

# ASSISTID

## Estándares de Calidad Aplicados al Proyecto

### Información del Proyecto

**Nombre del Proyecto:** Sistema de Asistencia por Reconocimiento Facial

**Descripción:** Aplicación móvil que permite a los alumnos registrar su asistencia en las materias correspondientes mediante tecnología de reconocimiento facial.

### Normas y Estándares Aplicados

#### 1. ISO/IEC 25010 - Calidad del Producto de Software

Esta norma define un modelo de calidad para productos y sistemas de software, organizando las características de calidad en ocho categorías principales.

#### Características de Calidad Aplicadas:

Característica	Sub-característica	Aplicación en el Proyecto	Métrica/Criterio de Aceptación
<b>Adecuación Funcional</b>	Compleitud funcional	La app debe cubrir todas las funciones necesarias: registro facial, validación de identidad, registro de asistencia, consulta de historial	100% de las funcionalidades especificadas implementadas
	Corrección funcional	El sistema debe registrar correctamente la asistencia sin errores	Tasa de error < 1% en registros de asistencia
	Pertinencia funcional	Las funciones deben facilitar específicamente el registro de asistencia académica	Validación con usuarios finales (alumnos y docentes)
<b>Eficiencia de Desempeño</b>	Comportamiento temporal	El reconocimiento facial y registro de asistencia debe ser rápido	Tiempo de reconocimiento < 3 segundos; Tiempo total de registro < 5 segundos
	Utilización de recursos	La app debe funcionar eficientemente en dispositivos móviles con recursos limitados	Uso de RAM < 150MB; Uso de batería < 5% por sesión; Tamaño de app < 50MB

	Capacidad	El sistema debe soportar múltiples usuarios simultáneos	Capacidad para 500+ usuarios concurrentes sin degradación del servicio
<b>Compatibilidad</b>	Coexistencia	La app debe funcionar junto con otras aplicaciones del dispositivo	No conflictos con apps comunes (WhatsApp, navegadores, etc.)
	Interoperabilidad	Integración con sistemas de gestión académica existentes	API REST funcional para intercambio de datos con SGA
<b>Usabilidad</b>	Capacidad de reconocimiento	Interfaz intuitiva y fácil de entender para alumnos	90% de usuarios pueden completar registro sin ayuda
	Capacidad de aprendizaje	Proceso de registro facial inicial simple y guiado	Tiempo de aprendizaje < 5 minutos
	Operabilidad	Navegación sencilla y controles accesibles	Máximo 3 toques para completar cualquier acción principal
	Accesibilidad	Diseño accesible para personas con discapacidades	Cumplimiento WCAG 2.1 nivel AA; soporte para lectores de pantalla
<b>Fiabilidad</b>	Madurez	Sistema estable sin fallos frecuentes	MTBF (tiempo medio entre fallos) > 720 horas
	Disponibilidad	Servicio disponible durante horarios académicos	Disponibilidad del 99.5% en horario de clases
	Tolerancia a fallos	El sistema debe continuar operando ante fallos menores	Modo offline para registro temporal; sincronización posterior
	Capacidad de recuperación	Recuperación rápida ante fallos del sistema	Tiempo de recuperación < 2 minutos
<b>Seguridad</b>	Confidencialidad	Protección de datos biométricos y personales de alumnos	Encriptación AES-256 para datos en reposo y en tránsito
	Integridad	Prevención de modificación no autorizada de registros de asistencia	Firma digital de registros; logs de auditoría inmutables

	No repudio	Registro verificable de todas las asistencias	Timestamp y hash criptográfico de cada registro
	Autenticidad	Verificación de identidad mediante reconocimiento facial	Tasa de acierto > 99%; Tasa de falsos positivos < 0.1%
<b>Mantenibilidad</b>	Modularidad	Arquitectura modular que permita actualizaciones independientes	Separación clara entre módulos de UI, reconocimiento facial, backend
	Reusabilidad	Componentes reutilizables para futuras funcionalidades	Mínimo 60% de código reutilizable
	Analizabilidad	Logs y métricas para diagnóstico de problemas	Sistema de logging completo; dashboard de métricas
	Capacidad de modificación	Facilidad para implementar cambios y mejoras	Tiempo promedio para implementar cambios menores < 2 días
	Capacidad de prueba	Facilidad para realizar pruebas automatizadas	Cobertura de código > 80%; suite de pruebas automatizadas
<b>Portabilidad</b>	Adaptabilidad	Funcionamiento en diferentes versiones de sistemas operativos móviles	Soporte Android 8.0+ (sin soporte iOS)
	Capacidad de instalación	Instalación sencilla desde tiendas de aplicaciones	Proceso de instalación estándar; < 2 minutos
	Capacidad de reemplazo	Migración desde sistema de asistencia manual existente	Herramientas de migración de datos; documentación completa

## 2. ISO/IEC 19794-5 - Datos de Reconocimiento Facial

Esta norma especifica los formatos de intercambio de datos para información de reconocimiento facial, garantizando interoperabilidad y calidad de las imágenes biométricas.

### Requisitos Aplicados:

Aspecto	Requisito de la Norma	Implementación en el Proyecto	Criterio de Cumplimiento
<b>Formato de Imagen</b>	Formatos estandarizados para	Captura y almacenamiento de imágenes en formato	100% de imágenes en formato estándar

	imágenes faciales	JPEG2000 o PNG	
<b>Calidad de Imagen</b>	Resolución mínima y características de calidad	Resolución mínima: 480×640 píxeles; Profundidad de color: 24 bits; Iluminación uniforme	Todas las capturas cumplen estándares de calidad; rechazo automático de imágenes de baja calidad
<b>Características Faciales</b>	Posición y visibilidad de características faciales clave	Detección automática de ojos, nariz, boca; Rostro frontal con desviación < 15°; Distancia interpupilar especificada	Sistema de validación en tiempo real durante captura
<b>Condiciones de Captura</b>	Especificaciones de iluminación y fondo	Guía visual para el usuario; Detección de iluminación insuficiente; Recomendación de fondo neutro	Avisos automáticos si las condiciones no son óptimas
<b>Metadata</b>	Información asociada a cada imagen biométrica	Timestamp de captura; Tipo de sensor/cámara; Condiciones de captura; Versión del algoritmo	Metadata completa en formato XML embebido
<b>Expresión Facial</b>	Rostro con expresión neutra	Instrucciones claras al usuario; Validación de expresión mediante ML	Detección automática de sonrisas o expresiones exageradas
<b>Accesorios</b>	Restricciones sobre gafas, sombreros, etc.	Detección de obstáculos faciales; Advertencias al usuario	Alerta si se detectan gafas oscuras, gorras, cubrebocas que obstruyan
<b>Formato de Datos</b>	Estructura de datos para intercambio	Templates biométricos en formato estándar ISO; Compresión sin pérdida de características críticas	Compatibilidad con sistemas biométricos estándar
<b>Privacidad</b>	Protección de datos biométricos	Almacenamiento de templates (no imágenes originales); Encriptación de datos biométricos	Imposibilidad de reconstruir imagen facial original desde template

### 3. ISO/IEC 29100 - Marco de Privacidad

Esta norma proporciona un marco de privacidad aplicable al procesamiento de información personal identificable (PII), incluyendo datos biométricos.

#### Principios de Privacidad Aplicados:

Principio	Descripción	Implementación en el Proyecto	Medidas de Control
<b>1. Consentimiento y Elección</b>	Los individuos deben dar consentimiento informado	·Proceso de registro inicial con consentimiento explícito·Explicación clara del uso de datos biométricos·Opción de revocar consentimiento	·Formulario de consentimiento digital con firma electrónica·Documento de política de privacidad accesible·Función para eliminar datos biométricos
<b>2. Limitación de Propósito</b>	Datos recolectados solo para propósitos específicos	·Datos faciales usados ÚNICAMENTE para registro de asistencia·No compartir con terceros·No usar para otros propósitos sin consentimiento adicional	·Políticas de uso de datos documentadas·Restricciones técnicas en el código·Auditorías periódicas de uso de datos
<b>3. Limitación de Recolección</b>	Solo recolectar datos necesarios	·Captura solo de imagen facial (no datos innecesarios)·Información mínima del alumno (ID, nombre, materia)·No almacenar imágenes completas, solo templates biométricos	·Revisión de campos de datos requeridos·Minimización de metadata·Eliminación automática de datos temporales
<b>4. Minimización de Datos</b>	Procesar solo el mínimo necesario	·Conversión inmediata de imagen a template·Eliminación de imagen original después de procesamiento·Retención de registros solo por período académico	·Políticas de retención de datos·Eliminación automática después del período·Revisión trimestral de datos almacenados
<b>5. Limitación de Uso, Retención y Divulgación</b>	Uso limitado al propósito declarado	·Acceso restringido a administradores y docentes autorizados·No venta o intercambio de datos·Eliminación al término del ciclo escolar o graduación	·Sistema de control de acceso basado en roles·Logs de acceso a datos·Proceso de eliminación certificada
<b>6. Exactitud y Calidad</b>	Datos deben ser precisos y actualizados	·Proceso de actualización de datos faciales semestral·Validación de calidad en cada captura·Corrección de errores reportados en < 24 horas	·Sistema de verificación de calidad·Proceso de actualización guiado·Mecanismo de reporte de errores

<b>7. Apertura, Transparencia y Notificación</b>	Transparencia sobre prácticas de manejo de datos	·Política de privacidad clara y accesible·Notificaciones sobre cambios en políticas·Información sobre quién tiene acceso a datos	·Aviso de privacidad en lenguaje sencillo·Notificaciones push sobre actualizaciones·Página de información sobre privacidad en la app
<b>8. Participación Individual y Acceso</b>	Derecho a acceder y gestionar datos personales	·Portal para consultar datos almacenados·Función para descargar historial de asistencias·Solicitud de corrección o eliminación de datos	·Dashboard de usuario con datos personales·Exportación en formato estándar (PDF, CSV)·Sistema de tickets para solicitudes
<b>9. Responsabilidad</b>	Responsabilidad por cumplimiento de principios	·Designación de oficial de protección de datos·Evaluaciones de impacto de privacidad·Capacitación de personal en protección de datos	·Responsable designado y contactable·DPIA (Data Protection Impact Assessment) documentada·Programa de capacitación anual
<b>10. Seguridad de la Información</b>	Protección apropiada de datos personales	·Encriptación AES-256 de datos biométricos·Comunicación mediante HTTPS/TLS·Autenticación de dos factores para administradores·Backups encriptados	·Auditorías de seguridad trimestrales·Pruebas de penetración anuales·Plan de respuesta a incidentes·Monitoreo de seguridad 24/7
<b>11. Cumplimiento de Privacidad</b>	Mecanismos para verificar cumplimiento	·Auditorías internas semestrales·Revisión legal de cumplimiento normativo·Proceso de quejas y resolución	·Checklist de cumplimiento documentado·Reportes de auditoría·Canal de denuncias anónimo

## Plan de Implementación de Estándares

### Fase 1: Diseño y Planificación

- Análisis de requisitos basado en normas ISO/IEC 25010
- Diseño de arquitectura cumpliendo principios de ISO/IEC 29100
- Selección de tecnologías compatibles con ISO/IEC 19794-5
- Evaluación de impacto de privacidad (DPIA)

## Fase 2: Desarrollo

- Implementación de módulo de captura facial según ISO/IEC 19794-5
- Desarrollo de algoritmo de reconocimiento con validación de calidad
- Implementación de medidas de seguridad y privacidad
- Desarrollo de funcionalidades de gestión de consentimiento
- Integración con sistemas académicos existentes

## Fase 3: Pruebas de Calidad

- Pruebas funcionales (corrección, completitud)
- Pruebas de rendimiento (tiempo de respuesta, capacidad)
- Pruebas de usabilidad con usuarios reales
- Pruebas de seguridad y penetración
- Validación de cumplimiento de estándares biométricos
- Auditoría de privacidad

## Fase 4: Despliegue

- Piloto con grupo reducido de usuarios
- Recolección de feedback y ajustes
- Capacitación a docentes y personal administrativo
- Lanzamiento general
- Monitoreo continuo de métricas de calidad

## Fase 5: Mantenimiento y Mejora Continua

- Revisiones periódicas de cumplimiento normativo
- Actualizaciones de seguridad
- Optimización de algoritmos de reconocimiento
- Mejoras basadas en retroalimentación de usuarios
- Auditorías anuales de calidad y privacidad

## Métricas de Seguimiento

Categoría	Métrica	Objetivo	Frecuencia de Medición
-----------	---------	----------	------------------------

Funcionalidad	Tasa de éxito en reconocimiento facial	> 99%	Diaria
Funcionalidad	Tasa de falsos positivos	< 0.1%	Diaria
Rendimiento	Tiempo de reconocimiento	< 3 segundos	Continua
Rendimiento	Tiempo total de registro de asistencia	< 5 segundos	Continua
Fiabilidad	Disponibilidad del sistema	99.5%	Diaria
Fiabilidad	Tiempo medio entre fallos (MTBF)	> 720 horas	Mensual
Usabilidad	Satisfacción de usuario (encuesta)	> 4.0/5.0	Trimestral
Usabilidad	Tasa de completitud sin ayuda	> 90%	Mensual
Seguridad	Incidentes de seguridad	0	Continua
Seguridad	Tiempo de respuesta a vulnerabilidades	< 48 horas	Por incidente
Privacidad	Solicitudes de acceso a datos	100% resueltas en < 5 días	Mensual
Privacidad	Cumplimiento de políticas de retención	100%	Trimestral
Calidad Biométrica	Porcentaje de imágenes con calidad adecuada	> 95%	Semanal

## Documentación Requerida

- **Manual de Usuario:** Guía para alumnos sobre uso de la aplicación
- **Manual de Administrador:** Guía para gestión del sistema
- **Política de Privacidad:** Documento legal sobre manejo de datos personales
- **Aviso de Privacidad:** Resumen accesible para usuarios
- **Documento de Consentimiento:** Formulario de autorización de uso de datos biométricos
- **Especificaciones Técnicas:** Detalles de implementación y arquitectura
- **Plan de Seguridad:** Medidas de protección implementadas
- **Plan de Respuesta a Incidentes:** Procedimientos ante brechas de seguridad
- **Matriz de Cumplimiento:** Mapeo de requisitos normativos vs implementación
- **Reportes de Auditoría:** Resultados de auditorías de calidad y privacidad



## Responsabilidades del Equipo

Rol	Responsabilidades en Estándares de Calidad
Líder de Proyecto	·Supervisión general del cumplimiento de estándares·Coordinación entre equipos·Reportes de avance
Arquitecto de Software	·Diseño conforme a ISO/IEC 25010·Decisiones técnicas alineadas con estándares·Revisión de arquitectura
Desarrolladores	·Implementación según especificaciones·Código limpio y documentado·Pruebas unitarias
Especialista en Biometría	·Implementación conforme a ISO/IEC 19794-5·Optimización de algoritmos de reconocimiento·Validación de calidad biométrica
Oficial de Protección de Datos	·Cumplimiento de ISO/IEC 29100·Gestión de consentimientos·Auditorías de privacidad·Atención de solicitudes de usuarios
Ingeniero de Seguridad	·Implementación de controles de seguridad·Gestión de vulnerabilidades·Monitoreo y respuesta a incidentes·Pruebas de penetración y hardening