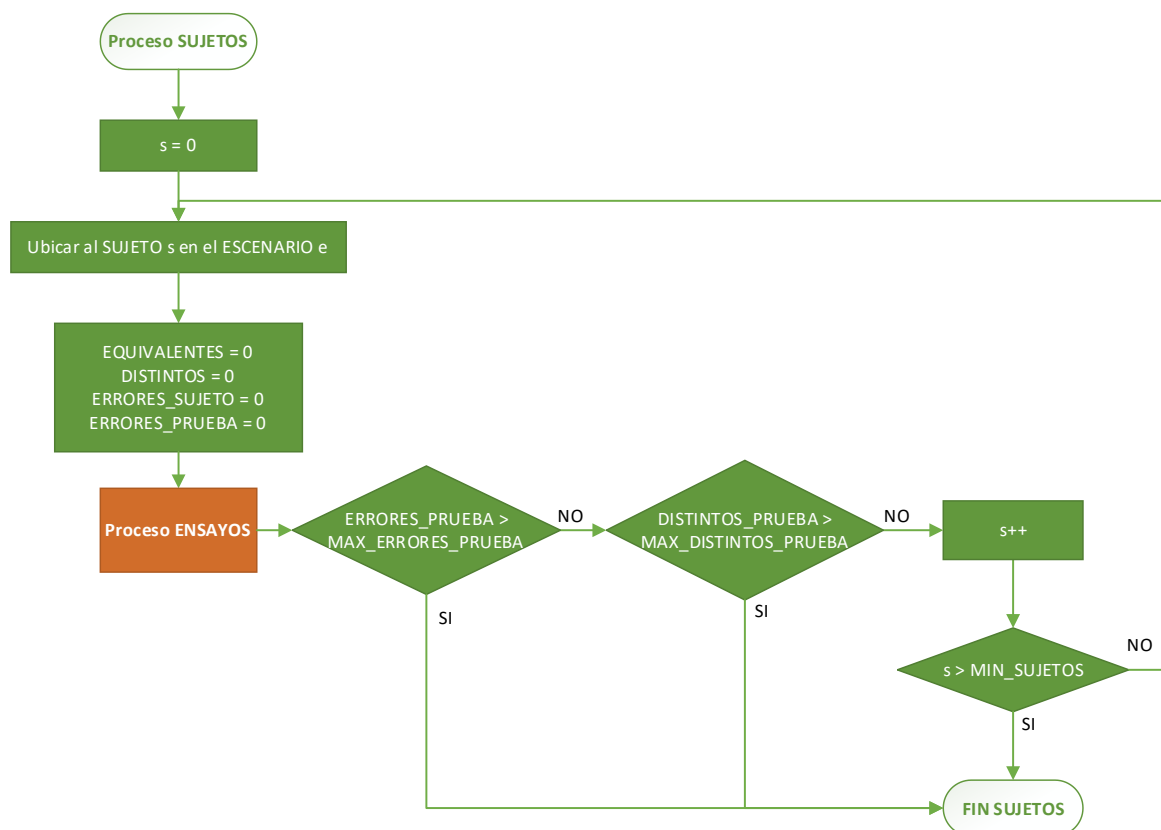


Figura 3: Diagrama de flujo – Proceso SUJETOS (Fases 1 y 2)

19. Con cada SUJETO, se realizarán una serie de ENSAYOS, hasta cumplir con un mínimo marcado por MIN_ENSAYOS. El laboratorio deberá ampliar el número de ensayos en caso de resultados de ERROR como se ha visto en el párrafo 13, hasta un número no superior a MAX_ENSAYOS. En la ejecución de cada ENSAYO, se podrán hacer varios INTENTOS (con un límite máximo dado por MAX_INTENTOS), hasta obtener un EQUIVALENTE, un DISTINTO o un ERROR.
20. Si al ejecutar un INTENTO, el TOE no ofrece un resultado, sino que falla en su ejecución, se realizará un nuevo INTENTO. Esto se realizará hasta alcanzar el límite dado por MAX_INTENTOS. En caso de superar dicho umbral, el ENSAYO se calificará como ERROR. Si el número de ENSAYOS que dan ERROR supera el límite MAX_ERRORES_SUJETO, se finalizarán los ENSAYOS para ese SUJETO, incrementando el contador de ERRORES_PRUEBA.
21. Si a lo largo de la PRUEBA, el número de ERRORES_PRUEBA supera el límite establecido por MAX_ERRORES_PRUEBA (es decir, hay demasiados SUJETOS que no permiten una captura adecuada de sus datos), se informará de la situación en el ETR. Además, se añadirá un nuevo SUJETO, que cumpla las condiciones establecidas, y se ejecutarán los ensayos de la PRUEBA para ese nuevo SUJETO, decrementándose en una unidad el contador ERRORES_PRUEBA. De volver a darse esta situación, se finalizará la PRUEBA y se considerará que la PRUEBA FALLA.
22. Si el resultado del TOE es la comparación exitosa de la muestra presentada, se incrementará el contador de EQUIVALENTES y de EQUIVALENTES_PRUEBA. En caso contrario, se incrementarán los contadores DISTINTOS, DISTINTOS_PRUEBA y DISTINTOS_ESCENARIO.

23. Si el número de DISTINTOS es superior al indicado por MAX_DISTINTOS_SUJETO, se finalizará la PRUEBA para ese SUJETO, indicando que la PRUEBA FALLA para ese SUJETO. En ese caso, se pasará al siguiente SUJETO. Si a lo largo de la ejecución de la PRUEBA, el número de DISTINTOS_PRUEBA supera el umbral dado por MAX_DISTINTOS_PRUEBA, se finalizará la PRUEBA, aplicándose el criterio correspondiente en la PRUEBA para esa situación.
24. Es muy importante tener en cuenta que, en cada INTENTO, el SUJETO tiene que interactuar con el TOE de la forma indicada en la guía de operación evaluada. Esto implicará que, entre INTENTO e INTENTO, el SUJETO debe retirarse de la interacción con el TOE de forma significativa (por ejemplo, que el SUJETO mueva temporalmente su posición respecto al TOE, para que, temporalmente salga de la misma línea perpendicular al objetivo del TOE).
25. El siguiente diagrama de flujo muestra el proceso de ejecución de los ENSAYOS:

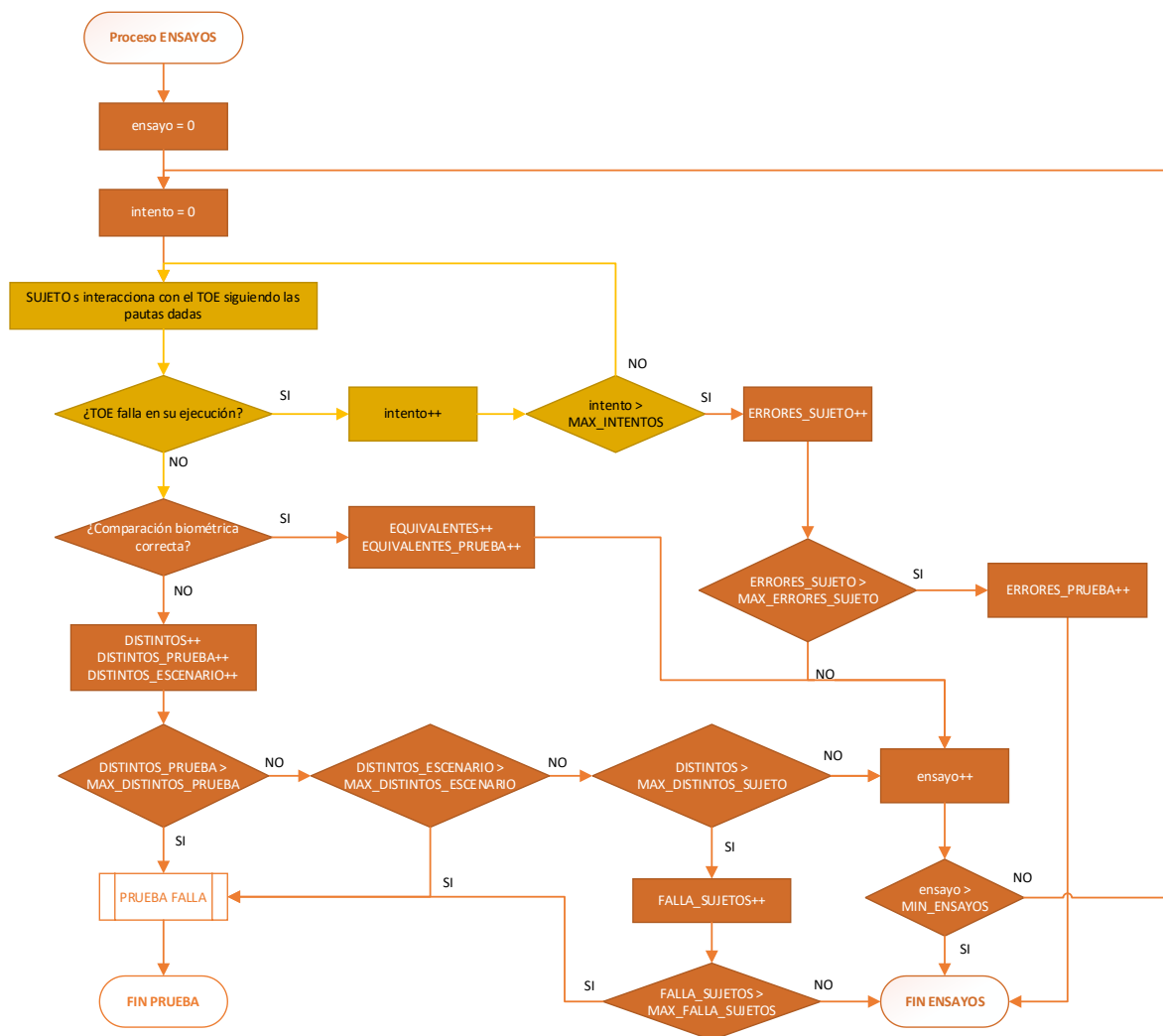


Figura 4: Diagrama de flujo de la ejecución de ENSAYOS (Fases 1 y 2)

26. Dependiendo de la PRUEBA, puede ser interesante intercambiar el orden entre ESCENARIOS y SUJETOS. Es decir, se permite que, en lugar de hacer las PRUEBAS para todos los SUJETOS en un mismo ESCENARIO, se hagan las PRUEBAS para todos los

ESCENARIOS, por parte de un mismo SUJETO. Dicha decisión será tomada por el laboratorio basándose en criterios de comodidad o de agilidad en la realización de las PRUEBAS.

27. También se permite al laboratorio intercambiar SUJETOS y PRUEBAS, de forma que se pueda explotar la presencia de un determinado SUJETO para hacerle ejecutar los ENSAYOS de todas las PRUEBAS.
28. Es decir, los siguientes diagramas son admisibles, y será potestad del Laboratorio, el decidir qué flujo le resulta más óptimo. No se recomienda, salvo por razón justificada, cambiar de flujo dentro de la misma evaluación. La aproximación seguida será documentada por el laboratorio en el Informe Técnico de Evaluación.

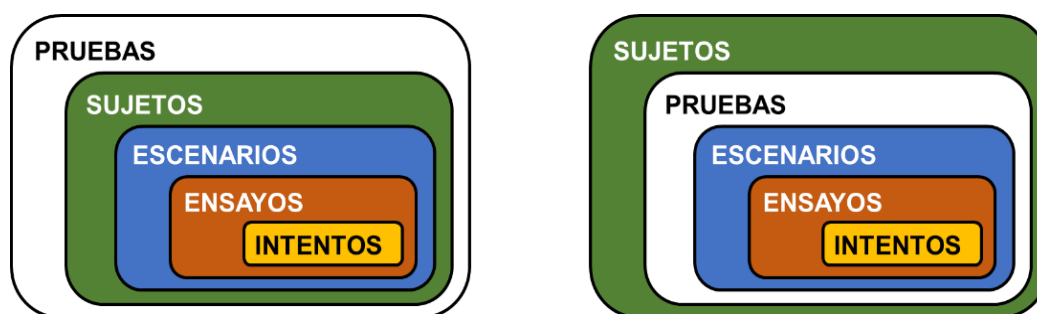


Figura 5: Flujos posibles

2.4 FLUJO DE EJECUCIÓN DE LAS PRUEBAS EN LA FASE 3

29. En la Fase 3 también es de aplicación lo indicado por los párrafos 14, 15, 26, 27 y 28.
30. En la Fase 3, el resultado deseable de cada PRUEBA es el de FALLA, ya que, si la PRUEBA da como resultado PASA, significa que el ataque ha sido satisfactorio.
31. El siguiente diagrama de flujo muestra el proceso de ESCENARIOS:

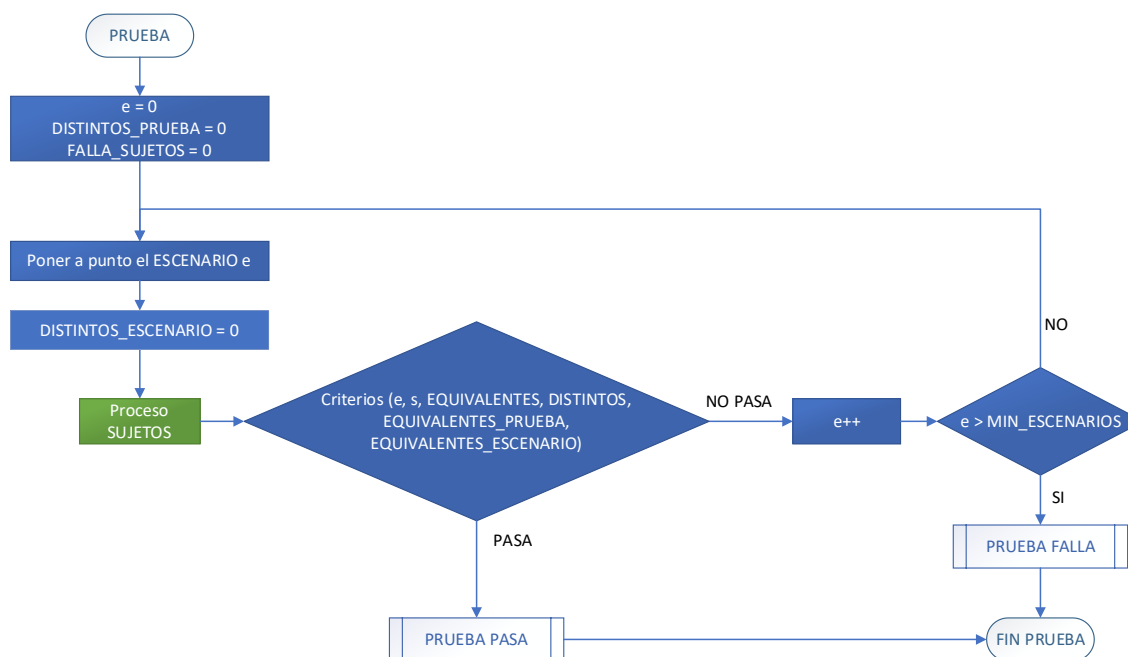


Figura 6: Diagrama de flujo – Proceso ESCENARIOS (Fase 3)

32. En la ejecución de cada ESCENARIO, participarán diversos USUARIOS FIDEDIGNOS hasta cumplir un mínimo de MIN_SUJETOS. El laboratorio deberá ampliar el número de USUARIOS FIDEDIGNOS en caso de resultados de ERROR como se ha visto en el párrafo 13, hasta un número no superior a MAX_SUJETOS. Una vez finalizada la ejecución de todos los ENSAYOS para cada SUJETO, se analizan los resultados obtenidos, atendiendo al número de EQUIVALENTES y DISTINTOS obtenidos para ese SUJETO. Finalizados todos los SUJETOS, se analizarán los resultados para saber si la PRUEBA PASA o FALLA, caso de que no hubiese dado un PASA antes.
33. El siguiente diagrama de flujo muestra el proceso de SUJETOS:

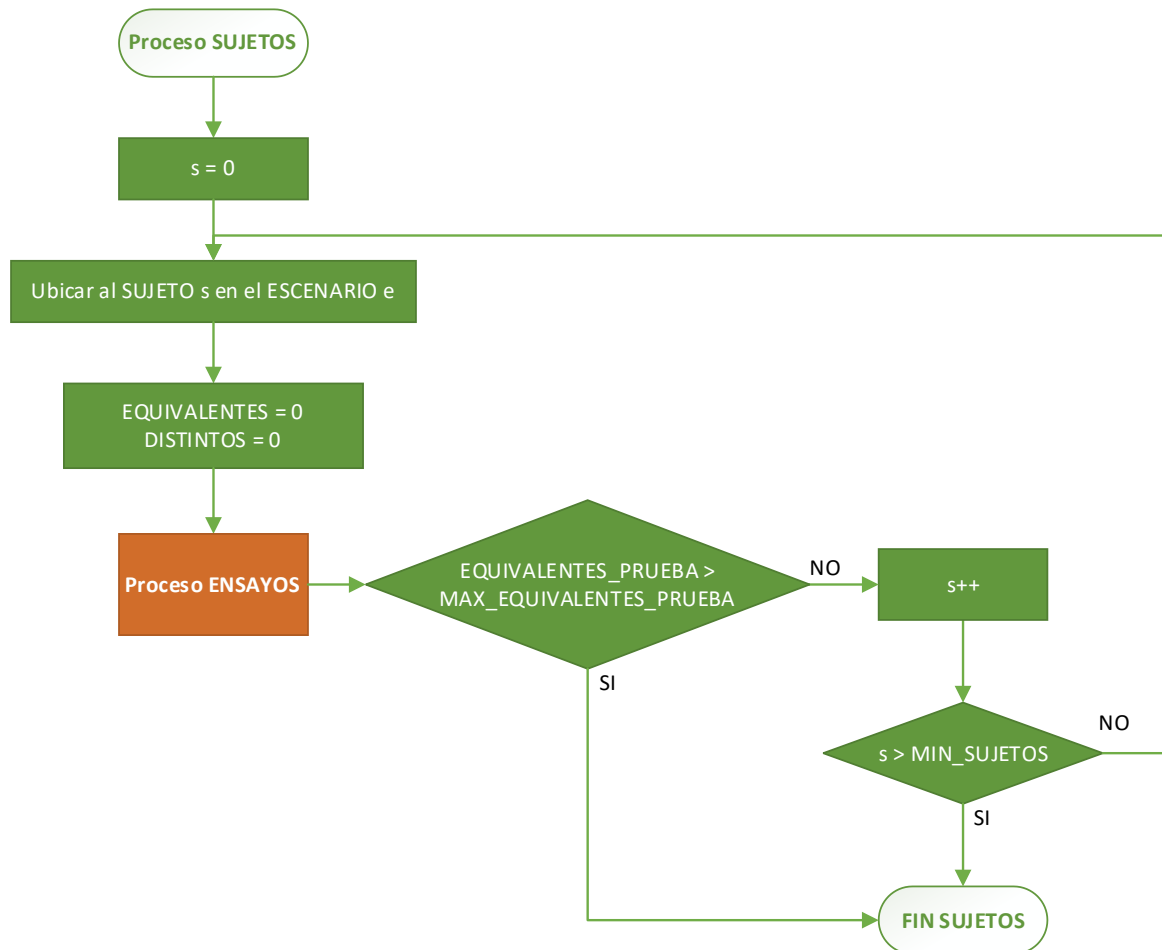


Figura 7: Diagrama de flujo – Proceso SUJETOS (Fase 3)

34. Con cada SUJETO, se realizarán una serie de ENSAYOS, hasta cumplir con un mínimo marcado por MIN_ENSAYOS. El laboratorio deberá ampliar el número de ensayos en caso de resultados de ERROR como se ha visto en el párrafo 13, hasta un número no superior a MAX_ENSAYOS. En la ejecución de cada ENSAYO, se podrán hacer varios INTENTOS (con un límite máximo dado por MAX_INTENTOS), hasta obtener un EQUIVALENTE, un DISTINTO o un ERROR.
35. Si al ejecutar un INTENTO, el TOE no ofrece un resultado, sino que falla en su ejecución, se realizará un nuevo INTENTO. Esto se realizará hasta alcanzar el límite dado por MAX_INTENTOS. En caso de superar dicho umbral, el ENSAYO se calificará como ERROR. En las PRUEBAS de la Fase 3, un ERROR es un resultado deseable, ya que

implica que el ENSAYO no ha sido satisfactorio, y por lo tanto que no provocaría un PASA en la PRUEBA.

36. Si el resultado del TOE es la comparación exitosa de la muestra presentada, se incrementarán los contadores EQUIVALENTES, EQUIVALENTES_PRUEBA y EQUIVALENTES_ESCENARIO. Por el contrario, se incrementará el contador de DISTINTOS y de DISTINTOS_PRUEBA.
37. Si el número de EQUIVALENTES es superior al indicado por MAX_EQUIVALENTES_SUJETO, se finalizará la PRUEBA para ese SUJETO, indicando que la PRUEBA PASA para dicho SUJETO. Se pasará al siguiente SUJETO. Si a lo largo de la ejecución de la PRUEBA, el número de EQUIVALENTES_PRUEBA supera el umbral dado por MAX_EQUIVALENTES_PRUEBA, se finalizará la PRUEBA, indicando que la PRUEBA PASA. De la misma forma, si a lo largo de la PRUEBA el número de EQUIVALENTES_ESCENARIO supera el umbral dado por MAX_EQUIVALENTES_ESCENARIO, se finalizará la PRUEBA, indicando que la PRUEBA PASA.
38. Es muy importante tener en cuenta que, en cada INTENTO, el SUJETO tiene que interactuar con el TOE de la forma indicada en la guía de operación evaluada, salvo por aquella característica propia de la PRUEBA. Esto implicará que, entre INTENTO e INTENTO, el SUJETO debe retirarse de la interacción con el TOE de forma significativa (por ejemplo, que el SUJETO mueva temporalmente su posición respecto al TOE, para que, temporalmente salga de la misma línea perpendicular al objetivo del TOE).
39. El siguiente diagrama de flujo muestra el proceso de ejecución de los ENSAYOS:

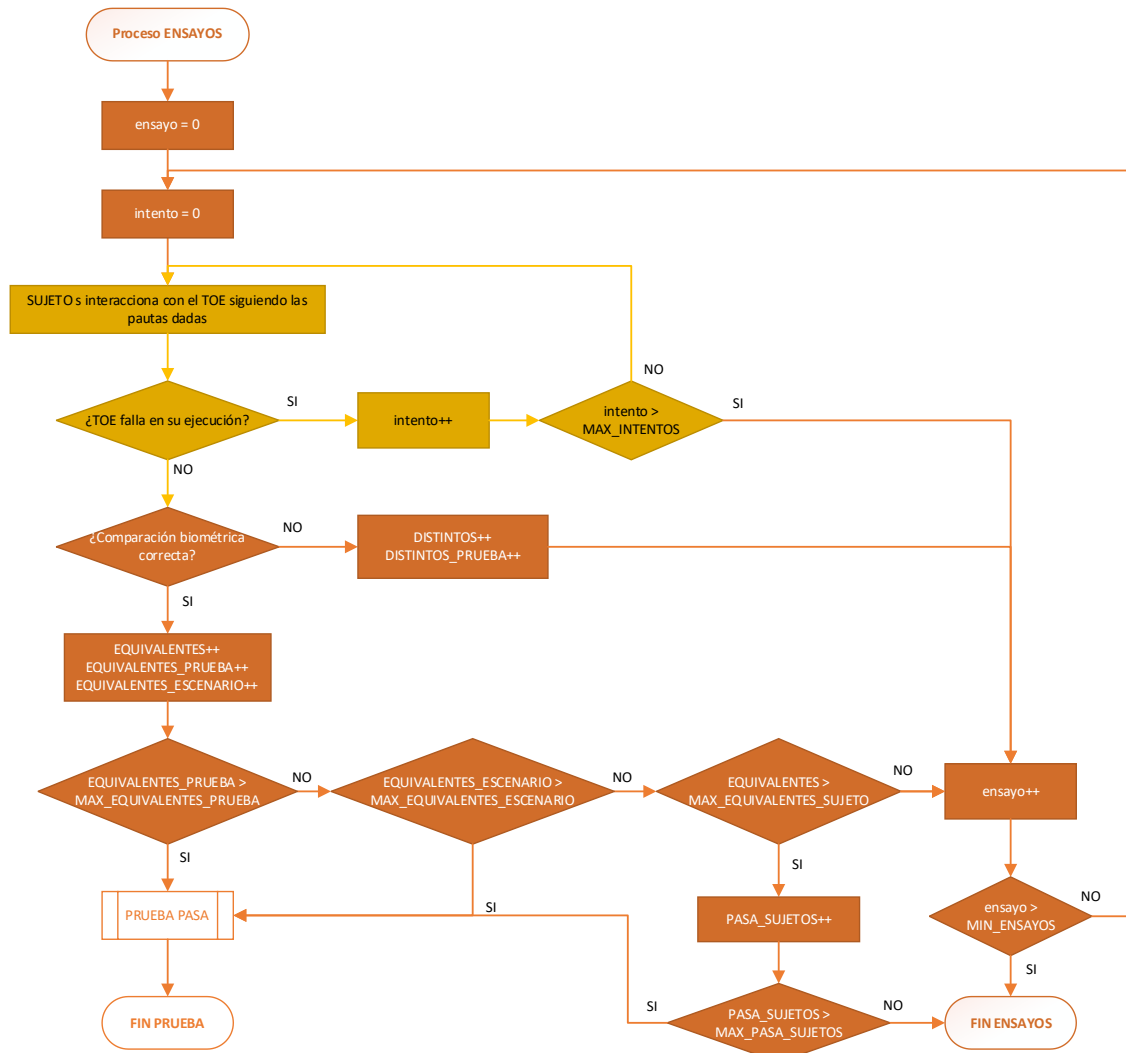


Figura 8: Diagrama de flujo de la ejecución de ENSAYOS (Fase 3)

3 RECURSOS NECESARIOS PARA LA EVALUACIÓN

40. A continuación, se presenta un resumen de los RECURSOS (MATERIALES y SUJETOS) necesarios para ejecutar las tareas de evaluación definidas en esta instrucción técnica y que será objeto de la inspección técnica propia para el dominio técnico definido en el [PO-008]:

- *Software* de referencia de comparación de parecido facial, proporcionado por el CCN, denominado CCN_MATCH, el cual determinará si dos imágenes faciales consiguen un nivel de parecido adecuado para ser consideradas en pruebas.
- Un mínimo de seis (6) USUARIOS fidedignos. Sus parecidos deben ser bajos, para lo cual la comparación entre los mismos debe dar un resultado superior al umbral 70 en la herramienta CCN_MATCH. Deberá haber, al menos, dos (2) USUARIOS de cada sexo.
- Un mínimo de dos (2) ATACANTES.
- Dispositivos de captura (cámaras), que podrán ser distintas de una PRUEBA a otra, pero siempre dentro de las que contemple el TOE dentro de la guía de operación evaluada. Los requisitos de cada cámara se definirán en cada PRUEBA y serán documentados en el Informe Técnico de Evaluación.
- Un **equipo de retroproyección** o, en su defecto, un **televisor de alta resolución**, donde emular el fondo en cada uno de los ESCENARIOS. En ningún caso, en la captura de la imagen/**video** del SUJETO, deben verse los bordes de la opción escogida para emular el fondo. En el caso de que se trate de un televisor de alta resolución, éste tiene que ser de resolución mínima 4K, ya que al tratarse de un televisor de gran formato la resolución debe ser suficientemente alta para que la captura de la imagen por el TOE no muestre artefactos. En el caso de que la solución sea un equipo de retroproyección, sus características deben ser las siguientes:
 - a. Pantalla de retroproyección óptica de mínimo 90". La relación de aspecto puede ser 4:3 o 16:9, con ganancia mínima de 1,0 y ángulo de visión superior a 90 grados. Su instalación debe dejarla libre de arrugas.
 - b. Proyector de video con resolución mínima Full HD (1920 x 1080), y con capacidad de ser usado como retroproyección. Luminosidad mínima de 3000 lúmenes.
- Un documento de identidad de cada uno de los USUARIOS fidedignos. El tipo de documento utilizado será el mismo para todos los usuarios y estará indicado en la Declaración de Seguridad y en la guía de operación del TOE. En caso de incluir N documentos en la Declaración de Seguridad deberán realizarse N evaluaciones, una por cada tipo de documento.
- Un **video** por cada uno de los **seis** (6) USUARIOS fidedignos participantes **en la PRUEBA** P3.3.2, con las siguientes características:

- Grabado con una cámara de alta resolución (resolución mínima de 1920 x 1080, con una tasa de refresco mínima de 50 fotogramas por segundo), para su posterior reproducción como artefacto.
- Grabado desde un punto de vista tan similar como sea posible al adoptado cuando el USUARIO fidedigno interactúa con el TOE (es decir, misma distancia, mismo ángulo de visión, etc.). El vídeo representará la interacción exitosa del SUJETO fidedigno utilizando el ESCENARIO definido. La grabación no sólo captará al SUJETO, sino también el fondo definido por el ESCENARIO.
- Si el TOE solicita diferentes tipos de prueba de vida de forma aleatoria entre un conjunto, deberá grabarse un vídeo de cada una de esas interacciones. Se recomienda al laboratorio emplear muestras abiertas del TOE que permitan controlar el tipo de prueba de vida.

Estos vídeos podrán ser generados a partir de las interacciones correctas de la Fase I.

- Un vídeo por cada uno de los escenarios definidos que contarán con las siguientes características:
 - a. ESCENARIO dinámico sin personas (E.1.2.1). Se trata de una secuencia de vídeo continuo (sin cortes entre fotogramas) en el que no aparecen individuos, pero sí hay movimiento (por ejemplo, un vídeo que muestre un paisaje panorámico, o una oficina vacía, donde la cámara se mueva de un extremo al otro del paisaje, pudiendo volver al inicio). El vídeo podrá ser de interiores (por ejemplo, una oficina) o de exteriores (por ejemplo, un paisaje montañoso o una ciudad). El vídeo debe durar, como mínimo, el tiempo que pueda llegar a durar cada uno de los ENSAYOS.
 - b. ESCENARIO dinámico con personas (E.1.2.2). Se trata de un vídeo, análogo al anterior, pero en el que ahora aparezcan personas, algunas de las cuales deben, temporalmente, mirar en dirección a la cámara. Algunas de esas personas que aparezcan, deberán ser los USUARIOS fidedignos que se utilizarán en las PRUEBAS. El vídeo podrá ser de interiores (por ejemplo, una oficina) o de exteriores (por ejemplo, un paisaje montañoso o una ciudad). El vídeo debe durar, como mínimo, el tiempo que pueda llegar a durar cada uno de los ENSAYOS.
- Dos tipos de máscaras de bajo coste que representen la cara de cada uno de los seis (6) USUARIOS fidedignos utilizados en la PRUEBA P3.3.3. (dos máscaras por cada USUARIO). Estas máscaras serán:
 - a. Una impresión en papel, recortada la cara y los ojos, y que se pueda poner sobre la cara del atacante. El material con el que esté hecha la máscara debe dar un aspecto natural frente al TOE, evitando, por ejemplo, reflejos de las luces del TOE o de la escena sobre dicho papel (por ejemplo, debe evitarse el utilizar papel fotográfico brillante). Dependiendo del TOE, la tinta con la que estén impresas dichas máscaras puede dar lugar a resultados distintos, por lo que se

recomienda que la mitad de las máscaras sean impresas con impresoras láser, mientras que la otra mitad estén impresas con inyección de tinta.

- b. Segunda piel facial personalizada. Se trata de una prenda de tela (al estilo de una media) con la cara del USUARIO fidedigno pintada y que se coloca en la cabeza del atacante. La prenda debe tener apertura para los ojos y la boca. Debe ser colocada de forma que las arrugas de la tela queden disimuladas y deberá ser completado con el uso de pelucas que simulen al USUARIO fidedigno, en caso de que este tenga pelo. La siguiente figura muestra ejemplos de este tipo de productos:



Figura 9: Ejemplos de productos de "segunda piel"¹

— Para la PRUEBA P3.3.4 se utilizarán dos (2) *máscaras avanzadas* que cumplan alguna de las siguientes condiciones:

- a. Representar la cara de dos (2) USUARIOS fidedignos.
- b. Representar la cara de dos (2) USUARIOS genéricos, para los cuales se disponga de su correspondiente documento de identidad válido. En este caso los USUARIOS representados serán considerados como USUARIOS fidedignos para la realización de la prueba.

Se considera *máscara avanzada* aquella máscara realista que refleje con todo detalle es aspecto facial del **USUARIO**, incluyendo tonalidad y estructura tridimensional de su cara. Se pueden ver ejemplos de estas máscaras en la siguiente figura:

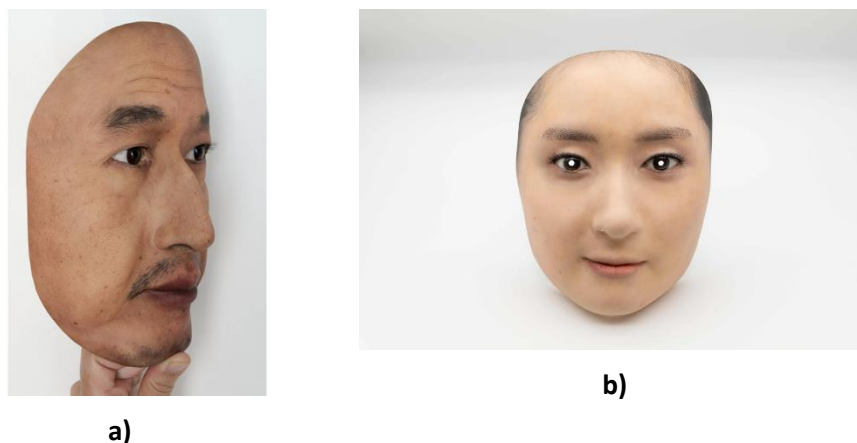


Figura 10: Ejemplos de máscaras avanzadas²

¹ Imágenes tomadas de <https://www.britishmade.gifts>

- Profesional maquillador y/o material de maquillaje, con más de 5 años de experiencia de maquillador profesional.

Deberá hacer aparentar a un atacante, como si fuese el USUARIO fidedigno (PRUEBA P3.3.5). El laboratorio deberá acreditar un máximo de 60 de parecido con respecto al **USUARIO** fidedigno empleando la herramienta CCN_MATCH. Las técnicas de maquillaje y el material pueden ser muy variados, atendiendo a las necesidades. Por ejemplo, una técnica a considerar es la de *contouring*, tal y como se puede ver en las siguientes imágenes:



Figura 11: Ejemplos de tipos de maquillaje³

- Un sistema de generación de vídeos de *deepfake* en tiempo real. El sistema debe permitir entrenar cuatro (4) modelos faciales de USUARIOS fidedignos que puedan utilizarse para reemplazar la cara del ATACANTE por la del sujeto a suplantar en tiempo real durante la realización de la PRUEBA 3.3.6. Se deberán utilizar las siguientes herramientas de forma combinada:
 - DeepFaceLive: <https://github.com/iperov/Deepfacelive>
 - OBS Studio: <https://obsproject.com/es>
 - DeepFaceLab: <https://sourceforge.net/projects/deepfacelab.mirror/>
 - Tarjeta de **video** con los siguientes requisitos mínimos:
 - GPU de frecuencia mínima de **1,4 GHz**
 - Memoria RAM mínima de **10 GB** GDDR6X e interfaz de memoria de mínimo **256 bits**

² Imágenes tomadas de: a) http://real-f.jp/en_news.html; b) <https://www.etsy.com/es/shop/maskshopOMOTE>

³ Imágenes tomadas de: a) <https://www.demilked.com/celebrity-makeup-artist-face-paint-contouring-lucia-pittalis/> y b) <https://celebrity.land/maquilladora-talentosa-se-transforma-en-celebridades/>

- Tecnología compatible (o superior) con la Arquitectura nVIDIA Ampere, con codificador de 7ª generación y decodificador de 5ª generación (o superior)
- Tecnología VR Ready
- Resolución digital de salida de hasta 7680 x 4320 (o superior)
- Si es necesario una interacción con audio, se puede utilizar un dispositivo de audio virtual (VB-CABLE)

El proceso de creación de los modelos faciales se basa en múltiples imágenes/vídeos de los USUARIOS fidedignos a partir de las cuales se realiza el entrenamiento. Este entrenamiento requiere de varias fases, cada una de ellas con múltiples iteraciones, en las que se van optimizando las diferentes características del modelo. La decisión de cómo realizar el proceso de entrenamiento (fases, parámetros a optimizar en cada fase y número de iteraciones) se deja a criterio del laboratorio al ser dependiente de los datos de entrada. El laboratorio deberá realizar una captura del vídeo de deepfake con los modelos entrenados y acreditar un máximo de 60 de parecido con respecto a los USUARIOS fidedignos empleando la herramienta CCN_MATCH.

3.1 ELECCIÓN DEL TIPO DE CÁMARA

41. En caso de que el fabricante no imponga ninguna limitación en lo que respecta a la calidad de la cámara, se utilizará una cámara que pueda capturar imágenes con resolución 0,9 megapíxeles en rango visible a 50 Hz, como cámara de peor calidad.
42. Si el fabricante impone alguna limitación en la guía de operación del TOE, se deberá utilizar la cámara de menor calidad impuesta por el fabricante.

4 PRUEBAS DE FUNCIONALIDAD DEL TOE

43. El objetivo de estas PRUEBAS es verificar que la funcionalidad declarada por el fabricante se mantiene en el ESCENARIO de uso previsto para el producto en cuestión.
44. Esta fase es fundamental para poder, de forma rápida, descartar productos que, aun teniendo unos resultados de rendimiento positivos en la evaluación FRVT VISA-BORDER, no cumplen con la funcionalidad básica para las especificaciones del TOE declaradas en la Declaración de Seguridad.

4.1 P1.2M: COMPROBAR VERIFICACIÓN CORRECTA BAJO DISTINTOS ENTORNOS

4.1.1 DESCRIPCIÓN

45. El objetivo es verificar que el TOE funciona correctamente en los casos habituales de uso, suponiendo un uso cooperativo, por parte del USUARIO fidedigno.
46. Para ello se ejecutará el proceso de reconocimiento, siguiendo las indicaciones del manual de uso del TOE, frente a una variedad de ESCENARIOS.

4.1.2 ESCENARIOS

47. Se contemplan los siguientes ESCENARIOS a utilizar durante esta PRUEBA:

- **E.1.2.1:** El SUJETO utilizará cooperativamente el TOE teniendo a su espalda un ESCENARIO dinámico sin personas. Es decir, se proyectará una secuencia de **vídeo** continuo (sin cortes entre fotogramas) en el que no aparezcan individuos, pero en el que haya movimiento (por ejemplo, un **vídeo** que muestre un paisaje panorámico, o una oficina vacía, donde la cámara se mueva de un extremo al otro del paisaje, pudiendo volver al inicio). El **vídeo** podrá ser de interiores (por ejemplo, una oficina) o de exteriores (por ejemplo, un paisaje montañoso o una ciudad). El **vídeo** debe durar, como mínimo, el tiempo que pueda llegar a durar cada uno de los ENSAYOS.
- **E.1.2.2:** El SUJETO utilizará cooperativamente el TOE teniendo a su espalda un ESCENARIO dinámico (como el del E.1.2.1), pero en el que ahora aparezcan personas, algunas de las cuales deben, temporalmente, mirar en dirección a la cámara. Algunas de esas personas que aparezcan, deberán ser los USUARIOS fidedignos que se utilizarán en las PRUEBAS. El **vídeo** podrá ser de interiores (por ejemplo, una oficina) o de exteriores (por ejemplo, un paisaje montañoso o una ciudad). El **vídeo** debe durar, como mínimo, el tiempo que pueda llegar a durar cada uno de los ENSAYOS.

4.1.3 MATERIALES

48. Para todos los ENSAYOS a realizar en esta PRUEBA, se utilizará el siguiente material:

- Un dispositivo de captura, que será la cámara, de rango visible, con peor resolución y menor capacidad de autoenfoco que soporte el fabricante del TOE dentro de las restricciones declaradas en la guía de operación.
- **Un equipo de retroproyección o televisor de gran formato**, de los definidos en la sección 3.
- El documento de identificación con el que se va a realizar la evaluación para cada uno de los USUARIOS fidedignos. El tipo de documento tendrá que haber sido declarado como aceptado por el solicitante en la Declaración de Seguridad y guía de operación del TOE.

4.1.4 SUJETOS

49. Los SUJETOS a formar parte de esta PRUEBA serán:

- Un mínimo de **seis (6)** USUARIOS fidedignos
- Cada uno de los USUARIOS dispondrá del documento de identificación considerado para la evaluación.
- Por lo tanto, el número de SUJETOS será 6.

4.1.5 ENSAYOS

50. Se realizarán un mínimo de ENSAYOS, para cada SUJETO y ESCENARIO, dado por la constante MIN_ENSAYOS.

51. Los pasos a seguir para realizar cada ENSAYO son:

- 1) El laboratorio pone en marcha el ESCENARIO y prepara al SUJETO indicándole como debe actuar y dónde colocarse.
- 2) El SUJETO prepara su propio documento de identificación para usarlo según la guía de operación evaluada del TOE.
- 3) El SUJETO procederá a identificarse de acuerdo a lo que indica la guía de operación evaluada del TOE. Dicho modo de interacción puede contener acciones que se utilicen como prueba de vida.
- 4) El SUJETO espera el resultado del TOE y el laboratorio apuntará el resultado obtenido, incrementando el número de EQUIVALENTES, DISTINTOS o ERRORES_SUJETO según corresponda.
- 5) El SUJETO sale parcialmente de la interacción con el TOE (por ejemplo, deja de mirar a la cámara y mueve de forma apreciable su cuerpo para asegurarse que el siguiente ENSAYO es una interacción distinta).
- 6) Si en el ENSAYO para ese SUJETO se ha superado el número de ERRORES_SUJETO dado por el umbral MAX_ERRORES_SUJETO, se irá al paso 9), incrementando la variable que acumule los ERRORES_PRUEBA. Si dicha variable supera el umbral dado por MAX_ERRORES_PRUEBA, se finalizarán los ENSAYOS para toda la PRUEBA, y se marcará la PRUEBA con FALLA.

- 7) Si en el ENSAYO para ese SUJETO se ha superado el número de DISTINTOS dados por el umbral MAX_DISTINTOS_SUJETO, se irá al paso 9, incrementando la variable que acumula los FALLA_SUJETOS. Si dicha variable supera el umbral dado por MAX_FALLA_SUJETOS, se finalizarán los ENSAYOS para toda la PRUEBA, y se marcará la PRUEBA con FALLA.
- 8) Se vuelve al paso 3, para repetir el proceso, hasta alcanzar un mínimo de MIN_ENSAYOS para ese SUJETO.
- 9) Se cambia al siguiente SUJETO, y se vuelve al paso 1.

4.1.6 INTENTOS

52. Para cada ENSAYO se establece un número máximo de MAX_INTENTOS, para lograr una captura adecuada de los datos de entrada (es decir, imagen/**vídeo** facial y documento), de forma que el TOE proporcione un resultado a la verificación, ya sea un EQUIVALENTE o un DISTINTO.
53. Si se supera ese número MAX_INTENTOS para un ENSAYO, se dará un ERROR.

4.1.7 PARÁMETROS

54. Atendiendo a los siguientes parámetros, el número total de ENSAYOS a realizar en esta PRUEBA es de 120:
 - MAX_DISTINTOS_ESCENARIO = 3
 - MAX_DISTINTOS_PRUEBA = 6
 - MAX_DISTINTOS_SUJETO = 3
 - MAX_ERRORES_PRUEBA = 3
 - MAX_ERRORES_SUJETO = 3
 - MAX_FALLA_SUJETOS = 2
 - MAX_INTENTOS = 3 (si el TOE permite un número de intentos menor que **3** se seleccionará dicho valor)
 - MIN_ENSAYOS = 10
 - MIN_ESCENARIOS = 2
 - MIN_SUJETOS = 6

4.1.8 CRITERIOS DE DECISIÓN Y UMBRAL DE ACEPTACIÓN

55. Los criterios se pueden observar en esta tabla. Caso de no darse ninguno de los casos la PRUEBA se calificará como **PASA**.

VARIABLE	OP.	UMBRAL	VEREDICTO
Número de ERRORES_PRUEBA	>	MAX_ERRORES_PRUEBA	FALLA
Número de FALLA_SUJETOS	>	MAX_FALLA_SUJETOS	FALLA
Número de DISTINTOS_PRUEBA	>	MAX_DISTINTOS_PRUEBA	FALLA
Número de	>	MAX_DISTINTOS_ESCENARIO	FALLA

DISTINTOS_ESCENARIO			
---------------------	--	--	--

Tabla 1: Criterios de decisión para P1.2

4.1.9 ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN

56. Adicionalmente a lo indicado en CCN-STIC-2004, el Informe Técnico de Evaluación deberá incluir un anexo con la siguiente información:

- Número y descripción (con fotografías/**vídeos**) de los ESCENARIOS.
- Número y tipo de los documentos utilizados. Se entregarán imágenes del documento con los datos personales anonimizados a excepción de la fotografía que contiene.
- Número y tipología (edad, sexo, etc.) de los USUARIOS utilizados. **Se deberán documentar los valores de parecido entre los USUARIOS fidedignos obtenidos en la herramienta CCN_MATCH.**
- Número total de SUJETOS ensayados.
- Número de ENSAYOS realizados.
- Una tabla con la información de ERRORES_SUJETO, EQUIVALENTES y DISTINTOS para cada SUJETO, ENSAYO y ESCENARIO. Un ejemplo puede ser la siguiente tabla:

SUJETO	ENSAYO	E.1.2.1			E.1.2.2			TOTALES	
		EQUIV.	ERROR	DIST.	EQUIV.	ERROR	DIST.	ERROR	DIST.
S1	E1								
S1	E2								
S1	En								
S2	E1								
...	...								
Sn									
TOTALES									

– Tabla 2: Ejemplo de tabla resumen de los resultados parciales de P1.2M

- Resultado de la aplicación de los criterios.

4.2

P1.6: COMPROBAR QUE EL PRODUCTO VERIFICA LA PRUEBA DE VIDA

4.2.1 DESCRIPCIÓN

57. Para facilitar la detección de ataques de presentación, el TOE debe incorporar mecanismos específicos para detectar una prueba de vida del SUJETO al que se está verificando. Un ejemplo puede ser, siguiendo una metodología de *challenge-response*, que el TOE requiera al SUJETO algún tipo de movimiento (por ejemplo, un pestañeo, o girar la cabeza), al que tenga que reaccionar el SUJETO correctamente.
58. Por lo tanto, esta PRUEBA verificará el funcionamiento de este tipo de mecanismo, que deberá estar documentado en la guía de operación evaluada del TOE. En la PRUEBA se forzará a usar el sistema sin presentar dicha prueba de vida, para ver si la verificación puede llevarse a cabo. En caso de realizarse la verificación, resultará en un FALLA de esta PRUEBA.
59. Los ENSAYOS se realizarán siempre con USUARIOS fidedignos, comportándose fielmente a lo indicado en la guía de operación evaluada del TOE, salvo por el hecho de la presentación de dicha prueba de vida.
60. Únicamente se realizará esta PRUEBA para los mecanismos reflejados en la documentación técnica del TOE aportada por el fabricante y declarados en la Declaración de Seguridad, siempre y cuando estos mecanismos impliquen una interacción específica del usuario con el TOE. Dichos mecanismos se especificarán en el Informe Técnico de Evaluación.
61. Es importante tener en cuenta que la no presentación de la prueba de vida, puede llevar a que el TOE quede en una espera infinita, por lo que se establecerá un TIMEOUT por ENSAYO, pasado el mismo, se dará el ENSAYO como un ERROR. Este es un resultado válido (el deseable del TOE), por lo que no hay que repetir un nuevo INTENTO.
62. También se puede dar el caso de que, al no presentar la prueba de vida, el TOE determine que hay un ERROR en el ENSAYO. Este es un resultado válido (el deseable del TOE), por lo que no hay que repetir un nuevo INTENTO.
63. En esta PRUEBA, los resultados deseables, a diferencia de la PRUEBA P1.2M, son los de ERROR y los de DISTINTO. El resultado no deseable será el de EQUIVALENTE. Esto implica que, en los diagramas de flujo de la sección 2.3, se han de hacer los cambios correspondientes entre EQUIVALENTES y DISTINTOS, ubicando las comparaciones de EQUIVALENTES, en las ramas en las que puede dar que la prueba de un FALLA. De la misma forma, las variables DISTINTOS_ESCENARIO, DISTINTOS_PRUEBA y DISTINTOS_SUJETO, cambiarán por EQUIVALENTES_ESCENARIO, EQUIVALENTES_PRUEBA y EQUIVALENTES_SUJETO. De forma análoga, las constantes MAX_DISTINTOS_ESCENARIO, MAX_DISTINTOS_PRUEBA y MAX_DISTINTOS_SUJETO, se cambiarán por MAX_EQUIVALENTES_ESCENARIO, MAX_EQUIVALENTES_PRUEBA y MAX_EQUIVALENTES_SUJETO.

4.2.2 ESCENARIOS

64. Se contempla sólo el siguiente ESCENARIO a utilizar durante esta PRUEBA:

- E.1.6.1: El SUJETO utilizará cooperativamente el TOE teniendo a su espalda un ESCENARIO dinámico (como el del E.1.2.2), pero en el que se asegure que aparezcan en torno a 5 o 6 rostros de personas, algunas de las cuales deben, temporalmente, mirar en dirección a la cámara. Algunas de esas personas que aparezcan, deberán ser los USUARIOS fidedignos que se utilizarán en las PRUEBAS. El vídeo podrá ser de interiores (por ejemplo, una oficina) o de exteriores (por ejemplo, un paisaje montañoso o una ciudad). El vídeo debe durar, como mínimo, el tiempo que pueda llegar a durar cada uno de los ENSAYOS.

4.2.3 MATERIALES

65. Para todos los ENSAYOS a realizar en esta PRUEBA, se utilizará el siguiente material:

- El dispositivo de captura será la cámara, de rango visible, con peor resolución y menor capacidad de autoenfoco de los declarados en la guía de operación evaluada.
- **Equipo de proyección y/o pantallas de gran formato**, definido la sección 3. donde emular el fondo en cada uno de los ESCENARIOS. En todo caso, en la captura de la imagen/vídeo del sujeto, no deben verse los bordes de dicho sistema de proyección y/o pantalla.
- Un documento por USUARIO fidedigno del tipo de documento de identidad considerado en la evaluación. Simplemente se utiliza para poder realizar la PRUEBA, ya que lo que se verifica no es el resultado de la identificación sino la realización o no de esta.

4.2.4 SUJETOS

66. Los SUJETOS a formar parte de esta PRUEBA serán:

- Un mínimo de dos (2) USUARIOS fidedignos.
- Cada uno de los USUARIOS dispondrá del documento de identificación considerado para la evaluación.
- Por lo tanto, el número de SUJETOS será 2.

4.2.5 ENSAYOS

67. Se realizarán un mínimo de ENSAYOS, para cada SUJETO y ESCENARIO, dado por la constante MIN_ENSAYOS.

68. Los pasos a seguir para realizar cada ENSAYO son:

- 1) El laboratorio pone en marcha el ESCENARIO y prepara al SUJETO indicándole como debe actuar y dónde colocarse. En esta explicación es preciso enfatizar al SUJETO que no debe reaccionar a la prueba de vida, que en la mayoría de los casos será que se quede lo más quieto posible.

- 2) El SUJETO prepara su propio documento de identificación para usarlo según la guía de operación evaluada.
- 3) El SUJETO procederá a identificarse de acuerdo a lo que indica en la guía de operación evaluada del TOE, salvo en lo que refiera a la prueba de vida, que tendrá que ignorarla. El SUJETO deberá quedarse quieto hasta que el TOE dé un resultado (ya sea EQUIVALENTE, DISTINTO o ERROR), o pase el tiempo dado por TIMEOUT, lo que pase antes.
- 4) Si el TOE resulta en un error no provocado por el TIMEOUT, sino por cualquier otro motivo, se repetirá el INTENTO. Esto se repetirá hasta llegar al número MAX_INTENTOS, resultando en ERROR para dicho ENSAYO.
- 5) Si pasado el tiempo dado por TIMEOUT, el TOE no ha dado una respuesta u error, resultará en un ERROR para dicho ENSAYO.
- 6) El laboratorio apuntará el resultado obtenido, incrementando el número de EQUIVALENTES, DISTINTOS o ERRORES_SUJETO según corresponda.
- 7) El SUJETO sale parcialmente de la interacción con el TOE (por ejemplo, deja de mirar a la cámara y mueve de forma apreciable su cuerpo para asegurarse que el siguiente ENSAYO es una interacción distinta)
- 8) Si en el ENSAYO para ese SUJETO, se ha superado el número de EQUIVALENTES dado por el umbral MAX_EQUIVALENTES_SUJETO, se irá al paso 9, incrementando la variable que acumula los FALLA_SUJETOS. Si dicha variable supera el umbral dado por MAX_FALLA_SUJETOS, se finalizarán los ENSAYOS para toda la PRUEBA, y se marcará la PRUEBA con FALLA.
- 9) Se vuelve al paso 3, para repetir el proceso, hasta alcanzar un mínimo de MIN_ENSAYOS para ese SUJETO.
- 10) Se cambia al siguiente SUJETO, y se vuelve al paso 1.

4.2.6 INTENTOS

69. Para cada ENSAYO se establece un número máximo de MAX_INTENTOS, para lograr una captura adecuada de los datos de entrada (es decir, imagen/**video** facial y documento), de forma que el TOE proporcione un resultado a la verificación, ya sea un EQUIVALENTE o un DISTINTO.
70. Si se supera ese número MAX_INTENTOS para un ENSAYO, se dará un ERROR.

4.2.7 PARÁMETROS

71. Atendiendo a los siguientes parámetros, el número total de ENSAYOS a realizar en esta PRUEBA es de 10:
 - MAX_DISTINTOS_ESCENARIO = No aplicable
 - MAX_DISTINTOS_PRUEBA = No aplicable
 - MAX_DISTINTOS_SUJETO = No aplicable
 - MAX_EQUIVALENTES_PRUEBA = 1

- MAX_EQUIVALENTES_SUJETO = 1
- MAX_ERRORES_PRUEBA = No aplicable
- MAX_ERRORES_SUJETO = No aplicable
- MAX_FALLA_SUJETOS = 1
- MAX_INTENTOS = 3
- MIN_ENSAYOS = 5
- MIN_ESCENARIOS = 1
- MIN_SUJETOS = 2
- TIMEOUT = 20 segundos (salvo que el manual del TOE indique un valor superior)

72. Atendiendo a estos parámetros, el número total de ENSAYOS a realizar en esta PRUEBA es de 10.

4.2.8 CRITERIOS DE DECISIÓN Y UMBRAL DE ACEPTACIÓN

73. Los criterios se pueden observar en esta tabla. Caso de no darse ninguno de los casos la PRUEBA se calificará como **PASA**.

VARIABLE	OP.	UMBRAL	VEREDICTO
Número de FALLA_SUJETOS	>	MAX_FALLA_SUJETOS	FALLA
Número de EQUIVALENTES_PRUEBA	>	MAX_EQUIVALENTES_PRUEBA	FALLA

Tabla 3: Criterios de decisión para P1.6

4.2.9 ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN

74. Adicionalmente a lo indicado en CCN-STIC-2004, el Informe Técnico de Evaluación debe incluir la siguiente información:

- Número y descripción (con fotografías/**vídeos**) de los ESCENARIOS.
- Número y tipo de los documentos utilizados. Se entregarán imágenes del documento con los datos personales anonimizados a excepción de la fotografía que contiene.
- **Número y tipología (edad, sexo, etc.) de los USUARIOS utilizados. Se deberán documentar los valores de parecido entre los USUARIOS fidedignos obtenidos en la herramienta CCN_MATCH.**
- Número total de SUJETOS ensayados.
- Número de ENSAYOS realizados.
- TIMEOUT utilizado, y si éste ha sido determinado por el manual del TOE, o por el requisito puesto en este documento.

- Una tabla con la información de ERRORES_SUJETO, EQUIVALENTES y DISTINTOS para cada SUJETO, ENSAYO y ESCENARIO. Un ejemplo puede ser la siguiente tabla:

SUJETO	ENSAYO	E.1.6.1			TOTALES	
		EQUIVALENTE	ERROR	DISTINTO	EQUIVALENTE	ERROR.
S1	E1					
S1	...					
S1	EN					
...						
Sn						
TOTALES						

Tabla 4: Ejemplo de tabla resumen de los resultados parciales de P1.6

- Resultado de la aplicación de los criterios.

5 PRUEBAS DE DETECCIÓN DE ATAQUES DE PRESENTACIÓN

75. El objeto de estas PRUEBAS es comprobar si el TOE es susceptible de ser atacado en el proceso de presentación de la muestra biométrica. Los ataques realizados en esta fase podrían ser tanto de suplantación como de ofuscación. Sin embargo, en esta instrucción técnica, las PRUEBAS se centrarán en los ataques de suplantación, es decir, que el atacante utilice artefactos para intentar suplantar a un USUARIO fidedigno. Las PRUEBAS se dividen en subgrupos en función del tipo de artefacto utilizado.
76. Los atacantes deben tener listos los ataques antes de iniciar el proceso **y disponer del documento del USUARIO fidedigno a atacar**, de forma que no haya retardos a la hora de presentar la muestra facial.
77. A la hora de realizar el cálculo del número de verificaciones, el número de artefactos final utilizados en la PRUEBA será el resultado de multiplicar el número de USUARIOS fidedignos por el número de tipos de artefactos que se utilizan.
78. Para cada una de las PRUEBAS descritas se plantea un número máximo de iteraciones por PRUEBA. No obstante, se considerará que el ataque ha tenido éxito la primera vez que el test de penetración (ENSAYO) haya tenido éxito, por lo que no será necesario repetir más ENSAYOS para esa PRUEBA.
79. Para aquellos productos que permitan varios INTENTOS por verificación en caso de que se produzcan ERRORES_SUJETO en la identificación, se considerará en cada PRUEBA un límite máximo de INTENTOS, iniciándose un nuevo ENSAYO si se ha alcanzado ese límite.
80. Para este tipo de PRUEBAS, la obtención de un PASA, es decir, un ataque exitoso contra el TOE hará fallar la evaluación de seguridad.

5.1 CARACTERÍSTICAS COMUNES A LAS PRUEBAS

81. Para facilitar la lectura, teniendo en cuenta que muchas características de las PRUEBAS son comunes, se van a reflejar en este apartado todas ellas. Todas estas características son aplicables a todas las PRUEBAS, salvo que en la PRUEBA se especifique algo diferente.

5.1.1 ESCENARIOS

82. Se contempla sólo un ESCENARIO a utilizar durante la PRUEBA, el cual es el mismo que el especificado en 4.1.2.

5.1.2 MATERIALES

83. Para todos los ENSAYOS a realizar en las PRUEBAS, se utilizará el siguiente material, salvo que en la PRUEBA se especifique algo diferente:
 - El dispositivo de captura, salvo que se indique lo contrario en alguna PRUEBA, será la cámara, **de rango visible**, con peor resolución y menor capacidad de

autoenfoco de las soportadas por el fabricante del TOE e indicadas en la guía de operación del TOE. Es importante que si el TOE permite cámaras de rango visible, no se utilice una cámara de infrarrojo cercano (NIR), puesto que estas cámaras pueden directamente eliminar algunos de los artefactos usados en los ataques.

- **Equipo de proyección y/o pantallas de gran formato**, definido en la sección 3.
- Un documento (sin manipular) por USUARIO fidedigno del tipo de documento de identidad considerado en la evaluación.

5.1.3 INTENTOS

84. Para cada ENSAYO se establece un número máximo de MAX_INTENTOS, para lograr una captura adecuada de los datos de entrada (es decir, imagen/**video** facial y documento), de forma que el TOE proporcione un resultado a la verificación, ya sea un EQUIVALENTE o un DISTINTO.

85. Si se supera ese número MAX_INTENTOS para un ENSAYO, se dará un ERROR.

5.1.4 PARÁMETROS

- MAX_EQUIVALENTES_ESCENARIO = 0, es decir, cualquier verificación exitosa dará PASA en la PRUEBA.
- MAX_EQUIVALENTES_PRUEBA = 0, es decir, cualquier verificación exitosa dará PASA en la PRUEBA.
- MAX_EQUIVALENTES_SUJETO = 0, es decir, cualquier verificación exitosa dará PASA en la PRUEBA.
- MAX_PASA_SUJETOS = 0, es decir, cualquier SUJETO para el que se obtenga un resultado exitoso en la PRUEBA, dará un PASA en la PRUEBA.
- MAX_INTENTOS = 3
- MIN_ENSAYOS = 10
- MIN_ESCENARIOS = 1

5.1.5 CRITERIOS DE DECISIÓN Y UMBRAL DE ACEPTACIÓN

86. Los criterios se pueden observar en esta tabla. Caso de no darse ninguno de los casos la PRUEBA se calificará como **FALLA**.

VARIABLE	OP.	UMBRAL	VEREDICTO
Número de PASA_SUJETOS	>	MAX_PASA_SUJETOS	PASA
Número de EQUIVALENTES_PRUEBA	>	MAX_EQUIVALENTES_PRUEBA	PASA
Número de EQUIVALENTES_ESCENARIO	>	MAX_EQUIVALENTES_ESCENARIO O	PASA

Tabla 5: Criterios de decisión generales para las PRUEBAS de la Fase 3

87. Atendiendo a los parámetros definidos, de forma resumida se puede decir que, si un ENSAYO resulta en un EQUIVALENTE, dará un PASA en la PRUEBA, y por lo tanto la evaluación recibirá el veredicto de FALLA.

5.1.6 ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN

88. Adicionalmente a lo indicado en CCN-STIC-2004, el Informe Técnico de Evaluación debe incluir la siguiente información:

- Número y descripción (con fotografías/**vídeos**) de los ESCENARIOS.
- Número y tipo (con fotografías) de los documentos utilizados. Dichas fotografías deben ser inalteradas. Para la elaboración del ETR, se entregarán imágenes del documento con los datos personales anonimizados a excepción de la fotografía que contiene.
- Número y tipología (edad, sexo, etc.) con fotografías de los USUARIOS utilizados.
- En el caso de utilizar artefactos se aportará la siguiente información:
 - i. Descripción de cómo se ha realizado la preparación del artefacto.
 - ii. El esfuerzo requerido (conocimientos técnicos, tiempo de creación, coste, creación y preparación de instrumentos, etc.).
 - iii. Descripción de la fuente de características biométricas (si está basado en representaciones directas o indirectas de muestras o características biométricas, representaciones modificadas o manipuladas, sintéticas, etc.).
 - iv. Tiempo de entrenamiento y habituación, es decir, indicar el tiempo de ensayo necesario para utilizar y presentar un artefacto y el tiempo de entrenamiento y habituación del atacante. Este parámetro puede impactar en la eficacia de artefactos.
 - v. Duración del artefacto. Ciertos tipos de artefactos basados en materiales pueden tener un ciclo de vida de utilización, de tal forma que su eficacia se reduzca tras una o más presentaciones. Un baremo de aceptación de un artefacto puede estar marcado por su tiempo de vida o el número de presentaciones.
 - vi. Especificación de uso del artefacto. En función del parámetro que defina la duración del artefacto descrita en el apartado anterior, se describirá cual ha sido el uso del artefacto (tiempo, número de presentaciones anteriores)
 - vii. Evidencia del artefacto utilizado (imagen, **vídeo** o audio, según el caso).
- En el caso de que la prueba especifique unos umbrales mínimos de parecido entre el USUARIO fidedigno y el ATACANTE o el artefacto, se deberán documentar los valores de parecido obtenidos en la herramienta CCN_MATCH.

- Número total de SUJETOS ensayados.
- Número de ENSAYOS realizados.
- Una tabla con la información de ERRORES_SUJETO, EQUIVALENTES y DISTINTOS para cada SUJETO, ENSAYO y ESCENARIO. Un ejemplo puede ser la siguiente tabla:

SUJETO	ENSAYO	ESCENARIO			TOTALES	
		EQUIVALENTE	ERROR	DISTINTO	EQUIVALENTE	ERROR.
S1	E1					
S1	...					
S1	EN					
...						
Sn						
TOTALES						

Tabla 6: Ejemplo de tabla resumen de resultados parciales de cada PRUEBA - Fase 3

- Resultado de la aplicación de los criterios.

5.2 P3.1: ATAQUES DE PRESENTACIÓN DE IMPOSTOR

5.2.1 DESCRIPCIÓN

89. El objetivo de esta PRUEBA es comprobar que el TOE no es vulnerable a la suplantación de un USUARIO fidedigno por parte de un atacante con parecido al USUARIO fidedigno cuya comparación utilizando el *software* CCN_MATCH suministrado por el CCN no supere el umbral de 60.
90. Es importante tener en cuenta que el concepto de "parecido" aquí es entre el atacante y la foto del USUARIO fidedigno. Parámetros como altura, peso, edad, etc., no son de interés aquí.
91. La decisión de si dos imágenes son suficientemente parecidas, la proporcionará el software CCN_MATCH, definido en la sección 3.
92. Para la realización de esta PRUEBA en este TOE, el USUARIO fidedigno no es necesario que esté presente, sino que se disponga de su documento.
93. En esta PRUEBA el atacante se comportará siguiendo la guía de operación evaluada del TOE, incluyendo la prueba de vida que se solicite (en el caso de que haya), con la única variación de que el documento utilizado no será el suyo.
94. En líneas generales, esta PRUEBA se ejecuta de forma análoga a la P1.2M, salvo que, en este caso, el resultado deseable en cada ENSAYO es el de DISTINTO. El resultado no deseable será el de EQUIVALENTE.

5.2.2 MATERIALES

95. Para todos los ENSAYOS a realizar en esta PRUEBA, se utilizará el material especificado en 5.1.2, junto con el software CCN_MATCH, definido la sección 3.

5.2.3 SUJETOS

96. Los SUJETOS a formar parte de esta PRUEBA serán:

- Un mínimo de dos (2) documentos de identidad, del tipo considerado en la evaluación, de cada uno de los USUARIOS fidedignos seleccionados.
- Dos (2) ATACANTES, uno por USUARIO fidedigno.
- Por lo tanto, el número de SUJETOS será 2.

5.2.4 ENSAYOS

97. Se realizarán un mínimo de ENSAYOS, para cada SUJETO y ESCENARIO, dado por la constante MIN_ENSAYOS.

98. Los pasos a seguir para realizar cada ENSAYO son:

- 1) El laboratorio pone en marcha el ESCENARIO y prepara al SUJETO indicándole como debe actuar y dónde colocarse. Se le recuerda al atacante que tiene que ser lo más cooperativo posible con el TOE para ser reconocido, incluyendo una correcta ejecución de la prueba de vida (si se solicita).
- 2) El SUJETO prepara el documento del USUARIO fidedigno para usarlo según la guía de operación del TOE.
- 3) El SUJETO procederá a identificarse de acuerdo a lo que indica la guía de operación del TOE.
- 4) Si el TOE resulta en un resultado distinto de EQUIVALENTE o DISTINTO, se procederá a repetir el INTENTO. Esto se hará hasta llegar al número MAX_INTENTOS, resultando en ERROR para dicho ENSAYO si se supera dicho número.
- 5) El laboratorio apuntará el resultado obtenido, incrementando el número de EQUIVALENTES, DISTINTOS o ERRORES_SUJETO según corresponda.
- 6) El SUJETO sale parcialmente de la interacción con el TOE (por ejemplo, deja de mirar a la cámara y mueve de forma apreciable su cuerpo para asegurarse que el siguiente ENSAYO es una interacción distinta).
- 7) Si en el ENSAYO para ese SUJETO, se ha superado el número de EQUIVALENTES dado por el umbral MAX_EQUIVALENTES_SUJETO, se irá al paso 9, incrementando la variable que acumula los PASA_SUJETOS. Si dicha variable supera el umbral dado por MAX_PASA_SUJETOS, se finalizarán los ENSAYOS para toda la PRUEBA, y se marcará la PRUEBA con PASA.
- 8) Se vuelve al paso 2, para repetir el proceso, hasta alcanzar un mínimo de MIN_ENSAYOS para ese SUJETO.
- 9) Se cambia al siguiente SUJETO, y se vuelve al paso 1.

5.2.5 PARÁMETROS

99. A los parámetros especificados en 5.1.4 se añaden los siguientes:

MIN_SUJETOS = 2

100. Atendiendo a estos parámetros, el número total de ENSAYOS a realizar en esta PRUEBA es de 20.

5.2.6 ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN

101. El Informe Técnico de Evaluación debe incluir lo indicado en CCN-STIC-2004, así como lo especificado en 5.1.6.

5.3 P3.3.2: ATAQUES DE PRESENTACIÓN USANDO VÍDEOS

5.3.1 DESCRIPCIÓN

102. El objetivo de esta PRUEBA es comprobar que el TOE no es vulnerable a la suplantación de un USUARIO fidedigno por parte de un atacante que utilice un vídeo de un USUARIO fidedigno, mientras interactuaba con el TOE previamente.

103. Será importante lograr un sincronismo adecuado entre el vídeo y el uso del TOE para que la presentación de la prueba de vida en el vídeo tenga sentido contextual con el uso del TOE.

104. En líneas generales, esta PRUEBA se ejecuta de forma análoga a la P3.1, donde el resultado deseable en cada ENSAYO es el de DISTINTO o ERROR, mientras que el resultado no deseable será el de EQUIVALENTE.

5.3.2 MATERIALES

105. Para todos los ENSAYOS a realizar en esta PRUEBA, se utilizará el material especificado en 5.1.2, junto con **los vídeos** definidos en la sección 3.

5.3.3 SUJETOS

106. Los SUJETOS a formar parte de esta PRUEBA serán:

- Un documento de identidad, del tipo considerado en la evaluación, de cada uno de seis (6) USUARIOS fidedignos.
- Dos (2) ATACANTES. Cada uno de ellos atacará a la mitad de los USUARIO fidedignos. El reparto lo realizará el laboratorio según su propio criterio.
- Por lo tanto, el número de SUJETOS será 6, correspondiente a cada pareja atacante-fidedigno.

5.3.4 ENSAYOS

107. Se realizarán un mínimo de ENSAYOS, para cada SUJETO y ESCENARIO, dado por la constante MIN_ENSAYOS.

108. Los pasos a seguir para realizar cada ENSAYO son:

- 1) El laboratorio pone en marcha el ESCENARIO. Se le recuerda al atacante que tiene que conseguir, en cada ENSAYO, lograr un sincronismo adecuado entre los vídeos reproducidos y la interacción real con el TOE.

- 2) El atacante prepara el **vídeo** correspondiente al USUARIO fidedigno, así como el documento de dicho USUARIO fidedigno para usarlo según la guía de operación del TOE.
- 3) El SUJETO procederá a identificarse. Para ello, el atacante presentará al TOE el documento y posteriormente saldrá de la escena para que el TOE capte únicamente el vídeo del USUARIO fidedigno.
- 4) Si el TOE resulta en un resultado distinto de EQUIVALENTE o DISTINTO, se procederá a repetir el INTENTO. Esto se hará hasta llegar al número MAX_INTENTOS, resultando en ERROR para dicho ENSAYO si se supera dicho número.
- 5) El laboratorio apuntará el resultado obtenido, incrementando el número de EQUIVALENTES, DISTINTOS o ERRORES_SUJETO según corresponda.
- 6) Si el resultado es un ERROR o un DISTINTO, el atacante analizará cómo ha ido el ENSAYO, y plantea las modificaciones oportunas para conseguir un EQUIVALENTE en el siguiente ENSAYO.
- 7) Si en el ENSAYO para ese SUJETO, se ha superado el número de EQUIVALENTES dado por el umbral MAX_EQUIVALENTES_SUJETO, se irá al paso 9, incrementando la variable que acumula los PASA_SUJETOS. Si dicha variable supera el umbral dado por MAX_PASA_SUJETOS, se finalizarán los ENSAYOS para toda la PRUEBA, y se marcará la PRUEBA con PASA.
- 8) Se vuelve al paso 2, para repetir el proceso, hasta alcanzar un mínimo de MIN_ENSAYOS para ese SUJETO.
- 9) Se cambia al siguiente SUJETO, y se vuelve al paso 1.

5.3.5 INTENTOS

109. Para cada ENSAYO se establece un número máximo de MAX_INTENTOS, para lograr una captura adecuada de los datos de entrada (es decir, imagen/**vídeo** facial y documento), de forma que el TOE proporcione un resultado de la verificación, ya sea un EQUIVALENTE o un DISTINTO.

110. Si el TOE emplea distintos tipos de prueba de vida (ej. sonreír, gestos, movimientos, etc.), y la solicitada en el INTENTO no se corresponde con la mostrada en el **vídeo**, no se considerará que se ha ejecutado dicho INTENTO, no incrementándose su cantidad. Se repetirá el INTENTO esperando que esta vez la prueba de vida solicitada pueda ser la misma que la del **vídeo**. Se recomienda al laboratorio emplear para este tipo de ENSAYO muestras abiertas del TOE que permitan controlar el tipo de prueba de vida.

111. Si se supera ese número MAX_INTENTOS para un ENSAYO, se dará un ERROR.

5.3.6 PARÁMETROS

112. A los parámetros especificados en 5.1.4, se añaden los siguientes:

MIN_SUJETOS = 6

113. Atendiendo a estos parámetros, el número total de ENSAYOS a realizar en esta PRUEBA es de 60.

5.3.7 ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN

114. Adicionalmente a lo indicado en CCN-STIC-2004 y en 5.1.6, el Informe Técnico de Evaluación debe incluir el número y descripción de los artefactos utilizados (los vídeos). Los vídeos se entregarán junto con el ETR.

5.4 P3.3.3: ATAQUES DE PRESENTACIÓN USANDO MÁSCARAS DE MUY BAJO COSTE

5.4.1 DESCRIPCIÓN

115. El objetivo de esta PRUEBA es comprobar que el TOE no es vulnerable a la suplantación de un USUARIO fidedigno por parte de un atacante que utilice una máscara de bajo coste (por ejemplo, de papel) como artefacto. En el caso en que portar la máscara de papel impida ofrecer la prueba de vida requerida por el producto, se considerará que el resultado de esta PRUEBA sería FALLA.

116. En líneas generales, esta PRUEBA se ejecuta de forma análoga a la P3.1, donde el resultado deseable en cada ENSAYO es el de DISTINTO o ERROR, mientras que el resultado no deseable será el de EQUIVALENTE.

5.4.2 MATERIALES

117. Para todos los ENSAYOS a realizar en esta PRUEBA, se utilizará el material especificado en 5.1.2, junto con **las máscaras de bajo coste** definidas la sección 3.

5.4.3 SUJETOS

118. Los SUJETOS a formar parte de esta PRUEBA serán:

- Un documento de identidad, del tipo considerado en la evaluación, de cuatro (4) USUARIOS fidedignos.
- Dos (2) ATACANTES. Cada uno de ellos atacará a la mitad de los USUARIOS fidedignos. El reparto lo realizará el laboratorio según su propio criterio.
- Dos (2) artefactos para cada uno de los USUARIOS fidedignos, de acuerdo a las máscaras descritas en la sección 3.
- Por lo tanto, el número mínimo de SUJETOS será 8, correspondiente a cada pareja atacante-artefacto.

5.4.4 ENSAYOS

119. Se realizarán un mínimo de ENSAYOS, para cada SUJETO y ESCENARIO, dado por la constante MIN_ENSAYOS.

120. Los pasos a seguir para realizar cada ENSAYO son:

- 1) El laboratorio pone en marcha el ESCENARIO y prepara al SUJETO indicándole como debe actuar y dónde colocarse. Se le recuerda al atacante que tiene que ser lo más cooperativo posible con el TOE para ser reconocido, incluyendo una correcta ejecución de la prueba de vida (si se solicita).
- 2) El SUJETO prepara el documento del USUARIO fidedigno para usarlo según el manual del TOE.
- 3) El SUJETO procederá a identificarse de acuerdo a lo que indica el manual de uso del TOE, con la excepción de que llevará puesta la máscara lo más correctamente posible.
- 4) Si el TOE resulta en un resultado distinto de EQUIVALENTE o DISTINTO, se procederá a repetir el INTENTO. Esto se hará hasta llegar al número MAX_INTENTOS, resultando en ERROR para dicho ENSAYO si se supera dicho número.
- 5) El laboratorio apuntará el resultado obtenido, incrementando el número de EQUIVALENTES, DISTINTOS o ERRORES_SUJETO según corresponda.
- 6) El SUJETO sale parcialmente de la interacción con el TOE (por ejemplo, deja de mirar a la cámara y mueve de forma apreciable su cuerpo para asegurarse que el siguiente ENSAYO es una interacción distinta)
- 7) Si en el ENSAYO para ese SUJETO, se ha superado el número de EQUIVALENTES dado por el umbral MAX_EQUIVALENTES_SUJETO, se irá al paso 9, incrementando la variable que acumula los PASA_SUJETOS. Si dicha variable supera el umbral dado por MAX_PASA_SUJETOS, se finalizarán los ENSAYOS para toda la PRUEBA, y se marcará la PRUEBA con PASA.
- 8) Se vuelve al paso 3, para repetir el proceso, hasta alcanzar un mínimo de MIN_ENSAYOS para ese SUJETO.
- 9) Se cambia al siguiente SUJETO, y se vuelve al paso 1.

5.4.5 PARÁMETROS

121. A los parámetros especificados en 5.1.4, se añaden los siguientes:

MIN_SUJETOS = 8.

122. Atendiendo a estos parámetros, el número total de ENSAYOS a realizar en esta PRUEBA es de 80.

5.4.6 ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN

123. Adicionalmente a lo indicado en CCN-STIC-2004 y en 5.1.6, el Informe Técnico de Evaluación debe incluir el número y tipo (con fotografías), de los artefactos utilizados (las máscaras)

5.5 P3.3.4: ATAQUES DE PRESENTACIÓN USANDO MÁSCARAS AVANZADAS

5.5.1 DESCRIPCIÓN

124.El objetivo de esta PRUEBA es comprobar que el TOE no es vulnerable a la suplantación de un USUARIO fidedigno por parte de un atacante que utilice una máscara avanzada como artefacto. En el caso en que portar la máscara impida ofrecer la prueba de vida requerida por el producto, se considerará que esta PRUEBA no aplica.

125.En líneas generales, esta PRUEBA se ejecuta de forma análoga a la P3.3.3, donde el resultado deseable en cada ENSAYO es el de DISTINTO o ERROR, mientras que el resultado no deseable será el de EQUIVALENTE.

5.5.2 MATERIALES

126.Para todos los ENSAYOS a realizar en esta PRUEBA, se utilizará:

127.El material especificado en 5.1.2, relativo a dispositivo de captura y equipo de proyección y/o pantalla de gran formato junto con, al menos, las máscaras avanzadas, definidas en la sección 3 y sus correspondientes documentos de identificación.

5.5.3 SUJETOS

128.Los SUJETOS a formar parte de esta PRUEBA serán:

- Un documento de identidad, del tipo considerado en la evaluación, de dos (2) USUARIOS fidedignos.
- Dos (2) ATACANTES. Cada uno de ellos atacará a un USUARIO fidedigno. La correspondencia la realizará el laboratorio según su propio criterio.
- Si para los USUARIOS fidedignos, se prepara más de un artefacto (más de una máscara), se tomarán como SUJETOS adicionales.
- Por lo tanto, el número mínimo de SUJETOS será 2, correspondiente a cada pareja atacante-artefacto de fidedigno.

5.5.4 ENSAYOS

129.Se realizarán un mínimo de ENSAYOS, para cada SUJETO y ESCENARIO, dado por la constante MIN_ENSAYOS.

130.Los pasos a seguir para realizar cada ENSAYO son:

- 1) El laboratorio pone en marcha el ESCENARIO y prepara al SUJETO indicándole como debe actuar y dónde colocarse. Se le recuerda al atacante que tiene que ser lo más cooperativo posible con el TOE para ser reconocido, incluyendo una correcta ejecución de la prueba de vida (si se solicita).
- 2) El SUJETO prepara el documento del USUARIO fidedigno para usarlo según la guía de operación del TOE.

- 3) El SUJETO procederá a identificarse de acuerdo a lo que indica el manual de uso del TOE, con la excepción de que llevará puesta la máscara lo más correctamente posible.
- 4) Si el TOE resulta en un resultado distinto de EQUIVALENTE o DISTINTO, se procederá a repetir el INTENTO. Esto se hará hasta llegar al número MAX_INTENTOS, resultando en ERROR para dicho ENSAYO si se supera dicho número.
- 5) El laboratorio apuntará el resultado obtenido, incrementando el número de EQUIVALENTES, DISTINTOS o ERRORES_SUJETO según corresponda.
- 6) El SUJETO sale parcialmente de la interacción con el TOE (por ejemplo, deja de mirar a la cámara y mueve de forma apreciable su cuerpo para asegurarse que el siguiente ENSAYO es una interacción distinta)
- 7) Si en el ENSAYO para ese SUJETO, se ha superado el número de EQUIVALENTES dado por el umbral MAX_EQUIVALENTES_SUJETO, se irá al paso 9, incrementando la variable que acumula los PASA_SUJETOS. Si dicha variable supera el umbral dado por MAX_PASA_SUJETOS, se finalizarán los ENSAYOS para toda la PRUEBA, y se marcará la PRUEBA con PASA.
- 8) Se vuelve al paso 2, para repetir el proceso, hasta alcanzar un mínimo de MIN_ENSAYOS para ese SUJETO.
- 9) Se cambia al siguiente SUJETO, y se vuelve al paso 1.

5.5.5 PARÁMETROS

131.A los parámetros especificados en 5.1.4, se añaden los siguientes:

MIN_SUJETOS = 2

132.Atendiendo a estos parámetros, el número mínimo de ENSAYOS a realizar en esta PRUEBA es de 20.

5.5.6 ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN

133.Adicionalmente a lo indicado en CCN-STIC-2004 y en 5.1.6, el Informe Técnico de Evaluación debe incluir la siguiente información del número y tipo (con fotografías), de los artefactos utilizados (las máscaras).

5.6 P3.3.5: ATAQUES DE PRESENTACIÓN USANDO MAQUILLAJE

5.6.1 DESCRIPCIÓN

134.El objetivo de esta PRUEBA es comprobar que el TOE no es vulnerable a la suplantación de un USUARIO fidedigno por parte de un atacante que utilice maquillaje como artefacto.

135.En líneas generales, esta PRUEBA se ejecuta de forma análoga a la P3.1, donde el resultado deseable en cada ENSAYO es el de DISTINTO o ERROR, mientras que el resultado no deseable será el de EQUIVALENTE.

5.6.2 MATERIALES

136. Para todos los ENSAYOS a realizar en esta PRUEBA, se utilizará el material especificado en 5.1.2, junto con **el personal maquillador y el material de maquillaje**, definido en la sección 3.

137. Se permite el uso de prótesis modificadoras del volumen facial. Por prótesis se entienden todos aquellos suplementos faciales que permitan crear volúmenes y modificar formas.

5.6.3 SUJETOS

138. Los SUJETOS a formar parte de esta PRUEBA serán:

- Un documento de identidad de **tres (3) USUARIOS** fidedignos del tipo **de documento** considerado en la evaluación.
- Uno o varios ATACANTES, en función de si es posible **cumplir con los requisitos que se detallan a continuación con uno o varios ATACANTES:**
 - **Deberá obtenerse una puntuación menor de 60** en la herramienta CCN_MATCH para las parejas USUARIO fidedigno/ATACANTE con ARTEFACTO.
 - **Deberá obtenerse una puntuación mayor de 70** en la herramienta CCN_MATCH para las parejas USUARIO fidedigno/ATACANTE **sin ARTEFACTO.**
- Cada USUARIO fidedigno será atacado, como mínimo, por un ATACANTE.
- Por lo tanto, el número mínimo de SUJETOS será 3, correspondiente a cada pareja ATACANTE-fidedigno.

5.6.4 ENSAYOS

139. Se realizarán un mínimo de ENSAYOS, para cada SUJETO y ESCENARIO, dado por la constante MIN_ENSAYOS.

140. Los pasos a seguir para realizar cada ENSAYO son:

- 1) El laboratorio pone en marcha el ESCENARIO y prepara al SUJETO indicándole como debe actuar y dónde colocarse. Se le recuerda al atacante que tiene que ser lo más cooperativo posible con el TOE para ser reconocido, incluyendo una correcta ejecución de la prueba de vida (si se solicita).
- 2) El SUJETO prepara el documento del USUARIO fidedigno para usarlo según la guía de operación del TOE. El ATACANTE, se maquillará de forma que se parezca lo más fielmente posible al USUARIO fidedigno.
- 3) El SUJETO procederá a identificarse de acuerdo a lo que indica el manual de uso del TOE, con la excepción de que su maquillaje intentará, no sólo ocultar su identidad, sino suplantar la del USUARIO fidedigno.
- 4) Si el TOE resulta en un resultado distinto de EQUIVALENTE o DISTINTO, se procederá a repetir el INTENTO. Esto se hará hasta llegar al número

MAX_INTENTOS, resultando en ERROR para dicho ENSAYO si se supera dicho número.

- 5) El laboratorio apuntará el resultado obtenido, incrementando el número de EQUIVALENTES, DISTINTOS o ERRORES_SUJETO según corresponda.
- 6) El SUJETO sale parcialmente de la interacción con el TOE (por ejemplo, deja de mirar a la cámara y mueve de forma apreciable su cuerpo para asegurarse que el siguiente ENSAYO es una interacción distinta)
- 7) Si en el ENSAYO para ese SUJETO, se ha superado el número de EQUIVALENTES dado por el umbral MAX_EQUIVALENTES_SUJETO, se irá al paso 9, incrementando la variable que acumula los PASA_SUJETOS. Si dicha variable supera el umbral dado por MAX_PASA_SUJETOS, se finalizarán los ENSAYOS para toda la PRUEBA, y se marcará la PRUEBA con FALLA.
- 8) Se vuelve al paso 3, para repetir el proceso, hasta alcanzar un mínimo de MIN_ENSAYOS para ese SUJETO.
- 9) Se cambia al siguiente SUJETO, y se vuelve al paso 1.

5.6.5 PARÁMETROS

141. A los parámetros especificados en 5.1.4, se añaden los siguientes:

MIN_SUJETOS = 3

142. Atendiendo a estos parámetros, el número mínimo de ENSAYOS a realizar en esta PRUEBA es de 30.

5.6.6 ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN

143. Adicionalmente a lo indicado en CCN-STIC-2004 y en 5.1.6, el Informe Técnico de Evaluación debe incluir el número y tipo (con fotografías) de los atacantes maquillados.

5.7 P3.3.6: ATAQUES USANDO HERRAMIENTAS INFORMÁTICAS DE DEEPFAKE

5.7.1 DESCRIPCIÓN

144. El objetivo de esta PRUEBA es comprobar que el TOE no es vulnerable a la suplantación de un USUARIO fidedigno por parte de un atacante que utilice herramientas informáticas de *deepfake*.

145. Estas herramientas son capaces de manipular el **vídeo** y el sonido, de tal manera que se superpongan elementos a las imágenes actuales.

146. Centrándose en un posible uso de usurpación de la identidad, el *deepfake* se utilizaría para modificar el rostro de una persona sobre el vídeo **en tiempo real** donde aparece **el ATACANTE**. Se debe utilizar las herramientas descritas en la sección 3.

147.En esta PRUEBA se instalará una solución de este tipo, donde al **vídeo** del atacante interactuando con el TOE, se le superpone la imagen de la cara del USUARIO fidedigno.

148.En líneas generales, esta PRUEBA se ejecuta de forma análoga a la P3.1, donde el resultado deseable en cada ENSAYO es el de DISTINTO o ERROR, mientras que el resultado no deseable será el de EQUIVALENTE.

149.En el caso de que el laboratorio demuestre que el TOE no permite el uso de cámaras virtuales la PRUEBA FALLA.

5.7.2 MATERIALES

150.Para todos los ENSAYOS a realizar en esta PRUEBA, se utilizará el material especificado en 5.1.2, junto con **el sistema de generación deepfake**, definido en la sección 3.

5.7.3 SUJETOS

151.Los SUJETOS a formar parte de esta PRUEBA serán:

- **Imágenes/vídeos de un** mínimo de cuatro (4) USUARIOS fidedignos, atendiendo a las necesidades **de entrenamiento** del sistema **utilizado para la creación de los modelos y la** generación de **los** vídeos *deepfake*.
- Un documento de identidad de cada uno de **los** USUARIOS fidedignos del tipo **de documento** considerado en la evaluación.
- Uno o dos ATACANTES, atendiendo a la disponibilidad y facilidad de suplantar la identidad de los USUARIOS fidedignos. La decisión la tomará el laboratorio siguiendo sus criterios justificados. Cada atacante puede atacar a uno o varios USUARIOS fidedignos dependiendo de la capacidad de las herramientas para recrear al USUARIO fidedigno.
- Por lo tanto, el número mínimo de SUJETOS será 4, correspondiente a cada SUJETO atacado.

5.7.4 ENSAYOS

152.Se realizarán un mínimo de ENSAYOS, para cada SUJETO y ESCENARIO, dado por la constante MIN_ENSAYOS.

153.Los pasos a seguir para realizar cada ENSAYO son:

- 1) El laboratorio pone en marcha el ESCENARIO y prepara al SUJETO indicándole como debe actuar y dónde colocarse. Se le recuerda al atacante que tiene que ser lo más cooperativo posible con el TOE para ser reconocido, incluyendo una correcta ejecución de la prueba de vida (si se solicita). También prepara el sistema de creación y suministro de los **vídeos** de deepfake en tiempo real.
- 2) El SUJETO prepara el documento del USUARIO fidedigno para usarlo según la guía de operación del TOE.

- 3) El SUJETO se identificará de acuerdo a lo que indica el manual de uso del TOE, a excepción de que la interacción será de forma indirecta a través de una cámara virtual.
- 4) Si el TOE resulta en un resultado distinto de EQUIVALENTE o DISTINTO, se procederá a repetir el INTENTO. Esto se hará hasta llegar al número MAX_INTENTOS, resultando en ERROR para dicho ENSAYO si se supera dicho número.
- 5) El laboratorio apuntará el resultado obtenido, incrementando el número de EQUIVALENTES, DISTINTOS o ERRORES_SUJETO según corresponda.
- 6) El SUJETO sale parcialmente de la interacción con el TOE (por ejemplo, deja de mirar a la cámara y mueve de forma apreciable su cuerpo para asegurarse que el siguiente ENSAYO es una interacción distinta).
- 7) Si en el ENSAYO para ese SUJETO, se ha superado el número de EQUIVALENTES dado por el umbral MAX_EQUIVALENTES_SUJETO, se irá al paso 9, incrementando la variable que acumula los PASA_SUJETOS. Si dicha variable supera el umbral dado por MAX_PASA_SUJETOS, se finalizarán los ENSAYOS para toda la PRUEBA, y se marcará la PRUEBA con PASA.
- 8) Se vuelve al paso 2, para repetir el proceso, hasta alcanzar un mínimo de MIN_ENSAYOS para ese SUJETO.
- 9) Se cambia al siguiente SUJETO, y se vuelve al paso 1.

5.7.5 PARÁMETROS

154.A los parámetros especificados en 5.1.4, se añaden los siguientes:

MIN_SUJETOS = 4

155.Atendiendo a estos parámetros, el número mínimo de ENSAYOS a realizar en esta PRUEBA es de 40.

5.7.6 ELEMENTOS A AÑADIR AL INFORME TÉCNICO DE EVALUACIÓN

156.Adicionalmente a lo indicado en CCN-STIC-2004 y en 5.1.6, el Informe Técnico de Evaluación debe incluir la siguiente información:

- 1) Descripción del sistema de deepfake utilizado y el proceso de entrenamiento para la generación de los modelos. Se deberán documentar los valores de parecido entre los modelos entrenados y los USUARIOS fidedignos obtenidos en la herramienta CCN_MATCH.
- 2) Número y descripción (con fotografías/videos), de los artefactos utilizados (las imágenes recogidas por el TOE).

6 LISTADO DE ACRÓNIMOS

CCN	Centro Criptológico Nacional
FRVT	<i>Face Recognition Vendor Test 1:1 Ongoing</i> (https://pages.nist.gov/frvt/html/frvt11.html)
NIST	<i>National Institute for Standards and Technology</i>
PAD	<i>Presentation Attack Detection</i>
STIC-140-F11	Anexo F.11 titulado "Herramientas de Videoidentificación", del documento de apoyo a la evaluación, que es parte de la Guía de Seguridad de las TIC CCN-STIC 140
TOE	<i>Target of Evaluation</i>