ESPECIFICACIONES TECNICAS REQUERIDAS

COMPONENTE DE SEGURIDAD PARA SOLUCION DE IDENTIFICACION BIOMETRICA

- La solución debe contar con acceso completamente WEB para usuario final.
- La solución debe tener alcance integral y funcional bajo una sola instalación, es decir, que no requiere de módulos externos o aplicaciones de terceros para lograr su completo desempeño funcional definido dentro del actual proyecto.
- La solución debe contar con sistema operativo propio integrado, bajo procesos de hardening y ajustado a la solución, No debe depender de hardware o software en funcionamiento para su normal operación.
- Debe tener la capacidad de crear usuarios localmente en una base de datos integrada y cifrada dentro de la solución para brindar acceso y aplicar políticas de seguridad a los mismos.
- Debe contar con la capacidad de llevar a cabo gestión de usuarios y grupos locales para aplicar políticas de seguridad y acceso desde la misma aplicación, es decir, esta funcionalidad debe estar inmersa, almacenada, cifrada y gestionada sin uso de recursos externos tales como bases de datos, módulos o software periférico para su operación, además que no debe generar costos adicionales en licenciamiento.
- Debe permitir la creación de múltiples portales de acceso a través de instancias basadas en subdominios, las cuales puedan conectarse de forma independiente a Directorios de usuarios externos de forma simultánea. Debe soportar dominios y subdominios múltiples sobre la misma instalación.
- Debe tener la capacidad de conectar tanto un Directorio Externo (LDAP) como con la base de usuarios creados localmente de forma simultánea entre los distintos portales o instancias a exponer. La integración con diferentes servicios de directorio (Active Directory, eDirectory y LDAP en general) se debe realizar de forma simultánea y transparente, sin requerimiento de plugins o extensiones sobre el servicio de directorio.

- Debe permitir configuraciones de Single Sign On para las aplicaciones web y/o Escritorios Remotos sin requerir la modificación o ajuste a las bases de datos de usuarios y/o de repositorios de usuarios.
- No debe utilizar software cliente o agentes para brindar acceso a servicios o aplicaciones web, carpetas compartidas y escritorio remoto. No debe requerir el uso de VPN´s.
- Debe contar con procesos de restablecimiento de contraseña segura tanto para el repositorio local y el repositorio remoto (LDAP) por parte del usuario a través de un correo electrónico alterno.
- Debe contar con la capacidad de autenticar usuarios mediante mecanismos solido (autenticación doble factor): OTP token, Llaves hardware, enigma, reconocimiento facial u otros para usos futuros.
- El componente de seguridad debe soportar los protocolos FIDO 2, OPEN ID CONNECT y SAML 2.0.
- Debe controlar el acceso de usuarios a todos los recursos y/o aplicativos web o escritorios remotos a través de un único portal para todos los usuarios definidos por el cliente con base en identificación biométrica facial.
- Debe permitir personalización del portal de acceso principal para que se ajuste a los estándares e imagen corporativa basado en HTML5.
- Debe permitir la comunicación encriptada/cifrada de información.
- Debe contar con funcionalidades de proxy inverso para la publicacion de aplicaciones además de cifrar la comunicación brindando mayor nivel de seguridad evitando el uso de Vpn´s.
- Debe generar enmascaramiento de la URL original de acceso a las aplicaciones para no revelar la ubicación final de las mismas.
- Debe entregar registros de trazabilidad para auditoria con intentos fallidos indicando usuario, fecha, hora y dirección IP, información del último cambio de contraseña realizado y la dirección IP de la máquina desde la cual se realizó el cambio.

CARACTERISTICAS TECNICAS DEL COMPONENTE DE SEGURIDAD PARA LA IDENTIFICACIÓN BIOMETRICA.

1. No debe requerir recursos de infraestructura adicionales para su configuración y operación tales como hardware o software una vez se entregue en producción.
2. Debe ser compatible con las herramientas de virtualización como Virtual Box, V.M. Ware, Hyper V, XEN, KVM, Proxmox.
3. Debe contar con mecanismos de prestación del servicio en clúster de alta disponibilidad activo-activo, activo-pasivo. Debe contar con balanceo de carga automático a través de los nodos de una instalación clúster.
4. Debe permitir el Re- direccionamiento de todo el tráfico a través de un único puerto seguro 443 (SSL/TLS).
5. Debe soportar los protocolos: TCP/IP, UDP/IP, HTTP, HTTPS, SMB, HTML5 RDP Client, SAML 2.0, SSL/TLS, XML, WEB-Services, PKI, OPEN VPN, HTML, HTML5, OCSP, LDAP, LDAPS, NTLMv1, OATH TOTP, OpenID Connect, OpenID RP. Todo de forma integral, sin módulos o componentes externos.
6. Debe garantizar la protección de las credenciales de usuario dentro del sistema, durante su transporte hacia y desde la aplicación, utilizando conexión segura fuerte, mediante el protocolo SSL –TLS 1,2 como mínimo.

COMPONENTE DE BIOMETRIA

- El componente debe contar con verificación biométrica dactilar, de iris o facial para confirmar la identidad de un individuo utilizando estos medios como una forma de identificación biométrica.
- El componente deberá mediante la toma de imágenes del documento de identidad del usuario (Cédula de Ciudadanía Colombiana) establecer si el documento es legítimo y que no cuenta con alteraciones con las

características de seguridad de los documentos de identidad presentadas por la Registraduría Nacional del Estado Civil.

- El componente deberá contar con la capacidad de extraer información de las imágenes tomadas del documento de identidad a través de tecnología de OCR.
- El componente deberá contar con la capacidad de clasificar el documento de identidad y extraer los datos de las ubicaciones correspondientes dentro de los campos de datos definidos en una configuración requerida.
- El componente debe generar la emisión de certificados de trazabilidad del proceso de identificación presentando todas la variables del proceso para garantizar un proceso jurídico en caso de ser requerido. El componente debe recopilar la mayor cantidad posible de información técnica sobre el dispositivo, incluyendo diversos puntos de datos como datos de usuario (rostros, huellas), información del dispositivo y detalles de la red.
- El componente deberá tener la capacidad de emitir como mínimo tres (3) decisiones finales para las sesiones:
  - Aprobado: Se completa la verificación del usuario y el aplicativo sugiere que se lo considere como un usuario verificado.
  - Rechazado: Es probable que el usuario está involucrado en fraude, haya sido víctima de robo de identidad o manipulación. El aplicativo no recomienda proporcionarle servicio.
  - Reenvío: El usuario no proporcionó al componente toda la información necesaria (imágenes, huellas), algunas de las imágenes pueden ser de baja calidad o el usuario final presentó un documento incompatible. En este caso, se sugiere que se le pida al usuario final que repita el proceso de sesión de verificación.
- El componente deberá contar con la capacidad de detectar:
  - Baja similitud de rostros y huellas
  - Mala nitidez de la imagen del documento

- El componente deberá tener la capacidad de detectar que el documento tiene una fecha expirada en caso de requerirse.
- El componente deberá tener la capacidad de detectar que el documento esta visiblemente recortado.
- El componente deberá tener la capacidad de detectar que la persona de la del documento de identidad no es la misma que se encuentra solicitando el servicio.
- El componente deberá tener la capacidad de detectar que la zona horaria del dispositivo y la red no coinciden.
- El componente deberá tener la capacidad de detectar que la red y el país del operador no coinciden: el país de origen de la tarjeta SIM es diferente del país de la red conectada.
- El componente deberá tener la capacidad de detectar el emulador de SDK: se emuló el flujo móvil en una computadora.
- La solución deberá solicitar repetir el proceso cuando
    - Falta videos y/o fotos.
    - Mala calidad de imagen.
    - Documento dañado.
    - Tipo de documento no admitido.
    - Documento expirado.

ENTRE OTRAS SOLUCIONES

Se busca implementar un sistema de biometría avanzado con el objetivo de satisfacer las necesidades específicas de nuestra organización. La intención es adoptar soluciones seguras que sean comparables a las tecnologías biométricas existentes, como huellas dactilares o escaneo de iris, sistema facial y otros. Este sistema de biometría pretende mejorar la seguridad y la eficiencia en el acceso a nuestros pacientes.

Tomando como referencia soluciones exitosas basadas en tecnologías de huella dactilar, escaneo de iris o facial. La seguridad y precisión son factores críticos para garantizar la integridad del sistema y evitar posibles amenazas de falsificación o suplantación de identidad.

La privacidad y el cumplimiento normativo son consideraciones prioritarias en el diseño e implementación de este sistema de biometría. Se buscará cumplir con los estándares y regulaciones aplicables para garantizar la protección de los datos biométricos y la privacidad de los usuarios.

En resumen, teniendo en cuenta lo anterior se pretende establecer un sistema de biometría robusto y seguro que incorpore tecnologías similares a las soluciones de huella dactilar, escaneo de iris, facial y otros. Este sistema deberá ser fácilmente integrable, garantizando la seguridad, precisión y privacidad necesarias para cumplir con las exigencias de nuestra organización.