REGISTRADURÍA
NACIONAL DEL ESTADO CIVIL

DOCUMENTO DE BUENAS PRÁCTICAS

AUTENTICACIÓN DE IDENTIDAD CON LA BASE DE DATOS BIOGRÁFICA Y BIOMÉTRICA DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL

GRUPO DE ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SEPTIEMBRE DE 2018

REGISTRADURÍA
NACIONAL DEL ESTADO CIVIL

Contenido

Introducción

La Registraduría Nacional del Estado Civil, ha evidenciado la importancia de proponer buenas prácticas orientadas al debido desarrollo de las actividades derivadas del proceso de autenticación biométrica.

Es así, que ha decidido elaborar este documento de BUENAS PRÁCTICAS que constituye una herramienta necesaria para obtener una adecuada prestación del servicio y mayor seguridad durante todo el ciclo de vida del proceso.
Esté documento esta dirigido a todos los actores que se involucran directa e indirectamente en el proceso de autenticación biométrica como son las entidades públicas y privadas, operadores biométricos, desarrolladores de software e integradores de soluciones tecnológicas, así como usuarios finales de la aplicación que consume el servicio de autenticación biométrica.

Resumen

El presente documento define las buenas prácticas que deben aplicar las entidades que acceden al proceso de autenticación biométrica con la base de datos dispuesta por la Registraduria Nacional del Estado Civil. Su aplicación es indispensable para prevenir y mitigar los riesgos presentes en cada una de las etapas previas y posteriores a la puesta en producción del servicio, siendo una medida estratégica y necesaria para la prevención del fraude, empleando estándares internacionales de seguridad informática, garantizando el debido tratamiento y custodia de la Información que produce y administra la Registraduría Nacional del Estado Civil, en pro de la debida autenticación de identidad de los colombianos en trámites y servicios en los que se utiliza el proceso de autenticación biométrica; en garantía de la protección de datos personales, la reserva de la información y confidencialidad de la información.

Objetivo general

Orientar y concienciar a las entidades que acceden a la información biográfica y biométrica que produce y administra la Registraduría Nacional, a través, del proceso de

autenticación biométrica, en cuanto a la aplicación de buenas prácticas en los procedimientos previos y posteriores al uso de las herramientas tecnologías dispuestas para la autenticación de identidad de los colombianos.

Objetivos específicos

- Sensibilizar acerca de los riesgos y consecuencias asociadas al uso indebido de la información que es consultada y los efectos de la omisión de la aplicación de las políticas de seguridad durante las diferentes etapas del proceso.
- Advertir la importancia de aplicar una adecuada y continua capacitación a los usuarios finales que utilizan herramientas para el consumo del servicio de autenticación biométrica.
- Describir las actividades que deben contemplar como críticas las entidades que acceden a la información que produce y administra la Registraduría Nacional del Estado Civil a través del proceso de autenticación biométrica.
- Documentar las buenas prácticas y riesgos relacionados al proceso de autenticación biométrica.
- Verificar el cumplimiento de lo plasmado en este documento a través de visitas en sitio por parte de la Registraduría sobre las entidades que acceden al servicio de autenticación biométrica.

Justificación

Conocedores de las casuísticas que podrían impactar el debido uso y resultados del proceso de autenticación biométrica y toda vez que se han identificado diferentes circunstancias que podrían afectar el buen uso y desempeño de las herramientas dispuesta para la autenticación de identidad de las personas, el debido tratamiento de los datos, poniendo en riesgo las operaciones de las entidades usuarias por posibles falsas aceptaciones en las transacciones que desarrollan durante sus labores cotidianas, se considera necesario emitir este compilado de buenas prácticas para garantizar la operación oportuna y exitosa del proceso de verificación de identidad a partir de la biometría dispuesta por la RNEC.

Alcance

Las actividades que se describen a continuación, van dirigidas a la alta gerencia, aliados tecnológicos, desarrolladores de software e integradores de soluciones tecnológicas, así como a los usuarios finales de las aplicaciones que accederán el servicio de autenticación biométrica con la base de datos de la Registraduría Nacional del Estado civil. La aplicación de dichas actividades, permitirán mitigar riesgos en la operación y garantizar el debido uso de las soluciones tecnológicas para lograr el mayor nivel de precisión y fiabilidad de la autenticación de identidad de los colombianos.

Principios y acciones a cargo de las entidades que acceden a las bases de datos que produce y administra la Registraduría Nacional del Estado Civil.

1. ACTIVIDADES A CARGO DE LAS ENTIDADES PARTIENDO DE LA ALTA GERENCIA.

1.1. Disposición al cumplimiento de la normatividad vigente

Garantizar el cumplimiento de obligaciones estipulada en contratos o convenios referentes al debido uso de la información, cumplimiento de las restricciones de no copiar, reproducir la información y/o complementar bases de datos a partir de la información consultada y suministrada a través del servicio de autenticación biométrica, esto tiene sustento ya que las bases de datos biográficas y biométricas que produce y administra la Registraduría Nacional del Estado Civil gozan de reserva legal, tienen conexidad a asuntos de defensa y seguridad nacional y la información en ellas es absolutamente dinámica, toda vez que los datos asociados a la identidad de los colombianos tienen variaciones respecto a los hechos del estado civil que modifican datos biográficos, a las afectaciones por vigencia de los documentos de identidad a partir de la información que reportan más de 19000 autoridades en el país, al igual que a ordenes emitidas por autoridades competentes que refieren cambios en los dato de identidad de los colombianos, por lo que el utilizar bases de datos propias, no solo coarta restricciones legales sobre el uso de la información, sino que también pone en riesgo las operaciones que se realicen sobre datos no actualizados y fidedignos de los colombianos.

Lo expuesto está orientado a garantizar la integridad, confidencialidad y disponibilidad de la información.

1.2. Responsabilidad del tratamiento de la información

Debe recordarse que la RNEC tiene la función constitucional de identificación de los colombianos, aunado a las condiciones de conexidad de su información con asuntos de defensa y seguridad nacional, motivo por el cual, no está autorizada la copia, reproducción, almacenamiento parcial o completo de información, pudiéndose configurar los delitos de acceso abusivo a un sistema informático (artículo 269 A), violación de datos personales (artículo 269F) y la tipificación de circunstancias de agravación punitiva contempladas en los numerales 1,3,5 y 8 del artículo 269H del Código Penal Colombiano (Ley 599 de 2000), entre otros.

1.3. Utilización de herramientas homologadas por la RNEC

Es de obligatorio cumplimiento emplear en los procesos de biometría las herramientas homologadas y autorizadas por parte de la Registraduría Nacional, en cuanto a hardware (dispositivos de autenticación biométrica integrados, captores biométricos) verificando que se encuentren configurados los parámetros de detección de materiales (dedo falso), dedo vivo y cifrado de minucia por hardware; así como del software y comunicaciones (infraestructura). Los dispositivos homologados se encuentran publicados en el link https://wsp.registraduria.gov.co/biometria/dispositivos/

1.4. Capacitación continua

Llevar a cabo procesos de inducción y reinducción a los funcionarios de la entidad, para que conozcan el proceso, herramientas, datos suministrados por los aplicativos; haciendo énfasis en la debida aplicación de políticas de seguridad de la información, la importancia e implicaciones del proceso de autenticación biométrica y sobre la aplicación de las recomendaciones indicadas en este documento.
De igual manera las entidades deberán definir, documentar y capacitar a los funcionarios que hacen uso de la autenticación biométrica sobre el procedimiento para la captura de huellas, indicando claramente el debido proceso para la verificación de identidad, así como la importancia de recopilar y contar con el consentimiento previo, expreso e informado del colombiano para el tratamiento de sus datos personales.

1.5. Actualización de la información suministrada a la Registraduría

Mantener informada a la Registraduría Nacional en cuanto a los equipos, usuarios y sedes autorizadas para el proceso de autenticación biométrica a través de cada uno de los sitios web dispuestos para dicho propósito, toda vez que el servicio será restringido y de estricto uso para aquellos previamente informados y autorizados por la Registraduría Nacional del Estado Civil.

1.6. Conexiones remotas

Prohibir el uso de cualquier software de conexión remota, fuera de los autorizados por cada entidad dentro de sus procesos misionales.

1.7. Tratamiento de datos a nivel Nacional

Garantizar que los servidores utilizados para el proyecto, se encuentren ubicados dentro del territorio nacional, la información biográfica y biométrica no puede salir del país. Se encuentra prohibida la transferencia internacional de datos personales de los colombianos respecto de la información suministrada a través de la consulta a la base de datos biométrica de la Registraduría Nacional del Estado Civil, en consonancia con el Artículo 26 de la Ley 1581 de 2012.

1.8. Alistamiento inicial

Realizar las inversiones de tiempo y logística necesarias para la apropiación de buenas prácticas en el servicio. Esto contempla actividades como:

- Un periodo de estabilización del servicio a partir de la entrada en producción con el servicio de autenticación biométrica, en donde se deben afinar en la práctica los procedimientos definidos y monitorear o auditar de manera proactiva, los resultados y la efectividad del servicio.
- Inducción y reinducción dirigidas a los operadores del sistema con el objeto de enfocar medidas para el correcto uso de los dispositivos biométricos al igual que las verificaciones de seguridad para la captura de impresiones dactilares, así como de las especificaciones de seguridad de la cédula de ciudadanía colombiana.

1.9. Mecanismos alternos al proceso de autenticación biométrica.

Definir mecanismos alternos al proceso de autenticación de biométrica, para los casos en los que no sea posible capturar las impresiones dactilares del ciudadano con la calidad suficiente para realizar un cotejo biométrico electrónico. Debe tenerse en cuenta que el artículo 18 del Decreto 019 de 2015 regula el procedimiento alterno a aplicar ante imposibilidad de validación biométrica por causas físicas del titular, al respecto, recuérdese que la verificación de la identidad se hará mediante la comparación de su información biográfica con la que reposa en la base de datos de la Registraduría Nacional del Estado Civil.

La entidad reportará a la Registraduría Nacional a través de los enlaces establecidos, únicamente los inconvenientes relacionados con inconsistencias sobre los datos de identificación del ciudadano o la no existencia de los mismos en el sistema.

2. ACTIVIDADES A CARGO DE ALIADOS TECNOLÓGICOS, DESARROLLADORES DE SOFTWARE E INTEGRADORES DE SOLUCIONES TECNOLÓGICAS

2.1. Cumplimiento de la normatividad

Diseñar el software de cotejo biométrico con todos los requisitos funcionales, técnicos y características de seguridad estipuladas y exigidas en los anexos técnicos No. 1 y No. 2 de la Resolución 5633 de 2016 con sus respectivas actualizaciones impartidas por la Registraduría Nacional, cumplir con las disposiciones legales y compromisos de confidencialidad suscritos, y las demás que la Entidad considere, al igual que determinar esfuerzos con el objeto de garantizar el cumplimiento de las políticas de seguridad de la información.

2.2. Selección aleatoria del dedo a cotejar y digitación del número de cédula.

El software de captura biométrica debe seleccionar de manera aleatoria el o los dedos a autenticar, de manera que no sea a elección del funcionario ni del ciudadano, ni que los índices (derecho o izquierdo) sean la primera opción. Para los módulos desatendidos esta opción debe ser de estricto cumplimiento. De igual manera, el software deberá incorporar un control para la digitación del número de cédula, donde se parametrice en

10 el máximo de caracteres y donde no se acepte la digitación de caracteres especiales. Adicionalmente la entidad evaluará si incorpora un espacio para la confirmación cuando se digite el número de cédula antes de enviar la solicitud a la base de datos de la Registraduría Nacional.

2.3. Buffer de memoria

Implementar mecanismos con el fin de eliminar o vaciar el buffer de memoria en los servidores de los operadores biométricos como matcher y orquestadores, entre otros, cada vez que sea entregado el resultado de un cotejo, con el fin de evitar que los resultados de cotejos anteriores generen confusiones o falsas aceptaciones en el proceso.

2.4. Cantidad máxima de intentos para consulta de una cédula

Se recomienda que el software contenga un parámetro de número de intentos con la misma cédula de ciudadanía, lo anterior, para evitar que el funcionario realice varios intentos con resultado no satisfactorio.

3. ACTIVIDADES A CARGO DE USUARIOS FINALES Y DE ATENCIÓN AL CLIENTE.

3.1. Verificación de las manos del ciudadano

Verificar cada uno de los dedos del ciudadano previo a realizar cada cotejo biométrico para determinar si el ciudadano no tiene desgaste natural de huellas o sufre algún tipo de dermatitis que le impida realizar verificación de identidad con las soluciones electrónicas dispuestas, esta práctica también permite verificar que el usuario no porte algún tipo de material que simule una huella digital, en intentos de suplantación de personas. Si bien es cierto el captor biométrico puede detectar materiales falsos, estas verificaciones refuerzan la seguridad del procedimiento.

3.2. Autorización de tratamiento de datos personales

Informar al ciudadano de manera previa respecto al procedimiento que se está realizando al momento de capturar la huella dactilar, al igual que indicarle la política de tratamiento de datos.

3.3. Limpieza del captor biométrico

Suministra kit de limpieza para mantener el captor biométrico limpio y sin residuos, toda vez que cada cotejo va dejando marcas de impresiones dactilares sobre el cristal del captor, lo cual podría generar lecturas y resultados no óptimos.

3.4. Debida utilización del captor biométrico

Ubicar el captor biométrico con la orientación correcta y en un lugar alejado de la luz directa del sol. Cualquiera de estas dos situaciones podría impactar de manera negativa la captura correcta de las impresiones dactilares. Así mismo se debe evitar la toma de huella rodada, el funcionario de la entidad deberá observar la manera como el cliente impone su dedo sobre el captor y evidenciar que sea de manera horizontal, plana y estática.
Evitar la toma de huella parcial o dedo mal ubicado en el captor, lo cual incide en la extracción de la minucia y por ende en la respuesta que suministra por parte del operador biométrico.

3.5. Procedimiento alterno al proceso de autenticación biométrica.

El funcionario deberá acatar el mecanismo alterno previamente definido por la entidad, para verificar o validar la identidad de las personas que por algún motivo médico (desgaste natural de huellas o algún tipo de dermatitis) no puedan ser autenticadas utilizando el proceso electrónico de verificación de identidad.

3.6. Políticas de seguridad de la información

Los funcionarios adscritos al proceso de autenticación biométrica deberán cumplir a cabalidad con las políticas de seguridad de la información emitidas por la Entidad. La

Registraduría Nacional realizará visitas en sitio para verificar el cumplimiento de las mismas.

3.7. Número de cédula del colombiano.

El funcionario deberá constatar que el número de cédula que incorpora para la autenticación es correcto, con el objeto de evitar imprecisiones en la validación.

3.8. Reinicio del software de autenticación biométrica.

El funcionario de la entidad deberá reiniciar la aplicación cuando el comportamiento del software sea anormal o presente fallas a la hora de autenticar a un ciudadano.