POL-028 POLITICA DE SEGURIDAD PARA DISPOSITIVOS DE SISTEMAS BIOMETRICOS

Versión Nro. 01

CONTENIDO

1. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
1	2020-11-23	Creación del Documento

2. INTRODUCCIÓN

El presente documento se elabora para suministrar un set de políticas que permitan aumentar la seguridad de los dispositivos que intervienen con el proceso de reconocimiento y/o registro de información de ciudadanos, los cuales interactúan con las soluciones de biometría desarrolladas por Olimpia,

3. OBJETIVO

Establecer condiciones de seguridad para los dispositivos que intervienen con el proceso de reconocimiento y/o registro de información de ciudadanos los cuales interactúan con las soluciones de biometría desarrolladas por Olimpia.

4. ALCANCE

Esta política aplica para los dispositivos que capturen información biométrica de los ciudadanos con el fin de cotejar con la base de datos administrada por la Registraduría Nacional.

5. POLÍTICAS

5.1. CONTRACTUAL

- Las políticas del presente documento deben ser cumplidas por los clientes autorizados, usuarios del sistema biométrico de Olimpia y terceros involucrados por los mismos.
- El acceso de consulta a la base de datos de la Registraduría Nacional del Estado Civil lleva implícito el deber de acatar todas las normas de seguridad de la información emitidas por esa entidad, por lo tanto, cualquier incumplimiento a las misma podrá llevar a la inmediata suspensión y/o terminación del contrato de suministro del servicio como operador biométrico.
- La recolección, almacenamiento y cualquier tratamiento de información por medios diferentes a los dispuestos por Olimpia constituye una violación a la presente política. Será responsabilidad de cada cliente de Olimpia asegurar que el tratamiento de la información se realice en los términos de las resoluciones emitidas por la RNEC.
- Con el fin de garantizar un adecuado nivel de seguridad, todo trabajador que preste sus servicios debe conocer, antes de su vinculación las responsabilidades asignadas al rol en cuanto a las labores que va a realizar y su grado de responsabilidad con la Seguridad de la Información.
- Cada persona que ya esté vinculada o que se esté vinculando con la organización debe propender por la protección de los activos que han sido entregados a su cargo; así mismo se deben tener claramente identificados los propietarios, custodios y usuarios de los activos de información.
- Se hace necesario que cada uno de los contratos realizados con los trabajadores incluyan las responsabilidades que de acuerdo con su cargo tienen con la seguridad de la información, y deben suscribir junto con el contrato un acuerdo de confidencialidad comprometiéndose con la protección, no divulgación de la

información confidencial que accedan o manejen por motivos de la prestación de sus servicios, en caso de ya estar vinculados firmar otro si para el conocimiento y aceptación de los mismos.

- Las personas a las que se les asigne usuarios que operaran la solución deben poseer contrato laboral o de prestación de servicios con los clientes y firmar acuerdo de confidencialidad.
- Contar con medios de comunicación suficientes y adecuados que garanticen que los usuarios conocen y aceptan las políticas que deben cumplir.
- Los equipos deben contar con un sistema operativo y aplicativos licenciados.
- Las cuentas de sesión de la estación donde opera el sistema biométrico deben ser no administradora para los usuarios que realizaran validación biométrica, cuyas contraseñas estarán definidas según las directrices de Olimpia.

5.2. ANTE SUPLANTACIONES

- Reportar a Olimpia y entes de control cualquier intento de suplantación detectado frente al uso del sistema.
- Cuando el estado de vigencia reportado por RNEC indique posible suplantación el ciudadano debe acercarse a la Registraduría a solicitar la rectificación.
- El cliente debe registrar las máquinas y dispositivos que usara para la validación biométrica en una plataforma suministrada por Olimpia y auditada por RNEC
- Informar a Olimpia cualquier cambio de hardware id y/o ubicación geográfica.
- Informar de manera inmediata a Olimpia cuando usuarios registrados en la aplicación tengan ausencia temporal o permanente y merezcan des habilitación de este.
- Los sistemas que incluyan autenticación por contraseña no deben utilizar contraseñas por defecto, en blanco, ni iguales a los nombres de cuenta.
- Las contraseñas en el sistema son de uso personal e intransferible, por lo que deben ser protegidas por el usuario.

- Los usuarios del sistema biométrico deben bloquear sus sesiones abiertas al alejarse de sus estaciones de trabajo, así mismo contar con un bloqueo automático cuando los equipos se desatiendan por más de cinco (5) minutos.

5.3. ANTE POSIBLES FALLAS O DEBILIDADES DEL SISTEMA BIOMÉTRICO

- Alertar a Olimpia cuando la solución biométrica presente fallas, irregularidades o se identifique debilidades en la misma.

5.4. INFORMACIÓN EN PROCESAMIENTO Y TRANSMISIÓN

- Los equipos deben contar con software antivirus y componentes de seguridad activos y actualizados, que no afecten la operación del sistema biométrico.
- Es responsabilidad de los clientes autorizados mantener los equipos informáticos, libres de cualquier tipo de malware, con medidas preventivas, y efectuar sobre las mismas revisiones periódicas a fin de garantizar el funcionamiento óptimo y seguridad de los equipos.
- No instalar software de propósito malicioso en sistemas que interactúen con la aplicación.
- Se debe deshabilitar el autorun para los medios extraíbles.
- Las aplicaciones y dispositivos que requieran conexión a redes e internet deben estar en redes propias, no compartidas, protegidas y que los equipos conectados en la misma sean autorizados.
- Las conexiones que se realicen mediante redes inalámbricas deben utilizar por lo menos el estándar de cifrado WPA2.

5.5. HARDWARE E INFORMACIÓN ALMACENADA

- Garantizar que las instalaciones cuenten con medidas y procedimientos para evitar daños, robos y accesos indebidos.

- Impedir el ingreso a las instalaciones de personal que se presente en nombre de Olimpia y carezca de identificación como empleado, en caso de presentarse una visita sin previo aviso se debe corroborar la identificación y obtener autorización de la mesa de servicio al cliente de Olimpia.
- Emplear medidas de protección para la sobrecarga de voltaje.
- Ante pérdida, daño, alteración y robo de elementos del sistema biométrico, se debe notificar a Olimpia para realizar el debido proceso.
- No extraer archivos generados por la instalación de la aplicación del sistema biométrico de Olimpia.
- Cuando el disco duro donde ha sido instalada la aplicación del sistema biométrico se deba cambiar por cualquier motivo, este debe ser entregado a Olimpia para efectuar borrado seguro de la información.

6. PROPIEDAD DE OLIMPIA

El presente documento es de carácter **confidencial** y está protegido por las normas de derechos de autor, cualquier reproducción, distribución o modificación total o parcial a usuarios no autorizados o cualquier uso indebido de la información confidencial será considerado un delito conforme a lo establecido por el Código Penal y Leyes vigentes del estado Colombiano.