

CARTA N° 001-2023- KAPA8- RENIEC

Lima, 22 de noviembre del 2023

Señores:

Registro Nacional de Identificación y Estado Civil
N°1472, Lima 1.

Presente. -

Atención: **Felipe Alexis Alegre Cuba**
Comité Evaluador

Asunto: Subsanación y/o aclaración de la Propuesta de la Licitación Publica N°005-2023-RENIEC-1 "SOFTWARE (INC. LICENCIA) PARA EL SISTEMA BIOMETRICO DACTILAR Y FACIAL, DE TIPO COMPONENTE SDK PARA EQUIPOS MOVILES CON SISTEMA OPERAIVO IOS

Referencia:

- a) Licitación Publica N°005-2023-RENIEC-1 "SOFTWARE (INC. LICENCIA) PARA EL SISTEMA BIOMETRICO DACTILAR Y FACIAL, DE TIPO COMPONENTE SDK PARA EQUIPOS MOVILES CON SISTEMA OPERAIVO IOS
- b) Carta N° 000001-2023/RENIEC

Estimados señores:

Tenemos el agrado de dirigirnos a usted, en relación con el documento de la referencia, haciendo las siguientes aclaraciones:

1. Se anexa a esta carta los siguientes antecedentes:
 - a. Copia Simple de la Vigencia de poder de la SUNARP con partida electrónica N° 13713556, Donde se hace mención la representación del señor Jhonatan Willy Escobar Cifuentes como consta registrado en el asiento A00001 a la constitución social de la empresa vigente e inscrita en los registros públicos de la empresa **KAPA8 S.A.C.**
 - b. Copia Simple del Carné de extranjería del Señor Jhonatan Willy Escobar Cifuentes N° 000594175.
 - c. Copia Simple y traducción al español de los informes de laboratorio que nos respaldan en conocimiento, experiencia e implementación. Certificada por un traductor colegiado en el Colegio de Traductores del Perú, del certificado de resultado de evaluación, de ataques de presentación acorde a las especificaciones ISO/IEC 30107-3 <Nivel 1 o Nivel A para biometría dactilar y Nivel 2 o Nivel B para biometría facial>, utilizando como instrumento de prueba equipos con sistema operativo iOS.

En atención a ello, hago propicia la ocasión para renovarles la muestra de mi especial estima.

Atentamente;


KAPA8 S.A.C.
Jhonatan Escobar
Gerente General

000001



ZONA REGISTRAL N° IX - SEDE LIMA
Oficina Registral de LIMA



Código de Verificación:
91431066
Solicitud N° 2023 - 7091723
15/11/2023 15:55:43

REGISTRO DE PERSONAS JURÍDICAS LIBRO DE SOCIEDADES ANONIMAS

CERTIFICADO DE VIGENCIA

El servidor que suscribe, **CERTIFICA:**

Que, en la partida electrónica N° 13713556 del Registro de Personas Jurídicas de la Oficina Registral de LIMA, consta registrado y vigente el **nombramiento** a favor de ESCOBAR CIFUENTES, JHONATAN WILLY, identificado con CARNET EXTRANJERIA N° 000594175, cuyos datos se precisan a continuación:

DENOMINACIÓN O RAZÓN SOCIAL: KAPA8 S.A.C.

LIBRO: SOCIEDADES ANONIMAS

ASIENTO: A00001 RECTIFICADO POR EL ASIENTO D00001

CARGO: GERENTE GENERAL

FACULTADES:

RÉGIMEN DE LA GERENCIA

ART.5°: LA SOCIEDAD PODRÁ TENER MÁS DE UN GERENTE.

EL GERENTE GENERAL DIRIGE LA MARCHA ADMINISTRATIVA Y ES EL REPRESENTANTE LEGAL DE LA SOCIEDAD CON TODAS LAS FACULTADES DEL MANDATO CONFORME AL CÓDIGO CIVIL Y LOS PODERES DE LOS ARTÍCULOS 74 Y 75 DEL CÓDIGO PROCESAL CIVIL, LOS QUE PODRÁ SUSTITUIR CONFORME AL ARTÍCULO 77 DEL MISMO CÓDIGO Y READQUIRIR CUANTAS VECES SEA NECESARIO Y OTORGAR LA FACULTAD DE EMPLAZAMIENTO CONFORME EL ARTÍCULO 436 DEL CÓDIGO PROCESAL CIVIL. ASIMISMO, TENDRÁ LAS FACULTADES A QUE SE REFIEREN LOS ARTÍCULOS 3 Y 28 DEL DECRETO SUPREMO 006-72-TR; Y LOS ARTÍCULOS 8, 9 Y 10 DE LA LEY 26636.

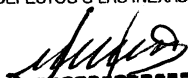
EL GERENTE GENERAL A SOLA FIRMA PODRÁ REPRESENTAR A LA SOCIEDAD ANTE LA SUNAT, SUNARP, MUNICIPALIDADES Y DEMÁS AUTORIDADES TRIBUTARIAS, ADMINISTRATIVAS Y LOCALES, FORMULANDO TODA CLASE DE PETICIONES, PROMOVER PROCESOS ADMINISTRATIVOS, INTERPONER TODO TIPO DE RECURSOS, APELACIONES, RECONSIDERACIONES, REVISIONES, SEAN ORDINARIOS Y EXTRAORDINARIOS, CANCELAR O RECLAMAR OBLIGACIONES TRIBUTARIAS; ASÍ COMO ANTE LAS AUTORIDADES DEL MINISTERIO DE TRABAJO Y PROMOCIÓN DEL EMPLEO EN LOS PROCESOS LABORALES JUDICIALES O PRIVATIVOS DE TRABAJO, EN LOS PROCESOS DE INSPECCIÓN, EN LAS NEGOCIACIONES COLECTIVAS, Y EN TODO LO RELATIVO A LAS RELACIONES INDIVIDUALES O COLECTIVAS DE TRABAJO CONFORME LOS DISPOSITIVOS LEGALES VIGENTES, CON LAS MISMAS FACULTADES SEÑALADAS EN LOS ARTÍCULOS 74 Y 75 DEL CÓDIGO PROCESAL CIVIL.

EL GERENTE GENERAL A SOLA FIRMA PODRÁ ABRIR Y CERRAR CUENTAS CORRIENTES, DE AHORRO, A PLAZOS O DE CUALQUIER OTRO GÉNERO, GIRAR CONTRA ELLAS, TRANSFERIR, TRANSFERIR A TERCEROS, TRANSFERIR ENTRE CUENTAS, DISPONER FONDOS DE ELLAS, EFECTUAR RETIROS Y SOBREGIRARSE EN CUENTA CORRIENTE CON O SIN GARANTÍA MOBILIARIA, HIPOTECARIA Y/O FIANZA EN TODO TIPO DE INSTITUCIONES DE CRÉDITO; CONTRATAR CAJAS DE SEGURIDAD, ABRIRLAS, OPERARLAS Y/O CERRARLAS; GIRAR, ACEPTAR Y COBRAR CHEQUES; GIRAR, GIRAR EN SOBREGIRO, ACEPTAR, EMITIR, SOLICITAR; OTORGAR, AVALAR, ENDOSAR, DESCOTAR, COBRAR, PROTESTAR, REACEPTAR, RENOVAR, CANCELAR, DEPOSITAR, RETIRAR Y COMPRAR, VENDER, Y/O DAR EN GARANTÍA O EN PROCURACIÓN, SEGÚN SU NATURALEZA, LETRAS DE CAMBIO, VALES, PAGARÉS, CHEQUES Y EN GENERAL TODO TIPO DE TÍTULOS VALORES, ASÍ COMO CUALQUIER OTRO

LOS CERTIFICADOS QUE EXTIENDEN LAS OFICINAS REGISTRALES ACREDITAN LA EXISTENCIA O INEXISTENCIA DE INSCRIPCIONES O ANOTACIONES EN EL REGISTRO AL TIEMPO DE SU EXPEDICIÓN (ART. 140° DEL T.U.O. DEL REGLAMENTO GENERAL DE LOS REGISTROS PÚBLICOS APROBADO POR RESOLUCIÓN N° 126-2012-SUNARP-SN)

LA AUTENTICIDAD DEL PRESENTE DOCUMENTO PODRÁ VERIFICARSE EN LA PÁGINA WEB [HTTPS://ENLINEA.SUNARP.GOB.PE/SUNARPWEB/PAGES/PUBLICIDADCERTIFICADA/VERIFICARCERTIFICADOLITERAL.FACES](https://enlinea.sunarp.gob.pe/sunarpweb/pages/publicidadcertificada/verificarcertificadoliteralfaces) EN EL PLAZO DE 90 DÍAS CALENDARIO CONTADOS DESDE SU EMISIÓN.

REGLAMENTO DEL SERVICIO DE PUBLICIDAD REGISTRAL : ARTÍCULO 81 - DELIMITACIÓN DE LA RESPONSABILIDAD. EL SERVIDOR RESPONSABLE QUE EXPIDE LA PUBLICIDAD FORMAL NO ASUME RESPONSABILIDAD POR LOS DEFECTOS O LAS INEXACTITUDES DE LOS ASIENTOS REGISTRALES, ÍNDICES AUTOMATIZADOS, Y TÍTULOS PENDIENTES QUE NO CONSTEN EN EL SISTEMA INFORMÁTICO.


KAPA8 S.A.C.
Jhonatan Escobar
Gerente General

Pag. 1 de 3

000002



ZONA REGISTRAL N° IX - SEDE LIMA
Oficina Registral de LIMA



Código de Verificación:
91431066
Solicitud N° 2023 - 7091723
15/11/2023 15:55:43

DOCUMENTO MERCANTIL Y/O CIVIL, INCLUYENDO PÓLIZAS, CONOCIMIENTOS DE EMBARQUE, CARTAS PORTE, FIANZA, CARTAS FIANZA, CARTAS DE CRÉDITO, CERTIFICADOS DE DEPÓSITO, WARRANTS, INCLUYENDO SU CONSTITUCIÓN, FIANZA Y/O AVALES; CELEBRAR ACTIVA O PASIVAMENTE CONTRATOS DE MUTUO; CON INSTITUCIONES BANCARIAS, FINANCIERAS O CON CUALQUIER OTRA PERSONA NATURAL O JURÍDICA, CON O SIN GARANTÍAS; OTORGAR, Y SUSTITUIR PODERES; CONTRATAR DERIVADOS, FORWARD, SWAPS, FIDEICOMISO, CONTRATAR COMISIÓN DE CONFIANZA, CONTRATAR CRÉDITO DE CUENTA CORRIENTE CON GARANTÍA Y SIN GARANTÍA, CONTRATAR PRÉSTAMO CON GARANTÍA Y SIN GARANTÍA; CESIÓN DE DERECHOS, CONTRATAR Y ENDOSAR SEGUROS DAR EN GARANTÍA MOBILIARIA, ARRENDAMIENTO FINANCIERO, CONTRATOS DE IMPORTACIÓN, CONSTITUIR HIPOTECAS, GRAVAR INMUEBLES, OTORGAR AVALES, FIANZAS Y CUALQUIER OTRA GARANTÍA, AÚN A FAVOR DE TERCEROS, PARA AFIANZAR OPERACIONES CREDITICIAS, FINANCIERAS Y/O COMERCIALES CON BANCOS, FINANCIERAS, SEGUROS, CAJAS DE AHORRO, COOPERATIVAS O CUALQUIER OTRA INSTITUCIÓN CREDITICIA Y/O PERSONA NATURAL Y/O JURÍDICA, NACIONAL Y/O EXTRANJERA; EN GENERAL CELEBRAR TODO TIPO DE OBLIGACIONES DE CRÉDITO, CON LAS QUE LA SOCIEDAD GARANTICE U OBTenga BENEFICIO O CRÉDITO A FAVOR Y/O PARA TERCEROS; COMPRAR, VENDER, ARRENDAR, PERMUTAR, DONAR, BIENES DE O PARA LA SOCIEDAD, SEAN MUEBLES O INMUEBLES; TRANSFERIR Y CONDONAR OBLIGACIONES; CELEBRAR CONTRATOS DE FIDEICOMISO ASÍ COMO DAR LOS BIENES DE LA SOCIEDAD EN FIDEICOMISO DE GARANTÍA Y ADMINISTRACIÓN; CELEBRAR CONVENIOS ARBITRALES Y TODO TIPO DE CONTRATOS DE LEASING, ARRENDAMIENTO FINANCIERO, FACTORING, JOINT VENTURE, FRANCHISING, CONCESIÓN, KNOW HOW, ADVANCE ACCOUNT, TRANSFERENCIA DE TECNOLOGÍA, COLABORACIÓN EMPRESARIAL, CONFIRMING, FORWARD, OPCIONES, SWAPS, COMISIÓN DE CONFIANZA, CESIÓN DE DERECHOS, CESIÓN DE OPOSICIÓN CONTRACTUAL, GARANTÍAS DE AFECTAR DEPÓSITOS, GARANTÍAS DE AFECTACIÓN DE COBRANZA, TRANSFERENCIA DE TECNOLOGÍA, COLABORACIÓN EMPRESARIAL; SOLICITAR CARTAS FIANZA, TARJETAS DE CRÉDITO, REPORTES, DESCUENTOS; COMPRA Y VENTA DE ACCIONES EN BOLSA O FUERA DE ELLA, SEA EN MONEDA NACIONAL O EXTRANJERA; CONSTITUIR EMPRESAS Y/O TODO TIPO DE PERSONAS JURÍDICAS, SEA EN EL PAÍS O EL EXTRANJERO; REPRESENTAR A LA SOCIEDAD EN LAS JUNTAS DE ACCIONISTAS, DONDE LA SOCIEDAD SEA ACCIONISTA; OTORGAR, SUSTITUIR, DELEGAR Y REVOCAR PODERES; INTERVENIR EN LICITACIONES Y CONCURSOS PÚBLICOS; Y EN GENERAL FIRMAR TODA CLASE DE CONTRATOS, SEAN CIVILES, MERCANTILES Y/O BANCARIOS, CON CUALQUIER PERSONA NATURAL Y/O JURÍDICA, NACIONAL Y/O EXTRANJERA; ASÍ COMO SUSCRIBIR LOS INSTRUMENTOS PÚBLICOS Y PRIVADOS A QUE HUBIERE LUGAR; Y PARA LA CELEBRACIÓN Y EJECUCIÓN DE LOS ACTOS Y CONTRATOS CORRESPONDIENTES AL OBJETO SOCIAL.

AUTORIZAR A SOLA FIRMA LA ADQUISICIÓN DE LOS BIENES, CONTRATACIÓN DE OBRAS Y PRESTACIÓN DE SERVICIOS PERSONALES.

NOMBRAR, PROMOVER, SUSPENDER Y DESPEDIR A LOS EMPLEADOS Y SERVIDORES DE LA EMPRESA. CUIDAR DE LA CONTABILIDAD Y FORMULAR EL ESTADO DE PÉRDIDAS Y GANANCIAS, EL BALANCE GENERAL DE LA EMPRESA Y LOS DEMÁS ESTADOS Y ANÁLISIS CONTABLES QUE SOLICITE EL TITULAR. SOLICITAR, ADQUIRIR, TRANSFERIR REGISTROS DE PATENTES, MARCAS, NOMBRES COMERCIALES CONFORME A LEY, SUSCRIBIENDO CUALQUIER CLASE DE DOCUMENTOS VINCULADOS A LA PROPIEDAD INDUSTRIAL O INTELECTUAL, QUE CONLLEVE A LA REALIZACIÓN DEL OBJETO SOCIAL. PARTICIPAR EN LICITACIONES, CONCURSOS PÚBLICOS Y/O ADJUDICACIONES, SUSCRIBIENDO LOS RESPECTIVOS DOCUMENTOS, QUE CONLLEVE A LA REALIZACIÓN DEL OBJETO SOCIAL.

(...)

GERENTE GENERAL : JHONATAN WILLY ESCOBAR CIFUENTES, IDENTIFICADO CON C.E. N° 000594175.-****

DOCUMENTO QUE DIO MÉRITO A LA INSCRIPCIÓN:


POR ESCRITURA PÚBLICA DEL 29.09.2016 OTORGADO ANTE EL NOTARIO DE LIMA DR. FERNANDO

LOS CERTIFICADOS QUE EXTIENDEN LAS OFICINAS REGISTRALES ACREDITAN LA EXISTENCIA O INEXISTENCIA DE INSCRIPCIONES O ANOTACIONES EN EL REGISTRO AL TIEMPO DE SU EXPEDICIÓN (ART. 140° DEL T.U.O. DEL REGLAMENTO GENERAL DE LOS REGISTROS PÚBLICOS APROBADO POR RESOLUCIÓN N° 126-2012-SUNARP-SN)

LA AUTENTICIDAD DEL PRESENTE DOCUMENTO PODRÁ VERIFICARSE EN LA PÁGINA WEB [HTTPS://ENLINEA.SUNARP.GOB.PE/SUNARPPWEB/PAGES/PUBLICIDADCERTIFICADA/VERIFICARCERTIFICADO/ITERAL.FACES](https://enlinea.sunarp.gob.pe/sunarpweb/pages/publicidadcertificada/verificarcertificado/iteral.faces) EN EL PLAZO DE 90 DÍAS CALENDARIO CONTADOS DESDE SU EMISIÓN.

REGLAMENTO DEL SERVICIO DE PUBLICIDAD REGISTRAL : ARTÍCULO 81 - DELIMITACIÓN DE LA RESPONSABILIDAD. EL SERVIDOR RESPONSABLE QUE EXPIDE LA PUBLICIDAD FORMAL NO ASUME RESPONSABILIDAD POR LOS DEFECTOS O LAS INEXACTITUDES DE LOS ASIENTOS REGISTRALES, ÍNDICES AUTOMATIZADOS, Y TÍTULOS PENDIENTES QUE NO CONSTEN EN EL SISTEMA INFORMÁTICO.

Pag. 2 de 3


JAPAS S.A.C.
Jhonatan Escobar
Gerente General

000003



ZONA REGISTRAL N° IX - SEDE LIMA
Oficina Registral de LIMA



Código de Verificación:
91431066
Solicitud N° 2023 - 7091723
15/11/2023 15:55:43

TARAZONA ALVARADO.

II. ANOTACIONES EN EL REGISTRO PERSONAL O EN EL RUBRO OTROS:
NINGUNO.

III. TÍTULOS PENDIENTES:
NINGUNO.


IV. DATOS ADICIONALES DE RELEVANCIA PARA CONOCIMIENTO DE TERCEROS:
REGLAMENTO DEL SERVICIO DE PUBLICIDAD REGISTRAL : ARTÍCULO 81 - DELIMITACIÓN DE LA RESPONSABILIDAD. EL SERVIDOR RESPONSABLE QUE EXPIDE LA PUBLICIDAD FORMAL NO ASUME RESPONSABILIDAD POR LOS DEFECTOS O LAS INEXACTITUDES DE LOS ASIENTOS REGISTRALES, ÍNDICES AUTOMATIZADOS, Y TÍTULOS PENDIENTES QUE NO CONSTEN EN EL SISTEMA INFORMÁTICO.

V. PÁGINAS QUE ACOMPAÑAN AL CERTIFICADO:
PAG.(1-3).

N° de Fojas del Certificado: 3

Derechos Pagados: 2023-99999-2266781 S/ 30.00
Tasa Registral del Servicio S/ 30.00

Verificado y expedido por ESPICHAN VICENTE, SAILING YANELLI'S, Abogado Certificador de la Oficina Registral de Lima, a las 12:30:46 horas del 16 de Noviembre del 2023.


.....
SAILING YANELLI'S ESPICHAN VICENTE
ABOGADO - CERTIFICADOR
Zona Registral N° IX - Sede Lima

LOS CERTIFICADOS QUE EXTIENDEN LAS OFICINAS REGISTRALES ACREDITAN LA EXISTENCIA O INEXISTENCIA DE INSCRIPCIONES O ANOTACIONES EN EL REGISTRO AL TIEMPO DE SU EXPEDICION (ART. 140° DEL T.U.O.DEL REGLAMENTO GENERAL DE LOS REGISTROS PUBLICOS APROBADO POR RESOLUCION N° 126-2012-SUNARP-SN)

LA AUTENTICIDAD DEL PRESENTE DOCUMENTO PODRÁ VERIFICARSE EN LA PÁGINA WEB [HTTPS://ENLINEA.SUNARP.GOB.PE/SUNARPWEB/PAGES/PUBLICIDADCERTIFICADA/VERIFICARCERTIFICADOLITERALFACES](https://enlinea.sunarp.gob.pe/sunarpweb/pages/publicidadcertificada/verificarcertificadoliteralfaces) EN EL PLAZO DE 90 DÍAS CALENDARIO CONTADOS DESDE SU EMISION.

REGLAMENTO DEL SERVICIO DE PUBLICIDAD REGISTRAL : ARTÍCULO 81 - DELIMITACIÓN DE LA RESPONSABILIDAD. EL SERVIDOR RESPONSABLE QUE EXPIDE LA PUBLICIDAD FORMAL NO ASUME RESPONSABILIDAD POR LOS DEFECTOS O LAS INEXACTITUDES DE LOS ASIENTOS REGISTRALES, ÍNDICES AUTOMATIZADOS, Y TÍTULOS PENDIENTES QUE NO CONSTEN EN EL SISTEMA INFORMÁTICO.

Pag. 3 de 3



KAPA8 S.A.C.
Jhonatan Escobar
Gerente General

000004

REPÚBLICA DEL PERÚ
SUPERINTENDENCIA NACIONAL DE MIGRACIONES
 CALIDAD MIGRATORIA: RFR RESIDENTE

APellidos: ESCOBAR CIFUENTES
Nombre: JHONATAN WILLY
Nacionalidad: GUATEMALTECA
Nacimiento: 01 Sep 1975
Estatus Civil: V

DUPLICADO
 ESTE CARNÉ
 INVALIDA EL ANTERIOR

**CARNÉ DE
 EXTRANJERÍA N° 000594175**

Firma

MIGRACIONES
 Superintendencia Nacional
 PERÚ

Departamento: LIMA **Provincia:** LIMA
Distrito: SANTIAGO DE SURCO
Dirección: CALLE BERNARDO ALCEDO 326, APTO. 4, URB. LOS PROCERES

N° Pasaporte: 600543261
Fec. Inscripción: 06 Jul 2009
Fec. Emisión: 09 Ene 2020
Caducidad C.E.: 09 Ene 2024
Venc. Residencia: Consultar en la página web www.migraciones.gob.pe

Lug. Expedición: DSW

418759

**C<GUAESCOBAR<CIFUENTES<<JHONATAN<WIL
 0005941759GUA7509018M2401092<<<<<<<6**

Índice Derecho

Firma Autorizada

Jhonatan Escobar
 KAPA8 S.A.C.
 Jhonatan Escobar
 Gerente General

000005

COLEGIO DE TRADUCTORES DEL PERÚ

Creado por Ley N° 26684

MARIA ISABEL BRICEÑO SALAZAR
CTP 0874
TRADUCTORA COLEGIADA CERTIFICADA
Español - Inglés - Portugués

Urb. Juan Pablo II Mz. 1 Lote 18. La Perla, Callao
+51 932487471
mariaisabel.bricenosalazar@gmail.com

TRADUCCIÓN CERTIFICADA DIGITAL

TCD 0857-2023

Detección de ataques de presentación
Servicios de evaluación de nivel 1
Informe de pruebas



La Decana Nacional del Colegio de Traductores del Perú certifica que la firma de la derecha corresponde a un miembro hábil y activo de la Orden que cuenta con la autorización del Colegio de Traductores del Perú para realizar traducciones certificadas digitales. Se legaliza únicamente la firma, no el contenido de los documentos adjuntos.

Mary Ann Elsa Monteagudo Medina
Decana Nacional del Colegio de Traductores del Perú

La Traductora Colegiada Certificada, miembro del Colegio de Traductores del Perú (CTP) que suscribe, declara que la presente Traducción Certificada Digital es una versión fiel y correcta del documento adjunto que se ha tenido a la vista. Se certifica la fidelidad de la traducción, mas no se asume responsabilidad por la autenticidad ni por el contenido del documento en lengua origen.



COLEGIO DE TRADUCTORES DEL PERÚ
Fecha: 22/11/2023 14:09:29 UTC-05:00
ID: 20376744940
<https://ictp.trisigne.com/documento/validar/B1A497EE-15F4-4980-AA7E-D98D3F4718F1>



Maria Isabel Briceño Salazar
Fecha: 22/11/2023 14:08:47 UTC-05:00
ID: IDCPE-73039137

El ejemplar impreso de este documento es válido según el D.S. n.° 026-2016-PCM.

KAPAS S.A.C.
Jonathan Escobar
Gerente General

000006

000007

Historial de versiones

Número de versión	Descripción del cambio	Autor	Fecha
V1.0	Versión inicial (Borrador)	BixeLab	15/09/2022
V1.01	Información adicional añadida en el resumen ejecutivo Los tipos de ataque cooperativo de nivel B reclasificados han vuelto a ser de nivel A.	BixeLab	17/10/2022

AVISO DE PROPIEDAD DE BIXELAB PTY LTD



BixeLab Pty Ltd ha puesto el máximo cuidado en la preparación de este documento. La información contenida en el mismo es exacta según el leal saber y entender de BixeLab en la fecha de su publicación. BixeLab no puede aceptar ninguna responsabilidad ante ninguna persona o empresa por cualquier pérdida financiera o daño derivado del uso de este documento. No debe reproducirse ni ponerse a disposición, de ninguna forma, de personas ajenas al grupo o grupos directamente responsables de la evaluación de su contenido, sin el consentimiento por escrito de BixeLab Pty Ltd.

Todas las marcas y productos mencionados en este documento son marcas comerciales o marcas registradas de sus respectivos propietarios.

Este informe no debe ser utilizado por el cliente para reclamar la certificación, aprobación o respaldo de un producto por el NIST, el NVLAP o cualquier agencia del gobierno de los Estados Unidos.

Tech 5 SA

Clasificación: Información comercial confidencial



COLEGIO DE TRADUCTORES DEL PERU

Fecha: 22/11/2023 14:09:29 UTC-05:00

ID: 20376744940


<https://ctp.insigne.com/documento/validar/B1A497EE-15F4-43B0-AA7E-D98D3F4718F1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137


KAPAS S.A.C.
Jhonatan Escobar
Gerente General

000008

1.7 Auditoria de configuración

Cada día de pruebas, se realizó una auditoría de la configuración del sistema en el IUT sometido a evaluación PAD. La información registrada se resume en un registro de auditoría que incluye especificaciones de hardware y software, versiones de SO, número de serie y fabricación.

Este registro de auditoría sirve para verificar que todas las configuraciones de software y hardware relacionadas con cada prueba se han mantenido inalteradas durante la ejecución. El objetivo es mitigar las variaciones relacionadas con el software y el hardware del sistema y llevar a cabo el protocolo de laboratorio esencial para la integridad.

Las tablas de la sección Anexo 3: Registros de auditoría de configuración proporcionan registros detallados de auditoría de configuración centrados en lo anterior sin anomalías identificadas.

1.8 Resultados previstos

1.8.1 Datos de resultados previstos

En la tabla siguiente se resumen los datos de resultados previstos del IUT.

Tabla 2 Resumen de los datos de resultados previstos

Componente IUT	Componentes	Resultados	Rango de puntuación	(Opciones basadas en umbrales conocidos)
Detección de ataques de presentación (vida)	Vida	Puntuación de vida	0 – 100	Aprobado (≥ 50) Fallido (< 50)
	Calidad de imagen	Puntuación de NFIQ2	0 – 100	N/A

La IUT utilizó un umbral de puntuación de vida de 50 (0,5) para decidir si la muestra adquirida estaba activa (aprobado) o era artificial (fallido). El NIST Fingerprint Image Quality (NFIQ) 2 es un software de código abierto que define una puntuación de calidad normalizada para las imágenes de huellas dactilares. La puntuación NFIQ2 indica la calidad de la muestra obtenida.

1.8.2 Rendimiento de resultados previstos

En las evaluaciones tradicionales del rendimiento biométrico, la verdad fundamental desempeña un papel crucial para garantizar la validez de las métricas de error notificadas. En el contexto de la evaluación PAD, la verdad fundamental se refiere a si una determinada respuesta de detección de vida es genuina y de buena fe o representa un impostor (ataque).

Las métricas incluirán una tasa de error de clasificación de presentación de ataques (APCER) y una tasa de error de clasificación de presentación de buena fe (BPCER) para evaluar el rendimiento de los mecanismos de ataque de presentación en el IUT.

El objetivo de la evaluación PAD era medir la precisión del mecanismo de detección de vida. Una presentación de buena fe se refería a un sujeto humano vivo que presentaba huellas dactilares según las indicaciones de la aplicación, y un ataque de presentación se refería al operador de la prueba que montaba el biométrico del objetivo utilizando un PAI.

En este caso, el resultado esperado para una presentación de buena fe era una puntuación de vida igual o superior a 50 (0,5), y una presentación de ataque debería haber devuelto una puntuación de vida inferior a 50 (0,5). En la tabla siguiente se resumen los resultados esperados de la evaluación PAD para la detección de vida.

Tech 5 SA

Clasificación: información comercial confidencial



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:09:29 UTC-05:00

ID: 20376744940

<https://ctp.theigme.com/documento/validar/B1A497EE-15F4-49B0-AA7E-D9BD3F4718F1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137

KAPA8 S.A.C.
Jhonatan Escobar
Cuenta Corriente

000009

Tabla 3 Resumen de los resultados previstos para el IUT

Objetivo del componente de la evaluación	Clasificación de componentes	Componentes	Base fiable	Opciones de resultados basadas en umbrales conocidos
Detección de ataques de presentación	Principal	Vida	De buena fe	Aprobado (≥ 50)
			Ataque	Fallido (< 50)
	Secundario	Calidad de imagen	De buena fe	N/A ²
			Ataque	

² La norma ISO 30107-3 afirma que "no hay razón para suponer un determinado nivel de calidad de los artefactos [PAD]"
Por lo tanto, no debe haber ninguna suposición de calidad correlacionada con el tipo de ataque.

Tech 5 SA

Clasificación: Información comercial confidencial



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:09:29 UTC-05:00

ID: 20376744940

<https://ctp.theigpe.com/documento/validar/B1A497EE-15F4-49B0-AA7E-D9B03F4718F1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137


KAPA8 S.A.C.
Jhonatan Escobar
Gerente General

000010

Descripción de la base de datos

1.9 Evaluación PAD

1.9.1 Instrumentos de ataque de presentación

Los tipos de ataques de presentación utilizados en esta evaluación se basaron en umbrales operativos para la puntuación más alta alcanzada en los siguientes criterios, de modo de establecer una justificación para hacer una afirmación sustancial de seguridad biométrica sobre el sistema sometido a prueba:

- **Tipo:** Designación del artefacto definido por sus propiedades y origen.
- **Acceso a las características biométricas:** La relativa facilidad de acceso a fuentes adecuadas a partir de las cuales se puede producir el artefacto.
- **Equipamiento/Coste:** La dificultad relativa y el gasto para producir el artefacto.

Estos factores se describen en la tabla siguiente.

Tabla 4 Evaluación de los tipos de ataques de presentación

Clasificación	Niveles	Descripción
Tipo	Simple	Suelen ser bidimensionales o recuperados de otra fuente.
	Especializado	Suelen ser tridimensionales y/o especialmente producidos o alterados a partir de una fuente.
	Sofisticado	Artefactos sofisticados de producción específica que suelen aprovechar múltiples fuentes de alta calidad.
Acceso a las características biométricas	Fácil	Pública o comúnmente disponible, normalmente sin conocimiento del objetivo.
	Moderado	Suele requerir la cooperación del objetivo o el acceso a la biométrica o a la plantilla biométrica en sí.
	Difícil	Suele requerir múltiples fuentes que pueden ser alteradas o aumentadas. A menudo implica el acceso a la biométrica o a la plantilla biométrica en sí.
Equipamiento/Coste	Bajo	Puede fabricarse con materiales estándar utilizando equipos de oficina o domésticos.
	Medio	Puede requerir el uso de proveedores, software o equipos genéricos
	Alto	Puede requerir el uso de proveedores, programas informáticos o equipos especializados.

Tech 5 SA

Clasificación: Información comercial confidencial



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:09:29 UTC-05:00

ID: 20376744940

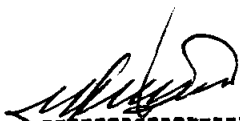
<https://ctp.theigmc.com/documento/validar/51A497EE-15F4-4980-AA7E-D98D3F4718F1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137


KAPAS S.A.C.
Jonathan Escobar
Gerente General

000011

MARÍA ISABEL BRICEÑO SALAZAR
CTP N° 874

Traductora Colegiada Certificada
Español-Inglés-Portugués

TRADUCCIÓN CERTIFICADA DIGITAL N° 0857-2023
Página 6 de 15

Los tipos de ataques de presentación (como tipos de artefactos) se crearon basándose tanto en la fuente de las características biométricas como en los criterios ISO/IEC 30107-3 para la creación, procedencia, uso y manipulación de las propiedades de los artefactos —pertencientes desde la creación hasta la utilización de la prueba— como criterios formalizados para la evaluación de los mecanismos PAD. Como se especifica en la sección 8.1 de la norma ISO/IEC 30107-3, los ataques de presentación previstos para esta evaluación entraban en la categoría de ataques biométricos de impostores y tenían las tres propiedades siguientes:

1. Las muestras aparecieron como características biométricas naturales para el IUT.
2. Las muestras aparecieron como características biométricas naturales a los controles de calidad de datos biométricos establecidos para el IUT.
3. Las muestras adquiridas por la cámara del dispositivo del artefacto presentado contenían características extraíbles que coincidían con las referencias del individuo seleccionado.

Sobre la base de los criterios de evaluación de la ISO, los tipos de ataques de presentación se clasificaron a continuación en los niveles A y B. El operador de prueba que se hizo pasar por atacante tuvo acceso a cada nivel de representaciones de ataques sobre la base de las características biométricas originales obtenidas a través de sujetos cooperativos. En la tabla siguiente se especifican los ataques de presentación, las clasificaciones de los niveles y el número de fuentes por tipo de ataque.

Tabla 5 Resumen de los tipos de ataques de presentación

Nivel de ataque de presentación	Instrumentos artificiales de ataques de presentación	Fuente	Descripción	Técnica de presentación
A (no cooperativo)	Foto en blanco y negro de una huella dactilar	2	Los dedos de los sujetos de la prueba se capturaron con una cámara desde unos metros de distancia, y las imágenes capturadas se recortaron para extraer los dedos individuales de los sujetos. Se midieron para que tuvieran aproximadamente el mismo tamaño que los dedos reales, se imprimieron y se presentaron directamente al sensor.	No cooperativa - Las características biométricas se capturaron simulando condiciones no cooperativas (es decir, el participante saludando en una foto). Con ello se pretende simular que un atacante obtiene datos biométricos de las redes sociales y otras fuentes fotográficas de acceso público.
	Huella dactilar levantada con celofán	2	La huella dactilar de los sujetos de la prueba se colocó sobre el cristal de forma similar a la huella dactilar residual sobre cristal y se levantó utilizando cinta adhesiva. El trozo de cinta se colocó sobre un fondo oscuro para facilitar la visualización de la rugosidad de los dedos y se presentó directamente al sensor.	
	Huella dactilar residual en cristal	2	Los sujetos de prueba se humedecieron el dedo y lo colocaron sobre un cristal. La huella que quedaba en el cristal se utilizó directamente contra el sensor.	



Tech 5 SA

Clasificación: Confidencialidad comercial



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:08:23 UTC-05:00

ID: 20376744940

<https://cp.trisign.com/documento/validar/B1A497EE-15F4-4960-AA7E-D96C9F471B81>



María Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137

KAPA8 S.A.C.
Jonathan Escobar
Gerente General

000012

MARÍA ISABEL BRICEÑO SALAZAR
CTP N° 874

Traductora Colegiada Certificada
Español-Inglés-Portugués

TRADUCCIÓN CERTIFICADA DIGITAL N° 0857-2023
Página 7 de 15

Nivel de ataque de presentación	Instrumentos artificiales de ataques de presentación	Fuente	Descripción	Técnica de presentación
A (cooperativo) ³	Huella dactilar impresa con tinta (brillante)	3	Los sujetos de prueba introdujeron sus dedos en tinta y los presionaron contra papel mate y brillante. Las impresiones resultantes se dejaron secar durante la noche y se presentaron al sensor.	Cooperativa – Las características biométricas se capturaron directamente de los participantes del equipo de pruebas, además de algunos participantes adicionales que no participaron en persona, pero proporcionaron sus datos biométricos con el fin de crear ataques de presentación. Se tomaron fotografías de las huellas dactilares con una cámara de alta calidad. Las huellas dactilares impresas con tinta se adquirieron bajo la supervisión de operadores de pruebas.
	Huella dactilar impresa con tinta (mate)	3		
	Foto a color de la huella dactilar (brillante)	3	Se capturaron imágenes de cerca de los dedos de los sujetos de prueba y se imprimieron con la configuración de color y papel correspondiente. Las imágenes se midieron para que tuvieran aproximadamente el mismo tamaño que los dedos reales y se presentaron directamente al sensor.	
	Foto a color de la huella dactilar (mate)	3		
	Foto en blanco y negro de la huella dactilar (brillante)	2	Se capturaron imágenes de cerca de los dedos de los sujetos de prueba y se imprimieron con la configuración de color y papel correspondiente. Las imágenes se midieron para que tuvieran aproximadamente el mismo tamaño que los dedos reales y se presentaron directamente al sensor.	
	Foto en blanco y negro de la huella dactilar (mate)	3		

Para apoyar una clasificación más detallada de los tipos de ataque de nivel A, se tuvo en cuenta la naturaleza cooperativa frente a la no cooperativa de los tipos de ataque. Véase la sección 1.3 en referencia a los tipos de ataque cooperativos y no cooperativos.

³ Ataques exploratorios y de presentación suplementaria.



Tech 5 SA

Clasificación: Confidencialidad comercial



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:06:28 UTC-05:00

ID: 20378744940

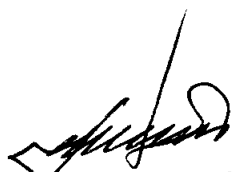
<https://cp.trasigna.com/documentos/validar/B1A497EE-15F4-4960-AA7E-D98D3F471BF1>



María Isabel Briceño Salazar

Fecha: 22/11/2023 14:06:47 UTC-05:00

ID: IDCPE-73039137


KAPAS S.A.C.
Jhonatan Escobar
Gerente General

000013

1.9.2 Perfil del equipo de pruebas

El reclutamiento de los sujetos de prueba se ajustó a la recomendación de la norma ISO/IEC 19795-5 a efectos de la inscripción y el reconocimiento en evaluaciones de pruebas. Por ende, se reclutó a un grupo de sujetos de prueba de 5 voluntarios para la evaluación PAD, compuesto de acuerdo con los requisitos de unicidad, consentimiento voluntario a la cantidad y el tipo de datos por recopilarse, incluida la distribución por edad, género y origen étnico. En las siguientes tablas, se describe el resumen de los datos demográficos del grupo de prueba. Las instrucciones operativas y el esquema de habituación de los sujetos de prueba a los dispositivos utilizados y al IUT se proporcionan en la sección 1.11.3

Presentaciones de buena fe.

Tabla 6 Distribución por grupo etario

Rango de edad	Procedente de BixeLab
< 18 años	-
18 – 30 años	Sí
31 – 50 años	No
51 – 70 años	Sí
> 70 años	-

Tabla 7 Distribución por género

Género	Porcentaje procedente de BixeLab
Masculino	67%
Femenino	33%

Tabla 8 Distribución por grupo étnico

Origen étnico	Procedente de BixeLab
Europa	Sí
Polinesia	-
Norte de África y Medio Oriente	-
Asia nororiental	Sí
Asia meridional y central	Sí
África subsahariana	-



Tech 5 SA

Clasificación: Confidencialidad comercial



COLEGIO DE TRADUCTORES DEL PERÚ
Fecha: 22/11/2023 14:09:29 UTC-05:00
ID: 20376744940
<https://ctp.lhsigne.com/documento/validar/B1A497EE-15F4-49B0-AA7E-D9BD3F4718F1>



Maria Isabel Briceño Salazar
Fecha: 22/11/2023 14:08:47 UTC-05:00
ID: IDCPE-73039137

KAPAS S.A.C.
Jonathan Escobar
Traductor

000014

Desviaciones y exclusiones

La norma ISO/IEC 30107-3 cubre los tipos de ataque de presentación, los tipos operativos del sistema y las técnicas de evaluación.

Este informe certifica únicamente los siguientes elementos evaluados:

- **Aplicación Tech 5 SA T-5 de huellas dactilares AirSnap (v2.4.6.8) – elemento sometido a prueba (IUT) para la evaluación PAD**
 - Ataques de clasificación de nivel A descritos en la Sección 3.1.1 Instrumentos de ataque de presentación.
 - La prueba del mecanismo PAD de la IUT correspondió a la evaluación del subsistema de clasificación PAD.
- A efectos de esta evaluación, los tipos de ataque de nivel A se subdividieron en ataques de nivel A no cooperativos y cooperativos. Esto se debió a que la solución de huellas dactilares se basa en fotografías del dedo de un sujeto en lugar de en los escáneres de huellas dactilares de contacto tradicionales (véase la página 12).
- BixeLab ha tomado todas las medidas necesarias para garantizar que no se produzcan desviaciones con respecto a las especificaciones de las normas.



Tech 5 SA

Clasificación: Confidencialidad comercial



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:09:29 UTC-05:00

ID: 20376744940

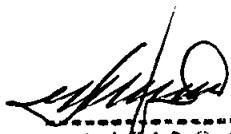
<https://ctc.theisgnc.com/documento/validar/B1A497EE-15F4-49B0-AA7E-D9B03F4718F1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137


KAPAS S.A.C.
Jhonatan Escobar
Gerente General

000015

Conclusiones y recomendaciones

Recomendaciones

BixeLab ha completado una evaluación PAD de Nivel 1 de la **aplicación Tech 5 SA T-5 de huellas dactilares AirSnap (v2.4.6.8)**. El propósito de este informe es presentar los resultados basados en las pruebas que se llevaron a cabo, así como las métricas que se generaron. Consulte la sección Conclusiones y observaciones en el Resumen ejecutivo de este informe.

Restricciones

BixeLab ha evaluado lo que considera una muestra representativa de la solución disponible en el mercado utilizando una metodología de prueba adecuada basada en las especificaciones de la norma ISO/IEC 30107-3.

Los resultados asociados a la evaluación PAD del IUT se han comunicado en la sección Resultados de rendimiento de este informe.

Consulte la sección Restricciones de la prueba para conocer las restricciones de la prueba asociadas a esta evaluación.

Nótese que los resultados presentados en este informe sirven para corroborar que la solución de la **aplicación Tech 5 SA T-5 de huellas dactilares AirSnap (v2.4.6.8)** ha sido sometida a pruebas de conformidad con la norma ISO/IEC 30107-3. Dado que la norma no proporciona criterios de aprobado o fallido para las métricas comunicadas, este informe no indica si se obtuvo un aprobado o fallido en relación con estas normas.

Desviaciones

A efectos de esta evaluación, los tipos de ataque de nivel A se subdividieron en ataques de nivel A no cooperativos y cooperativos. Esto se debió a que la solución de huellas dactilares se basa en fotografías del dedo de un sujeto en lugar de los escáneres de huellas dactilares de contacto tradicionales (véase la página 12).

BixeLab ha tomado todas las medidas necesarias para garantizar que no se produzcan desviaciones con respecto a las especificaciones de las normas.

Conclusiones

No hay otros comentarios o consideraciones de BixeLab que no se aborden en este informe.

Dr. Ted Dunstone
Responsable principal
ted@bixelab.com

17 de octubre de 2022



Tech 5 SA

Clasificación: Confidencialidad comercial



COLEGIO DE TRADUCTORES DEL PERU

Fecha: 22/11/2023 14:09:29 UTC-05:00

ID: 20376744940

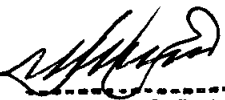
<https://cp.ihsigme.com/documento/validar/B1A497EE-15F4-4980-AA7E-D88D3F4718F1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137


KAPAS S.A.C.
Jonathan Escobar
Gerente General

000016

Anexo 1: Métricas de verificación

1.15 Evaluación PAD

El subsistema de verificación incluye el mecanismo PAD para el sistema sometido a prueba. Se prevé que el procedimiento de verificación sea remoto en un escenario del mundo real, lo que tiene repercusiones para el uso de artefactos y los intentos de captura no conformes. Los artefactos del mundo real pueden no necesitar un alto nivel de verosimilitud visual, y los participantes en la captura pueden experimentar con varios niveles de esfuerzos de captura no conformes para producir falsas coincidencias.

Por lo tanto, la evaluación PAD se realizó con políticas de presentación y decisión predefinidas, que se describen en las secciones 1.12 y 1.9.

Evaluación de subsistemas PAD: Evaluación de sistemas PAD basados en hardware o software.

Métricas para la evaluación de sistemas PAD -

Tasa de error de clasificación de presentación de ataques (APCER): proporción de presentaciones de ataques que utilizan los mismos tipos de instrumentos de ataque de presentación que se clasifican incorrectamente como presentaciones de buena fe en el subsistema PAD en un escenario determinado.

La APCER para un determinado tipo de instrumento de ataque de presentación (PAIS) se calcula del siguiente modo:

$$APCER_{PAIS} = 1 - \left(\frac{1}{N_{PAIS}} \sum_{i=1}^{N_{PAIS}} (RES_i) \right)$$

Donde N_{PAIS} es el número de presentaciones de ataque para el tipo de PAI del instrumento de ataque de presentación dado y RES_i toma el valor 1 si la i -ésima presentación se clasifica como presentación de ataque y el valor 0 si se clasifica como presentación de buena fe.

Tasa de error de clasificación de presentaciones de buena fe (BPCER): proporción de presentaciones de buena fe clasificadas incorrectamente como ataques a la presentación en el subsistema PAD en un escenario determinado.

La BPCER puede calcularse del siguiente modo:

$$BPCER = 1 - \frac{\sum_{i=1}^{N_{BF}} (RES_i)}{N_{BF}}$$

Donde N_{BF} es el número de presentaciones de buena fe. RES_i toma el valor 1 si la i -ésima presentación se clasifica como presentación de ataque y el valor 0 si se clasifica como presentación de buena fe.

Métricas para la evaluación completa del sistema: Se trata de evaluaciones integrales del sistema que incluyen los resultados del subsistema de comparación, además del subsistema PAD para los sistemas de verificación.

Sistemas de verificación o autenticación: Los resultados se presentan normalmente con Tasas de Coincidencia Falsa / Tasas de No Coincidencia Falsa con las muestras de buena fe. En el caso de las muestras de ataque, se informa de la Tasa de Coincidencia de Presentación de Ataque de Impostor (IAPMR). La IAPMR puede definirse como la proporción de presentaciones de ataque de impostores que utilizan el mismo tipo de PAI en que coincide con el objetivo de referencia.



Tech 5 SA

Clasificación: Confidencialidad comercial



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:09:29 UTC-05:00

ID: 20376744940

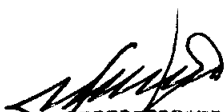
<https://cto.fisigne.com/documento/validar/B1A497EE-15F4-4980-AA7E-D98D3F4718F1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137


KAPAS S.A.C.
Jhonatan Escobar
j.escobar@kapas.com

000017

Anexo 2. Términos y definiciones

1.16 Glosario

Término	Abreviación	Definiciones
Potencial de ataque		Medida de la capacidad de atacar una IUT (TOE) dados los conocimientos, competencia, recursos y motivación del atacante.
Tipo de ataque		Elemento y característica de un ataque de presentación, incluidas los tipos de PAI, el ataque encubridor o impostor, el grado de supervisión y el método de interacción con el dispositivo de captura.
Presentaciones de buena fe		Presentaciones conformes a las especificaciones ANZ, es decir, autenticación de sujetos auténticos en condiciones de calidad ideales con su propia plantilla de huellas vocales.
Ataques encubridor		Cuando un actor intenta subvertir el sistema ocultando que sus datos biométricos están registrados en el sistema.
Ataques de identificación		Cuando un actor pretende ser identificado en una o varias búsquedas en una base de datos.
Ataques de registro		Cuando un actor intenta registrar una característica no viva con el fin de subvertir el sistema.
Tasa de error de clasificación de presentación de ataques	APCER	Proporción de las presentaciones de ataque que utilizan el mismo tipo de PAI clasificadas incorrectamente como presentaciones de buena fe en un escenario específico.
Tasa de error de clasificación de presentación de buena fe	BPCER	Proporción de presentaciones de buena fe clasificadas incorrectamente como ataques de presentación en un escenario específico.
Ataque de presentación	PA	Presentación al subsistema de captura de datos biométricos con el objetivo de interferir en el funcionamiento del sistema biométrico.
Detección de ataque de presentación	PAD	Determinación automatizada de un ataque de presentación.
Instrumento de ataque de presentación	PAI	Objeto utilizado en un ataque de presentación
Tipo de ataque de presentación	PAS	Clase de instrumentos de ataque de presentación creados con un método de producción común y basados en características biométricas diferentes.
Serie PAI		Instrumentos de ataque de presentación basados en un medio y método de producción comunes y una única fuente de características biométricas.
Implementación sometida a prueba	IUT	La que aplica la norma o normas sometidas a prueba.
Sujeto		La persona a la que se tomó el registro biométrico.



Tech 5 SA

Clasificación: Confidencialidad comercial



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:09:29 UTC-05:00

ID: 20376744940

<https://cjp.theigme.com/documento/validar/B1A487EE-15F4-49B0-AA7E-D6B03F4718F1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137

KAPA8 S.A.C.
Jhonatan Escobar

000018

		El objetivo del ataque.
Objetivo de la evaluación	TOE	Dentro de los Criterios Comunes, el producto informático objeto de la evaluación. Nota: El TOE en las evaluaciones de Criterios Comunes equivale al IUT en las evaluaciones biométricas.
Enfoque de la prueba		Consideraciones y factores que intervienen en la evaluación PAD
Verificador		La persona que simula el ataque PAD.

1.17 Documentos relacionados

Nombre del documento	Referencia
Evaluación del rendimiento biométrico Propuesta de servicios múltiples a Tech5 SA	Propuesta de evaluación de la solución Tech5 SA con respecto a las Directrices de detección de ataques de presentación de nivel 1 conforme a la norma ISO 30107-3.
Acuerdo de garantía de servicios totalmente ejecutado Tech 5 SA v1	Acuerdo de servicio totalmente ejecutado que menciona el alcance del proyecto, los entregables acordados, los plazos, los costes, las obligaciones del cliente y las expectativas.
ISO/IEC 30107-3:2017 (E)	Detección de ataques de presentación biométrica - Parte 3: Normas sobre pruebas e informes.



Tech 5 SA

Clasificación: Confidencialidad comercial



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:08:29 UTC-05:00

ID: 20376744940

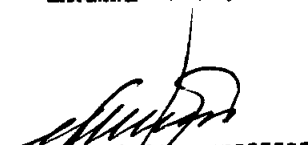
<https://cp.theigne.com/documento/validar/B1A497EE-15F4-49B0-AA7E-D9B03F4718F1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137


KAPA8 S.A.C.
Jhonatan Escobar
Calle 100 N° 100

000019

MARÍA ISABEL BRICEÑO SALAZAR
CTP N° 874

Traductora Colegiada Certificada
Español-Inglés-Portugués

TRADUCCIÓN CERTIFICADA DIGITAL N° 0857-2023
Página 14 de 15

Anexo 3: Registros de auditoría de la configuración

1.18 Evaluación PAD

Las especificaciones del Hardware del Cliente en el que se probó el sistema sometido a prueba (aplicación Tech5 SA) son las siguientes:

Nombre del fabricante y modelo	Especificaciones	Código BXL (si procede)	Sistema operativo	Número de serie	Anomalías identificadas	Versión del firmware	Fecha y hora de la comprobación
Apple iPhone 12 Pro	Teléfono móvil	TECH5 DEVICE 2	iOS	F17F9SSV0D92	N/A	15.1	12/08/2022 3:20 p. m.
Samsung S20+ 5G	Teléfono móvil	TECH5 DEVICE 4	Android 12	RFCN30L3NDR	N/A	One UI versión 4.0, Android versión 12	12/08/2022 3:29 p. m.
Samsung S20+ 5G	Teléfono móvil	TECH5 DEVICE 3	Android 12	RFCN20Y80VN	N/A	One UI versión 4.0, Android versión 12	15/08/2022 2:05 p. m.
Samsung S20+ 5G	Teléfono móvil	TECH5 DEVICE 4	Android 12	RFCN30L3NDR	N/A	One UI versión 4.0, Android versión 12	15/08/2022 2:23 p. m.



Tech 5 SA

Clasificación: Confidencialidad comercial



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: 20376744940

<https://dtp-design.com/documento/validar/B1A487EE-15F4-49B3-AA7E-D36D3F4719F1>



María Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137

KAPAS S.A.C.
Jhonatan Escobar
Gerente General

000020

Anexo 5: Lista de tablas

1.19 Documentos internos y externos

En esta sección figura una lista de todos los documentos pertinentes utilizados para esta evaluación.

Tabla 12 Lista de documentos internos

Número de versión	Título	Abreviatura / Código de BixeLab	Fecha	Propietario
Documentos contractuales				
V1.0	Propuesta de servicios múltiples de la evaluación del rendimiento biométrico a Tech 5 SA	BXL_016	11 de mayo de 2022	-
V1.0	Acuerdo de Garantía de Servicios Tech5 SA v1.0			-
V1.1	Acuerdo de garantía de servicios totalmente ejecutado Tech 5 SA			-
Procedimientos				
V1.2	Procedimiento de atención al cliente	BXL_09_CSP	-	BixeLab
V1.2	Procedimiento sobre condiciones ambientales y de las instalaciones	BXL_07_FEC	-	BixeLab
v1.1	Procedimiento de equipamiento	BXL_08_EPP		BixeLab
v1.2	Procedimiento del método de prueba	BXL_10_TMP		BixeLab
Documentos del proyecto				
V1.0	BXL_TestPlan_Tech5_v1.0	22-016-TP-00 Tech 5 SA	30 de junio de 2022	-

Tabla 13 Lista de documentos externos

Número de versión	Título	Abreviatura / Código de BixeLab	Fecha	Propietario
-	30107-1	-	2016	ISO/IEC
-	30107-3	-	2017	ISO/IEC



Tech 5 SA

Clasificación: Confidencialidad comercial



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:09:29 UTC-05:00

ID: 20376744940


<https://cp.theigme.com/documento/validar/B1A497EE-15F4-49B0-AA7E-09B03F4718F1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137


KAPAS S.A.C.
Jonathan Escobar
Gerente General

000021

Presentation Attack Detection Level 1 Evaluation Services - Test Report

Prepared for

Tech 5 SA

by

BixeLab

3/16 Bentham Street, Yarralumla,
ACT 2600, Australia

PAD Level 1 Evaluation for:

Tech 5 SA T-5 AirSnap Fingerprint (v2.4.6.8) Application – item under test (IUT)



Document Code 22-016-TR-01

Submit Date 17 October 2022

Submitted by BixeLab Pty Ltd

Contact Ms. Somya Singh

M: 0412802334

E: s.singh@bixelab.com



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:09:28 UTC-05:00

ID: 20375744940


<https://cp.thsigne.com/documento/validar/01A497EE-15F4-4900-AA7E-09D03F471BF1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137


KAPAS S.A.C.
Jhonatan Escobar
Gerente General

000022

Version History

Version Number	Description of change	Author	Date
V1.0	Initial version (Draft)	BixeLab	15/09/2022
	Additional information added in the executive summary		
V1.01	Re-classified Level B's have been restored to Level A cooperative attack types	BixeLab	17/10/2022



BIXELAB PTY LTD PROPRIETARY NOTICE



Classification: Commercial in confidence



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:09:29 UTC-05:00

ID: 20376744940


<https://cp.thesigne.com/documento/validar/61A487EC-15F4-49B0-AA7E-D9B03F4718F1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137


KAPAS S.A.C.
Jhonatan Escobar
Gerente General

000023

1.7 Configuration Audit

An audit of the system configuration in the IUT submitted for PAD evaluation was conducted on each day of testing. The information recorded is outlined in an audit log that includes hardware and software specifications, OS versions, serial number, and build.

This audit log is to verify that all software and hardware configurations related to each testing remained unchanged through the execution. The aim is to mitigate system software and hardware related variations and to perform essential laboratory protocol for integrity.

Tables in the section Appendix 3: Configuration Audit Logs provide detailed configuration audit logs focusing on the above with no identified anomalies.

1.8 Expected Outputs

1.8.1 Expected Output Data

Summary of the expected output data from the IUT is provided in the table below.

Table 2 Summary of Expected output data

IUT Component	Components	Output	Score Range	(Options based on known threshold
Presentation Attack (liveness) Detection	Liveness	Liveness Score	0 – 100	Pass (≥ 50) Fail (< 50)
	Image Quality	NFIQ2 Score	0 – 100	N/A

The IUT used a liveness Score threshold of 50 (0.5) to make decisions for whether the acquired sample was live (pass) or artificial (fail). The NIST Fingerprint Image Quality (NFIQ) 2 is an open-source software that defines a standardised quality score for fingerprint images. The NFIQ2 Score output details the quality of the acquired sample.

1.8.2 Expected Output Performance

In traditional biometric performance evaluations, ground truth plays a pivotal role to ensure the validity of the reported error metrics. In PAD evaluation context, the ground truth relates to whether a given liveness detection response is genuine and bona fide or represents an imposter (attack).

The metrics will include an attack presentation classification error rate (APCER) and a bona fide presentation classification error rate (BPCER) for evaluating the performance of presentation attack mechanisms in the IUT.

The purpose of the PAD evaluation was to measure the accuracy of the liveness detection mechanism. A bona fide presentation referred to a live human subject submitting fingerprints as directed by the application, and a presentation attack referred to the test operator mounting the target's biometric using a PAI.



Classification Commercial in confidence



COLEGIO DE TRADUCTORES DEL PERU

Fecha: 22/11/2023 14:08:29 UTC-05:00

ID: 20376744940

<https://cp.thesign.com/documento/validar/61A497EC-15F4-49B0-AA7E-D9B03F471BF1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137

RAPAS S.A.C.
Jhonatan Escobar
Gerente General

000024

Here, the expected output for a bona fide presentation was a liveness score greater than or equal to 50 (0.5), and an attack presentation should have returned a liveness score less than 50 (0.5). The table below summarises the expected output performance for the PAD evaluation in liveness detection.

Table 3 Summary of expected output performance for IUT

Target of Evaluation Component	Component Classification	Components	Ground Truth	Result Options based on known threshold
Presentation Attack Detection	Primary	Liveness	Bona fide	Pass (≥ 50)
			Attack	Fail (< 50)
	Secondary	Image Quality	Bona fide	N/A ²
			Attack	

² ISO 30107-3 asserts that "there is no reason to assume a certain quality level from [PAD] artefacts". Therefore, there should be no assumption of quality correlated with attack type.



Classification: Commercial in confidence



COLEGIO DE TRADUCTORES DEL PERÚ
 Fecha: 22/11/2023 14:09:28 UTC-05:00
 ID: 20376744940
<https://cp.thesigne.com/documento/validar/31A4975C-15F4-49B0-AA7E-D9B03F4718F1>



Maria Isabel Briceño Salazar
 Fecha: 22/11/2023 14:08:47 UTC-05:00
 ID: IDCPE-73039137

KAPAS S.A.C.
 Jhonatan Escobar
 Gerente General

000025

Dataset Description

1.9 PAD Evaluation

1.9.1 Presentation Attack Instruments

The presentation attack types utilised in this evaluation were based on operational thresholds for the highest score achieved in following criteria to establish the rationale for making substantial biometric security claim about the system under test:

- **Type:** A designation of the artefact defined by its properties and origin.
- **Access to biometric characteristics:** The relative ease of access to suitable sources from which the artefact can be produced.
- **Equipment/Cost:** The relative difficulty and expense to produce the artefact.

These factors are described in the table below.

Table 4 Presentation attack species assessment

Classification	Levels	Description
Type	Simple	Typically, two-dimensional and/or repurposed from another source
	Specialised	Typically, three-dimensional, and/or specially produced or altered from a source
	Sophisticated	Specifically produced, sophisticated artefacts that typically leverage multiple high-quality sources
Access to biometric characteristics	Easy	Publicly or commonly available, usually without knowledge of the target
	Moderate	Usually requires cooperation of the target or access to the biometric or biometric template itself
	Difficult	Usually requires multiple sources which may be altered or augmented. Often involves access to the biometric or biometric template itself
Equipment/cost	Low	Can be produced with standard materials using office or home equipment
	Medium	May require the use of generic suppliers, software, or equipment
	High	May require the use of specialised suppliers, software, or equipment



Classification: Commercial in confidence



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:09:29 UTC-05:00

ID: 20376744940

<https://cp.thsigne.com/documento/validar/B1A497E1-15F4-49B0-AA7E-09B03F4718F1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137

RAPAS S.A.C.
Jonathan Escobar
Escobar

000026

Presentation attack species (as artefact types) were created based on both source of the biometric characteristics and ISO/IEC 30107-3 criteria for artefact property creation, provenance, usage, and handling – pertaining from creation to test utilisation – as formalised criteria to evaluation of PAD mechanisms. As specified in section 8.1 of the ISO/IEC 30107-3 standard, the presentation attacks planned for this evaluation fell into the category of biometric imposter attacks and had the following three properties:

1. The samples appeared as natural biometric characteristics to the IUT
2. The samples appeared as natural biometric characteristics to the biometric data quality checks in place for the IUT
3. The samples acquired by the device camera from the presented artefact contained extractable features that matched against the targeted individual's references.

Based on ISO assessment criteria, the presentation attack species were then classified into Levels A and B. The test operator posing as an attacker had access to each level of attack representations based upon the original biometric characteristics obtained through cooperative subjects. The table below provides a specification of presentation attacks, level classifications and number of sources per attack species.

Table 5 Summary of Presentation Attack species

Presentation Attack Level	Artificial Presentation Attack Instruments	Source	Description	Presentation Technique
A (non-cooperative)	B&W Candid Photo of Fingerprint	2	Test subjects' fingers were captured with a camera from a few meters distance, and the captured images were cropped to extract the subjects' individual fingers. These were sized to be approximately the same size as real life fingers, printed, and then presented to the sensor directly	Uncooperative – Biometric characteristics were captured simulating uncooperative conditions (i.e., participant waving in a photo). This is to simulate an attacker sourcing biometrics from social media and other publicly available photo sources.
	Lifted Fingerprint with Cellotape	2	Test subjects' fingerprint was placed on the glass similar to the Residual Fingerprint on Glass and was lifted using tape. The piece of tape was placed against a dark background to help the finger ridges show more easily and was presented directly to the sensor.	
	Residual Fingerprint on Glass	2	Test subjects moisturised finger and placed it on a glass. The print that was left on the glass was then directly used against the sensor.	



Classification: Commercial in confidence



COLEGIO DE TRADUCTORES DEL PERÚ
Fecha: 22/11/2023 14:08:29 UTC-05:00
ID: 70579744943
<https://dcp.thalga.com/documentos/validez/5F4497EE15F44960AA7E09B03F473F1>



Maria Isabel Bencio Solazar
Fecha: 22/11/2023 14:08:47 UTC-05:00
ID: IDOPE-73039137

KATA S.A.C.
Jonathan Escobar
11/11/2023

000027

Presentation Attack Level	Artificial Presentation Attack Instruments	Source	Description	Presentation Technique
A (cooperative)³	Ink Pressed Fingerprint (Glossy)	3	Test subjects placed their fingers in ink and pressed it against Matte and Glossy Paper. The resulting impressions were left to dry overnight and presented to the sensor.	Cooperative – Biometric characteristics were captured directly from test crew participants in addition to some additional participants who did not participate in person but provided their biometrics for the purpose of creating presentation attacks. Photos of fingerprints were taken on a high quality camera. Ink pressed fingerprints were acquired under supervision of test operators.
	Ink Pressed Fingerprint (Matte)	3		
	Colour Photo of Fingerprint (Glossy)	3	Close up images of the test subjects' fingers were captured and printed with the respective colour and paper configuration. The images were sized to be approximately the same size as real-life fingers, and were presented to the sensor directly	
	Colour Photo of Fingerprint (Matte)	3		
	B&W Photo of Fingerprint (Glossy)	2	Close up images of the test subjects' fingers were captured and printed with the respective colour and paper configuration. The images were sized to be approximately the same size as real-life fingers, and were presented to the sensor directly	
	B&W Photo of Fingerprint (Matte)	3		

To support further classification of Level A attack types, the cooperative vs. uncooperative nature of the attack types was taken into consideration. Refer to section 1.3 in reference to cooperative and non-cooperative attack types.

³ Exploratory and supplementary presentation attacks



Classification: Commercial in confidence



COLEGIO DE TRADUCTORES DEL PERÚ
 Fecha: 22/11/2023 14:08:29 UTC-05:00
 ID: 20375744943
<https://csp.thelga.com/documentos/val/67A4B7EE-15F4-436C-AA7E-D96D3F47-9F1>



Maria Isabel Briceño Solazar
 Fecha: 22/11/2023 14:08:47 UTC-05:00
 ID: IDCPE-73039137

KAPAS S.A.C.
 Jonathan Escobar
 Director General

000028

1.9.2 Test Crew Profile

The recruitment of test subjects was aligned with the ISO/IEC 19795-5 recommendation for the purpose of enrolment and recognition in testing evaluations. As such, a test subject crew of 5 volunteers was recruited for PAD evaluation and composed according to requirements for uniqueness, voluntary consent to the amount and type of data to be collected, including the distribution of age, gender, and ethnicity. Summary of the test crew demographics is described in the tables below. The operational instructions and outline of habituation of test subjects to devices used and IUT are provided in section 1.11.3 Bona Fide Presentations.

Table 6 Age group distribution

Age Range	BixeLab sourced
< 18 y/o	-
18 – 30 y/o	Yes
31 – 50 y/o	No
51 – 70 y/o	Yes
> 70 y/o	-

Table 7 Sex distribution

Sex	BixeLab sourced percentage
Male	67%
Female	33%

Table 8 Ethnic group distribution

Ethnic Origin	BixeLab sourced
European	Yes
Polynesian	-
North African and Middle Eastern	-
North-East Asian	Yes
Southern and Central Asian	Yes
Sub-Saharan African	-



Classification: Commercial in confidence



COLEGIO DE TRADUCTORES DEL PERU
Fecha: 22/11/2023 14:09:29 UTC-05:00
ID: 20376744940
<https://cip.ihugne.com/documento/validarID?AA97EE:5F4-49D0-AA7E-D98D3F4718F1>



Maria Isabel Briceño Salazar
Fecha: 22/11/2023 14:08:47 UTC-05:00
ID: IDCPE-73039137

KAPAS S.A.C.
Jonathan Escobar
Director General

000029

Deviations and Exclusions

ISO/IEC 30107-3 covers the presentation attack types, system operational types, and evaluation techniques.

This report certifies only the following items evaluated:

- **Tech 5 SA T5 AirSnap Finger (v2.4.6.8) – item under test (IUT) for PAD evaluation**
 - Attacks involved Level A classification attacks as described in [Section 3.1.1 Presentation Attack Instruments](#).
 - Testing of PAD mechanism of the IUT corresponded to evaluation of the PAD classification subsystem.
- For the purposes of this evaluation, Level A attack types were sub-divided into non-cooperative and cooperative level A attacks. This was as the fingerprint solution is based on photographs of a subject's finger rather than traditional contact fingerprint scanners (refer to page 12).
- BixeLab has taken every measure to ensure that no deviations were made from the specifications of the standards.



Classification: Commercial in confidence



COLEGIO DE INADJUDICADOS DEL PERÚ

Fecha: 22/11/2023 14:09:29 UTC-05:00

ID: 20376744940


<https://cp.thysign.com/documento/validar/31A497CE-15F4-49BD-AA7E-09BD3F4718F1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137


CAPAS S.A.C.
Norlan Escobar
Gerente General

000030

Findings and Recommendations

Recommendations

BixeLab has completed a Level 1 PAD evaluation of **Tech 5 SA T5 AirSnap Finger (v2.4.6.8)**. The purpose of this report is to present findings based on the testing that was undertaken as well as the metrics that were generated. Please refer to the Findings and Observations section in the Executive Summary of this report.

Constraints

BixeLab has evaluated what it believes to be a representative sample of the commercially available solution with the utilisation of appropriate testing methodology stemming from the specifications of the ISO/IEC 30107-3 standard.

The results associated with the PAD evaluation of the IUT have been reported in section Performance Results of this report.

Please refer to section Test Constraints for test constraints associated with this evaluation.

Note that the results presented in this report serve substantiate that the **Tech 5 SA T5 AirSnap Finger (v2.4.6.8)** solution has undergone testing in accordance with the ISO/IEC 30107-3 standard. As the standard does not provide pass or fail criteria for the reported metrics, this report does not indicate a pass or fail in association with these standards.

Deviations

For the purposes of this evaluation, Level A attack types were sub-divided into non-cooperative and cooperative level A attacks. This was as the fingerprint solution is based on photographs of a subject's finger rather than traditional contact fingerprint scanners (refer to page 12).

BixeLab has taken every measure to ensure that no deviations were made from the specifications of the standards.

Conclusions

There are no other comments or thoughts from BixeLab that are not addressed in this report.

Dr. Ted Dunstone
Senior Responsible Officer
ted@bixelab.com

17th October 2022



Classification: Commercial in confidence



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:09:29 UTC-05:00

ID: 20376744940

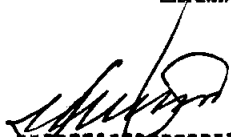
<https://cp.thissigne.com/documento/validar/31A497E1-15F4-49B0-AA7E-D9B03F4718F1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137


KAPAS S.A.C.
Karla Escobar
Traductora

000031

Appendix 1: Verification Metrics

1.15 PAD Evaluation

The verification subsystem includes the PAD mechanism for the system under test. The verification procedure is anticipated to be remote in a real-world scenario, which has ramifications for artefact usage and non-conformant capture attempts. Real-world artefacts may not need a high level of visual plausibility, and capture participants may be able to experiment with various levels of non-conformant capture efforts to produce false matches.

Hence, PAD evaluation was undertaken with pre-defined presentation and decision policies as described in sections 1.12 and 1.9.

PAD Subsystem Evaluation: Evaluation of PAD systems which is either hardware or software based

Metrics for PAD system evaluation –

Attack Presentation Classification Error Rate (APCER): proportion of attack presentations using same presentation attack instrument species that are incorrectly classified as bona fide presentations at the PAD subsystem in a certain scenario

APCER for a given presentation attack instrument species (PAIS) is calculated as follows:

$$APCER_{PAIS} = 1 - \left(\frac{1}{N_{PAIS}} \right) \sum_{i=1}^{N_{PAIS}} (RES_i)$$

Where N_{PAIS} is the number of attack presentations for the given presentation attack instrument PAI species and RES_i takes the value 1 if the i th presentation is classified as an attack presentation and value 0 if classified as bona fide presentation.

Bona fide Presentation Classification Error Rate (BPCER): proportion of bona fide presentations incorrectly classified as presentation attacks at the PAD subsystem in a certain scenario.

BPCER can be calculated as follows:

$$BPCER = 1 - \frac{\sum_{i=1}^{N_{BF}} (RES_i)}{N_{BF}}$$

Where N_{BF} is the number of bona fide presentations. RES_i takes the value 1 if the i th presentation is classified as an attack presentation and value 0 if classified as bona fide presentation.

Metrics for full system evaluation – These are end-to-end system evaluations including the comparison subsystem results in addition to PAD subsystem for verification systems

Verification or authentication Systems: The results are normally presented with False Match Rates/ False Non-Match Rates with the bona fide samples. In case of attack samples, Imposter Attack Presentation Match Rate (IAPMR) is reported. IAPMR can be



Classification: Commercial in confidence



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:09:29 UTC-05:00

ID: 20376744940

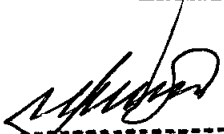
<https://cp.theagne.com/documento/validar/31A4975C-75F4-49B0-AA7E-1D9B03F4718F1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137


KAPA8 S.A.C.
Jonathan Escobar
Gerente General

000032

defined as the proportion of imposter attack presentations using the same PAI species in which the target reference is matched.



Classification: Commercial in confidence



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:09:29 UTC-05:00

ID: 20376744940


<https://cp.thsigne.com/documento/validar/61A497LE-15F4-49B0-AA7E-D9D03F4718F1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137



KAPA8 S.A.C.
Jonathan Escobar
Gerente General

000033

Appendix 2: Terms and Definitions

1.16 Glossary

Term	Abbreviation	Definitions
Attack potential		Measure of the capability to attack an IUT (TOE) given the attacker's knowledge, proficiency, resources and motivation
Attack type		Element and characteristic of a presentation attack, including PAI species, concealer or impostor attack, degree of supervision, and method of interaction with the capture device
Bona fide presentations		Presentations conforming to ANZ specifications i.e., genuine subject authentication under ideal quality conditions against their own voiceprint template
Concealer attacks		When an actor attempts to subvert the system by concealing that their biometric is enrolled in the system
Identification attacks		When an actor is attempting to be identified in a one-to-many search of a database
Enrolment attacks		When an actor attempts to enrol a non-live characteristic for the purpose of subverting the system
Attack Presentation Classification Error Rate	APCER	Proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario
Bona fide Presentation Classification Error Rate	BPCER	Proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario
Presentation Attack	PA	Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system
Presentation Attack Detection	PAD	Automated determination of a presentation attack
Presentation Attack Instrument	PAI	Object used in a presentation attack
Presentation Attack Species	PAS	Class of presentation attack instruments created using a common production method and based on different biometric characteristics
PAI series		Presentation attack instruments based on a common medium and production method and a single biometric characteristic source
Implementation Under Test	IUT	That which implements the standard(s) being tested
Subject		The person from whom the biometric enrolment was taken. The target of the attack.
Target Of Evaluation	TOE	Within Common Criteria, the IT product that is the subject of the evaluation. Note: The TOE in Common



Classification: Commercial in confidence



COLEGIO DE TRADUCTORES DEL PERÚ

Fecha: 22/11/2023 14:09:29 UTC-05:00

ID: 20376744940


<https://cp.cbsignet.com/documento/validar/81A497E1-15F4-4900-AA7E-09B03F471BF1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137


KAPAS S.A.C.
Jonathan Escobar
Gerente General

000034

		Criteria evaluations is the equivalent of IUT in biometric evaluations.
Test approach		Totality of considerations and factors involved in PAD evaluation
Tester		The person performing the simulated PAD attack.

1.17 Related Documents

Document Name	Reference
Biometric Performance Evaluation Multi Service Proposal to Tech5 SA	Proposal for evaluation of Tech5 SA solution against the ISO 30107-3 Presentation Attack Detection Level 1 Guidelines
Fully Executed Services Assurance Agreement Tech 5 SA v1	Fully executed service agreement lists the project scope, agreed deliverables, timelines, costs, client obligations, and expectations
ISO/IEC 30107-3:2017 (E)	Biometric presentation attack detection – Part 3: Testing and reporting standard



Classification: Commercial in confidence



COLEGIO DE INADJUDICADOS DEL PERÚ
Fecha: 22/11/2023 14:09:29 UTC-05:00
ID: 20376744940

<https://cp.itagene.com/documento/validar/31A4975E-15F4-49B0-AA7E-09B03F4718F1>



Maria Isabel Briceño Salazar

Fecha: 22/11/2023 14:08:47 UTC-05:00

ID: IDCPE-73039137

KAPAS S.A.C.
Ronatan Escobar
Gerente General

000035

Appendix 3: Configuration Audit Logs

1.18 PAD Evaluation

Specifications for the Client Hardware on which the system under test (Tech5 SA application) was tested are recorded below

Manufacturer & Model Name	Specifications	BXL CODE (if Applicable)	Operating System	Serial Number	Identified Anomalies	Firmware Version	Date and Time Check Performed
Apple iPhone 12 Pro	Mobile Phone	TECH5 DEVICE 2	iOS	F17F9SSV0D92	N/A	15.1	12/08/2022 3:20pm
Samsung S20+ 5G	Mobile Phone	TECH5 DEVICE 4	Android 12	RFCN30L3NDR	N/A	One UI version 4.0, Android version 12	12/08/2022 3:29pm
Samsung S20+ 5G	Mobile Phone	TECH5 DEVICE 3	Android 12	RFCN20Y80VN	N/A	One UI version 4.0, Android version 12	15/08/2022 2:05pm
Samsung S20+ 5G	Mobile Phone	TECH5 DEVICE 4	Android 12	RFCN30L3NDR	N/A	One UI version 4.0, Android version 12	15/08/2022 2:23pm




Classification: Commercial in confidence



COLEGIO DE TRADUCTORES DEL PERU
Fecha: 22/11/2023 14:08:29 UTC-05:00
ID: 20376744943
<https://dcp.thelga.com/documento/validerB?A497EE15F443BDAA7E05BD3F4713F1>



Maria Isabel Briceño Salazar
Fecha: 22/11/2023 14:08:47 UTC-05:00
ID: IDOPE 73039137


KAPA8 S.A.C.
Jonathan Escobar
Gerente General

000036

Appendix 5: List of Tables

1.19 Internal and External Documents

This section provides a list of all relevant documents utilised for this evaluation

Table 12 List of Internal Documents

Version Number	Title	Abbreviation/ BixeLab code	Date	Owner
Contractual Documents				
V1.0	Biometric Performance Evaluation Multi Service proposal to Tech 5 SA	BXL_016	11 May 2022	-
V1.0	Services Assurance Agreement Tech5 SA v1.0			-
V1.1	Fully Executed Services Assurance Agreement Tech 5 SA			-
Procedures				
V1.2	Customer Service Procedure	BXL_09_CSP	-	BixeLab
V1.2	Facilities and Environmental Conditions Procedure	BXL_07_FEC	-	BixeLab
v1.1	Equipment Procedure	BXL_08_EPP		BixeLab
v1.2	Testing Method Procedure	BXL_10_TMP		BixeLab
Project Documents				
V1.0	BXL_TestPlan_Tech5_v1.0	22-016-TP-00 Tech 5 SA	30 June 2022	-

Table 13 List of External Documents

Version Number	Title	Abbreviation/ BixeLab code	Date	Owner
-	30107-1	-	2016	ISO/IEC
-	30107-3	-	2017	ISO/IEC




Classification: Commercial in confidence



COLEGIO DE TRADUCTORES DEL PERÚ
Fecha: 22/11/2023 14:09:29 UTC-05:00
ID: 20376744940
<https://cp.thesign.com/documentos/validar/51A497EE-15F4-49B0-AA7C-D96D3F471BF1>



Maria Isabel Briceño Salazar
Fecha: 22/11/2023 14:08:47 UTC-05:00
ID: IDCPE-73039137


JAS S.A.C.
Juan Jacobo
Proprietario

000037