



LINEAMIENTOS 54 - HERRAMIENTAS BIOMÉTRICAS DE VERIFICACIÓN COMPLEMENTARIA

DESCRIPCION

Denominamos como “*herramientas biométricas de verificación complementaria (bvc)*” a aquellos sistemas, módulos, dispositivos, etc., que permiten que un sistema a desarrollar, o que ya se encuentre desarrollado, adquiera la capacidad de ofrecer un método de seguridad de acceso adicional, dentro del entorno en el que presta servicio, mediante la comparación de los datos biométricos registrados previamente en la fase de enrolamiento, con los datos presentados por el usuario al momento de ingresar al sistema, o a la hora de realizar consultas u operaciones.

Como ejemplo, al conocido factor simple de autenticación (user/pass) que se encuentra en innumerables sistemas, se le suman normalmente comprobaciones de más datos patronímicos, como ser totalidad o parcialidad del Documento Nacional de Identidad, direcciones, o preguntas, que son todas en formato de texto, con la finalidad de reducir las debilidades que posee.

En busca de mejorar la seguridad, algunos sistemas ya implementan el doble factor (user/pass+pk), lo que permite asociar a un nombre de usuario, una clave y una firma electrónica o una firma digital.

El objetivo de este lineamiento, es exponer una lista de sugerencias para implementar otras formas de doble factor de autenticación no dependientes de una infraestructura de pki, sino de parámetros biométricos (user/pass+bio); o bien para agregar un tercer factor de autenticación biométrico (user/pass+pk+bio), a sistemas que ya poseen doble factor de autenticación.

CARACTERÍSTICAS GENERALES

Método BVC:

- a) Dinámica de tecleo
- b) Unidactilar
- c) Vascular
- d) Facial
- e) Iris
- f) Vocal

Como información adicional y dependiendo del sistema o herramienta, podemos dar





un marco conceptual, bajo ningún contexto taxativo, y siendo el mismo acorde a la actualidad de cuando se generó el presente documento:

	Facilidad de USO (1)	Aceptación de los usuarios (2)	Perennidad (3)	Certidumbre (4)
Dinámica de tecleo	ALTA	ALTA	VARIABLE	ALTA
Unidactilar	ALTA	ALTA	MUY ALTA	MUY ALTA
Vascular	ALTA	ALTA	ALTA	MUY ALTA
Facial	ALTA	ALTA	ALTA	ALTA
Iris	MEDIA	MEDIA	ALTA	MUY ALTA
Vocal	ALTA	ALTA	ALTA	ALTA

- (1) Se refiere a la interacción usuario con el dispositivo de verificación acorde a diversos proyectos, culturas y legislaciones. Por lo cual varía según su entorno de aplicación
- (2) Se refiere a experiencias de usuario a nivel internacional, acorde a diversos proyectos, culturas y legislaciones. Por lo cual varía según su entorno de aplicación.
- (3) Corresponde a la persistencia del mismo rasgo o comportamiento biométrico a lo largo del tiempo. Cabe señalar que las dinámicas podrían variar según el proceso de re empadronamiento definido para cada proyecto.
- (4) En algunos casos varía según entornos (por ejemplo facial) y profesiones (por ejemplo dactilar).

Casos de uso:

Bajo la premisa de ilustrar algunos factibles casos de uso podríamos señalar extensivamente pero no taxativamente los siguientes ejemplos:

	Acceso a Áreas Críticas	Acceso a sistemas internos o plataformas	e-kioscos



Dinámica de tecleo (contemplar los casos de teclado reducido)	-	ALTA	MEDIA
Unidactilar	MUY ALTA	ALTA	ALTA
Vascular (contemplar tema de costos)	MUY ALTA	ALTA	ALTA
Facial (Contemplar ambientación)	ALTA	ALTA	ALTA
Iris (contemplar tema de costos)	MUY ALTA	ALTA	ALTA
Vocal (contemplar ruido ambiente)	ALTA	ALTA	ALTA

Nota 1:

La selección del BVC dependerá del requirente en virtud de las necesidades y características propias del proyecto donde será implementado. Es dable entender que las condiciones de uso en por ejemplo estaciones tipo “kiosco” no son las mismas que en sistemas “web on-line” por lo que cada requirente será el responsable de la selección.

Para todas y cada una de las BVC listadas deberá requerirse como mínimo la siguiente información:

Tipo de búsqueda:

Puede seleccionar una o ambas opciones.

- a) Búsqueda uno contra uno (1:1)
- b) Búsqueda uno contra todos los registros(1: N)

Velocidad:

Entre los puntos a requerir deberá estar especificado:

- a) Velocidad de enrolamiento
- b) Velocidad de búsqueda (1:1) en caso de requerirse



c) Velocidad de búsqueda (1: N) en caso de requerirse

La velocidad que se especifique debe ser acorde a las necesidades del proyecto, y deberá justificarse técnicamente, ya que es un parámetro que si se especifica en exceso, podría limitar innecesariamente el espectro de oferentes posibles.

Certidumbre:

La forma de especificar la “certidumbre” en la detección, es mediante algunos de los siguientes parámetros, los que se indican en la forma de porcentajes. Al igual que para la velocidad, la certidumbre que se especifique debe ser acorde a las necesidades del proyecto, y deberá justificarse técnicamente, ya que el valor indicado podría limitar innecesariamente el espectro de oferentes posibles:

a) TAR = “true acceptance rate” = tasa de aceptación o verificación verdadera

Representa la medida en que el sistema biométrico iguala correctamente los datos de la misma persona

Sugerencia: Cuanto más alto mejor.

b) FAR = “false acceptance rate” = tasa de falsa aceptación o verificación

Representa la medida en que el sistema biométrico iguala correctamente los datos de una persona (a) con la de otra persona (b), reportando un falso

Sugerencia: Cuanto más bajo mejor.

c) TRR = “true rejection rate” = tasa de rechazo o no verificación verdadera

Representa la frecuencia en que los sistemas no encuentran a una persona en la base de datos y ciertamente esa persona no está en la base de datos

Sugerencia: Cuanto más alto mejor.

d) FRR = “false rejection rate” = tasa de falso rechazo

Representa la frecuencia en que los sistemas no encuentran a una persona en la base de datos pero esa persona si se encuentra en la base de datos

Sugerencia: Cuanto más bajo mejor.

Nota 2:

Cabe aclarar que las mediciones de verdaderos y falsos son interdependientes, esto es, conociendo una medida la otra puede calcularse.

e) EER = “equal error rate” = tasa de error igual

Se desprende de la medición del FAR y su comparación con el FRR.

Sugerencia: para que sea óptimo, si es posible, se debe regular la sensibilidad del dispositivo biométrico de modo que el FAR sea igual al FRR. En esa



condición, cuanto más bajo el EER, mayor precisión se obtendrá en la medición.

f) FTE = “failure to enroll” = tasa de falla de enrolamiento

Representa la cantidad de personas cuyos rasgos biométricos se han tratado de inscribir en el sistema y el sistema no las aceptó.

Si el sensor biométrico funciona correctamente, y las condiciones ambientales son adecuadas, esto puede ser ocasionado por problemas físicos del individuo. Sugerencia: Cuanto más bajo mejor.

g) FTA = “failure to acquire rate” = tasa de falla de obtención (biométrica)

Representa la cantidad de personas cuyos rasgos biométricos se han tratado de inscribir en el sistema y el sistema no los aceptó, aunque los individuos eran aptos para ser inscriptos.

Esto puede ser ocasionado por condiciones ambientales como ser la luz o fallas en el sensor biométrico.

Sugerencia: Cuanto más bajo mejor.

Nota 3:

Como guía de las cifras a requerir debemos considerar la cantidad de personas que utilizara nuestro sistema. Por ejemplo: si esperamos un fallo cada 100 el FAR requerido deberá ser igual o menor a “FAR=1,0%”, si esperamos un fallo cada 1000 el FAR requerido deberá ser igual o menor a “FAR=0,1%”, y así sucesivamente.

DISPOSITIVOS:

Si bien no todos los métodos biométricos de comportamiento o físicos requieren dispositivos de adquisición de datos o estos ya pueden estar a disposición del requirente, se requiere la siguiente información:

Existencia:

- a) Requiere dispositivos de adquisición
- b) No requiere dispositivos de adquisición

Lenguaje:

Deberá contar con uno o varios de los drivers para el correcto funcionamiento bajo los siguientes sistemas operativos:

- a) Microsoft Windows
- b) Linux
- c) IOS



- d) Android
- e) Otros <indicar>

Deberá incluir los kit de desarrollo de software (SDK) para desarrollos de aplicativos de software basados en DLL's, controles ActiveX u otras soluciones de ágil integración a entornos de desarrollo.

Deberá detallar el tipo de licencia (exclusiva/no exclusiva) y el tiempo de vigencia de la misma.

PRIVACIDAD

Nota 4:

La administración de base de datos de personas debe ser declarada en la "Dirección Nacional de Protección de Datos Personales" (Ley 25.326).

ESTÁNDARES A TENER EN CUENTA

A los fines de ampliar el conocimiento se señalan algunos estándares que podrían ayudar a comprender las tecnologías a utilizar:

	Documentación
Dinámica de tecleo	<i>Estándar en estudio</i>
Unidactilar	ISO/IEC 19794-2:2005
Vascular	<i>Estándar en estudio</i>
Facial	ISO/IEC 19794-5:2011
Iris	ISO/IEC 19794-6:2011
Vocal	<i>Estándar en estudio</i>