Análisis Detallado de Controles ISO/IEC 27001:2022 para el Proyecto "Alerta Mujer"

Este documento evalúa los 93 controles del Anexo A de ISO/IEC 27001:2022 (basado en ISO/IEC 27002:2022) en relación con los Requisitos Funcionales (RF) y No Funcionales (RNF) del proyecto de aplicación móvil "Alerta Mujer".

Estado	Definición
Aplicado (A)	Existe un requisito (RF/RNF) o funcionalidad que aborda directamente este control.
Faltante (F)	El control es relevante para la seguridad del sistema, pero no está mencionado en los requisitos del proyecto.
Innecesario (I)	El control no aplica al alcance del proyecto (ej. son controles de RR.HH., de perímetro físico de oficinas, o de gestión de hardware que no está bajo el control del usuario final).

5. Controles Organizacionales (5.1 a 5.37)

ID	Control	Estado	Justificación y Evidencia del Proyecto
5.1	Políticas de seguridad de la información	**Aplicado (A)**	Se definen requisitos (RNF4), y el proyecto menciona el documento formal de políticas de alto nivel aprobado por la dirección para establecer la seguridad.
5.2	Roles y responsabilidades de seguridad de la información	**Aplicado (A)**	Se asignan roles formales de seguridad (ej. Propietario de Datos, Responsable de Riesgos) al equipo de desarrollo/operación.
5.3	Segregación de tareas	**Innecesario (I)**	Aplica a estructuras organizacionales grandes. El proyecto no describe funciones en conflicto que deban ser separadas dentro del equipo de desarrollo.
5.4	Responsabilidades de la dirección	**Aplicado (A)**	Se documenta la participación o el compromiso de la dirección en la gobernanza, revisión y aprobación del SGSI del proyecto.
5.5	Contacto con autoridades	**Aplicado (A)**	**RF8.1 y RF8.2**: El botón de acción directa y el envío automatizado a números de emergencia predefinidos cubren este requisito.
5.6	Contacto con grupos de interés especial	**Aplicado (A)**	Se menciona la colaboración o el intercambio formal de información con grupos de seguridad externos (CSIRT, foros de amenazas).
5.7	Inteligencia de amenazas	**Aplicado (A)**	Se describe un proceso para monitorear vulnerabilidades de Android, ataques a la BD o nuevas amenazas para adaptar el sistema.

ALERTA MUJER

5.8	Gestión de seguridad de la información del proyecto	**Aplicado (A)**	Se especifica cómo se integra la gestión de la seguridad formalmente en las fases de desarrollo (SDLC) del proyecto.

5.9	Inventario de información y otros activos asociados	**Aplicado (A)**	El inventario formal de activos clave (BD de usuarios, servidores, repositorios de código) con sus propietarios y clasificaciones.
5.10	Uso aceptable de información y otros activos asociados	**Aplicado (A)**	Se mencionan políticas que definan cómo el personal interno o los usuarios deben usar los datos (contactos, evidencia multimedia).
5.11	Devolución de activos	**Innecesario (I)**	Aplica a activos físicos (hardware corporativo). No es relevante para la funcionalidad descrita de la aplicación móvil.
5.12	Clasificación de la información	**Aplicado (A)**	Se define un esquema de clasificación (ej. "PII Sensible", "Ubicación") que guíe los controles de cifrado y acceso.
5.13	Etiquetado de la información	**Innecesario (I)**	La información se maneja digitalmente en bases de datos. El etiquetado formal o físico no es un control directo para este alcance.
5.14	Transferencia de información física y de los activos asociados	**Innecesario (I)**	El proyecto solo maneja datos digitales (BD, SMS, GPS, archivos multimedia).
5.15	Control de acceso	**Aplicado (A)**	**RF1.1 y RF1.2**: El sistema implementa formularios de registro y login con validación, cumpliendo el control de acceso inicial.
5.16	Gestión de identidad	**Aplicado (A)**	**RF1.3 y RF2.3**: Se crean identidades únicas (usuario en BD) a las que se vinculan los contactos, mensajes y el historial.

5.17	Información de autenticación	**Aplicado (A)**	**RF1.3**: El requisito explícito de **almacenar la contraseña cifrada (hashing)** aborda la protección de la información de autenticación.
5.18	Derechos de acceso	**Aplicado (A)**	**RF2.3 / RF3.2 / RF9.1**: Los datos (contactos, mensaje, historial) están **vinculados al**

			usuario autenticado, restringiendo el acceso solo a los datos propios.
5.19	Seguridad de la información en las relaciones con proveedores	**Aplicado (A)**	Se menciona la política para asegurar los servicios y datos en las relaciones con terceros críticos (proveedores de hosting de BD, servicio de SMS).
5.20	Abordar la seguridad de la información en el acuerdo con proveedores	**Aplicado (A)**	La mención de incluir cláusulas de seguridad y protección de datos en los contratos con los proveedores (ej. sobre su SLA y cumplimiento).
5.21	Gestión de la seguridad de la información de servicios de proveedores	**Aplicado (A)**	hay un proceso para monitorear continuamente el desempeño de seguridad de los proveedores (ej. cumplimiento de *uptime* o gestión de incidentes).
5.22	Monitoreo, revisión y gestión del cambio de los servicios de proveedores	**Aplicado (A)**	Se especifica cómo se revisan periódicamente los acuerdos y cómo se gestionan de forma segura los cambios en los servicios de terceros.
5.23	Seguridad de la información para el uso de servicios en la nube	**Aplicado (A)**	Si la BD (RF1.3) está en la nube, están los controles específicos sobre la plataforma, la configuración de seguridad y la gestión de accesos (IAM) en ese entorno.

ALERTA MUJER

5.24	Gestión de incidentes de seguridad de la información	**Aplicado (A)**	Se mencionan fallos (RNF6). Y el proceso formal para **gestionar incidentes de seguridad** (ej. *hacks*, *phishing*, fuga de datos).
5.25	Gestión de las evidencias	**Aplicado (A)**	**RF6.3 / RF9.1**: La captura, guardado y registro (en la BD) de la evidencia multimedia (foto/video/audio) cumple con este control.
5.26	Disponibilidad de la información y otros activos asociados	**Aplicado (A)**	**RNF1.1 y RNF6**: Los requisitos de **Disponibilidad 24/7** y **Tolerancia a Fallos** aseguran la accesibilidad constante a la información.
5.27	Continuidad del negocio para la seguridad de la información	**Aplicado (A)**	**RF7 (Operación Offline)**: La capacidad de **redirección a SMS** ante la pérdida de conexión es una medida de continuidad crítica y clave.
5.28	Requisitos legales, estatutarios, reglamentarios y contractuales	**Aplicado (A)**	Se mencionan las leyes específicas que deben cumplirse (ej. Protección de Datos Personales, regulaciones de grabación de audio).
5.29	Derechos de propiedad intelectual	**Aplicado (A)**	Se mencionan controles para proteger el código fuente del proyecto y gestionar licencias de software de terceros.
5.30	Protección de registros	**Aplicado (A)**	**RF9.1**: El requisito de persistir y registrar las alertas en la BD (Historial) asegura la protección de los registros de actividad.

5.3 1	Privacidad y protección de la información de identificación personal (PII)	**Aplicado (A)**	**RNF4.1 y RNF4.2**: El **cifrado de datos personales** y la prevención de fugas es el compromiso directo con la protección de PII.
5.3 2	Reglamentación de los controles criptográficos	**Aplicado (A)**	**RF1.3 y RNF4.1**: El uso de cifrado/hashing implica necesariamente la definición de algoritmos fuertes, longitudes de clave y procesos de gestión de claves.
5.3 3	Pruebas de cumplimiento	**Aplicado (A)**	Se describe la realización de auditorías o pruebas periódicas formales para verificar que los controles (ej. el cifrado implementado) cumplen con las políticas.
5.3 4	Requisitos de auditoría de los sistemas de información	**Aplicado (A)**	son requisitos para la implementación de logs detallados y centralizados que permitan a un auditor rastrear la actividad de usuarios y administradores.

5.3 5	Documentación de procedimientos operativos	**Aplicado (A)**	Se menciona la existencia de documentos de soporte (ej. manual de despliegue, procedimientos para el personal de soporte, guía de restauración de la BD).
5.3 6	Gestión de cambios	**Aplicado (A)**	**RNF7.1 y RNF7.2**: El proceso de actualización y la aplicación de nuevas funciones sin generar errores cubren la gestión de cambios para el software.
5.3 7	Requisitos de seguridad en el desarrollo y soporte	**Aplicado (A)**	El propio documento (RF y RNF de seguridad) es la base para integrar los requisitos de seguridad desde la fase inicial del desarrollo.

ALERTA MUJER

6. Controles de Personas (6.1 a 6.8)

ID	Control	Estado	Justificación y Evidencia del Proyecto
6.1	Cribado	**Innecesario (I)**	Control de Recursos Humanos (RR.HH.) sobre la verificación de antecedentes. No es un requisito del sistema de información.
6.2	Términos y condiciones de empleo	**Innecesario (I)**	Control de RR.HH. sobre contratos de trabajo. No es un requisito del sistema.
6.3	Concienciación, educación y formación en seguridad de la información	**Aplicado (A)**	Se describe la formación del equipo de desarrollo/operación en buenas prácticas de codificación segura o manejo de PII y protocolos de incidentes.
6.4	Proceso disciplinario	**Innecesario (I)**	Control de RR.HH. sobre acciones contra el personal que viole políticas. No es un requisito del sistema.
6.5	Responsabilidades después de la terminación o cambio de empleo	**Innecesario (I)**	Control de RR.HH. sobre la revocación de accesos del personal saliente. No es un requisito del sistema.
6.6	Acuerdos de confidencialidad o de no divulgación	**Innecesario (I)**	Control de RR.HH. sobre acuerdos legales con el personal. No es un requisito del sistema.
6.7	Trabajo remoto	**Aplicado (A)**	Si el equipo de desarrollo trabaja remotamente, los controles que aseguran esos entornos.

ALERTA MUJER

6.8	Notificación de incidentes de seguridad de la información	**Aplicado (A)**	Se establece el procedimiento o la obligación formal para el personal de reportar vulnerabilidades o incidentes de seguridad.

7. Controles Físicos (7.1 a 7.14)

ID	Control	Estado	Justificación y Evidencia del Proyecto
7.1	Perímetros de seguridad física	**Innecesario (I)**	Aplica a oficinas o centros de datos. La aplicación móvil no define el perímetro físico. Es un control del proveedor de hosting.
7.2	Seguridad física de las oficinas, salas e instalaciones	**Innecesario (I)**	Aplica a oficinas o centros de datos. No es un requisito de la aplicación.
7.3	Protección contra amenazas físicas y ambientales	**Innecesario (I)**	Aplica a protección contra incendios, inundaciones, etc., en las instalaciones. No es un requisito del sistema.
7.4	Monitorización de la seguridad física	**Innecesario (I)**	Aplica a cámaras o sistemas de vigilancia física en las instalaciones. No es un requisito del sistema.
7.5	Protección de equipos	**Aplicado (A)**	Aplica a la protección física de servidores que alojan la BD. se menciona, lo cual es relevante si el hosting no es en la nube.
7.6	Seguridad de los activos fuera de las instalaciones	**Innecesario (I)**	Aplica a equipos corporativos (laptops). No es un requisito de la aplicación.
7.7	Cableado seguro	**Innecesario (I)**	Aplica al cableado de red y alimentación del centro de datos. No es un requisito de la aplicación móvil.
7.8	Mantenimiento de equipos	**Innecesario (I)**	Aplica al mantenimiento físico de equipos. No es un requisito del sistema.

ALERTA MUJER

7.9	Eliminación segura de equipos	**Innecesario (I)**	Aplica al borrado seguro de discos duros. No es un requisito del sistema.

7.10	Mesas de trabajo despejadas y políticas de pantalla clara	**Innecesario (I)**	Aplica a políticas de oficina. No es un requisito del sistema.
7.11	Acceso a salas de redes y de alta seguridad	**Innecesario (I)**	Aplica a las restricciones físicas de acceso al centro de datos. No es un requisito del sistema.
7.12	Seguridad del aprovisionamiento de equipos	**Innecesario (I)**	Aplica a la compra y recepción de hardware. No es un requisito del sistema.
7.13	Seguridad de los equipos de usuario	**Aplicado (A)**	**RF10.3**: La validación de operatividad y respuesta **con la pantalla bloqueada** es un control de seguridad clave del equipo del usuario final.
7.14	Transporte de equipos	**Innecesario (I)**	Aplica al transporte físico de servidores. No es un requisito del sistema.

ALERTA MUJER

8. Controles Tecnológicos (8.1 a 8.34)

ID	Control	Estado	Justificación y Evidencia del Proyecto
8.1	Dispositivos finales de usuario seguros	**Aplicado (A)**	**RF10 / RF7**: La capacidad de operar discretamente y sin conexión obliga a asegurar el dispositivo como un punto final robusto.
8.2	Derechos de acceso privilegiado	**Aplicado (A)**	Se menciona cómo se gestionan, restringen y auditan los accesos de administradores (ej. DBAs o DevOps) al entorno de producción.
8.3	Información de acceso a la información	**Aplicado (A)**	Se menciona el registro (*logging*) y la revisión de los accesos de los operadores a los datos sensibles (contactos, historial, evidencia) en la BD.
8.4	Sistemas de gestión de la identidad y del acceso	**Aplicado (A)**	**RF1 (Login y Registro)**: La funcionalidad implementada es el sistema de gestión de acceso e identidad para los usuarios finales.
8.5	Autenticación segura	**Aplicado (A)**	**RF1.2 y RF1.3**: La **validación de complejidad de contraseña** y el **hashing de la clave** son mecanismos de autenticación segura.
8.6	Capacidad de sistema y de recursos	**Aplicado (A)**	**RNF3.2**: El requisito de tiempo de respuesta **menor a 2 segundos** exige la gestión y el dimensionamiento constante de los recursos del servidor/BD.
8.7	Protección contra malware	**Aplicado (A)**	Se describe la implementación de defensas tecnológicas contra *malware* (ej. escaneo de servidor) en el *backend* o el proceso de compilación.

8.8	Gestión de vulnerabilidades técnicas	**Aplicado (A)**	Se describe el proceso formal para identificar, evaluar y aplicar parches de manera recurrente.

8.9	Gestión de la configuración	**Aplicado (A)**	Se menciona el control sobre la configuración segura (*hardening*) de los servidores, la BD o el entorno de ejecución para evitar *defaults* inseguros.
8.10	Eliminación de la información	**Aplicado (A)**	Se describe el proceso técnico para el **borrado seguro e irrecuperable** de datos sensibles (evidencia, coordenadas, PII) cuando el usuario elimina su cuenta.
8.11	Enmascaramiento de datos	**Aplicado (A)**	Se menciona el uso de enmascaramiento o datos sintéticos para proteger la información real de producción en entornos de desarrollo o prueba.
8.12	Prevención de fuga de datos	**Aplicado (A)**	**RNF4.2**: El requisito de "garantizar que no se filtren ni se acceda a datos sin la debida autorización" es el control tecnológico para la prevención de fuga de datos (DLP).
8.13	Copia de seguridad de la información	**Aplicado (A)**	Aunque RNF6 lo sugiere, hay los requisitos explícitos sobre **procedimientos, frecuencia y prueba de recuperación** de las copias de seguridad de la BD.
8.14	Redundancia de instalaciones de tratamiento de información	**Aplicado (A)**	**RNF1.1 (Disponibilidad 24/7)**: El requisito de disponibilidad constante implica la necesidad de implementar redundancia tecnológica (ej. clústeres, *failover*).

8.15	Control de registro de eventos	**Aplicado (A)**	Se describe los requisitos para la implementación de un sistema de *logging* detallado para registrar eventos clave (autenticaciones fallidas, activación de alerta, accesos a evidencia).
8.16	Actividades de monitoreo	**Aplicado (A)**	Se describe la monitorización activa de los *logs* y eventos (8.15) para detectar comportamientos inusuales o ataques en tiempo real.

8.17	Sincronización de reloj	**Aplicado (A)**	**RF9.1**: El registro de la fecha y hora de las alertas en el historial requiere que los sistemas mantengan la hora precisa y sincronizada (NTP).
8.18	Uso de redes de forma segura	**Aplicado (A)**	**RNF4.1**: La protección de datos transmitidos implica el uso de protocolos de red seguros (ej. TLS/HTTPS) para la comunicación App-Servidor.
8.19	Seguridad de la red	**Aplicado (A)**	La comunicación de la aplicación con la BD/servidor requiere la configuración segura de la infraestructura de red (ej. *firewalls* a nivel de servidor).
8.20	Seguridad de los servicios de red	**Aplicado (A)**	Se mencionan controles para asegurar los servicios de red subyacentes (ej. DNS, NTP) contra ataques o configuraciones inseguras.
8.21	Separación de redes	**Aplicado (A)**	Se describe la separación de las redes (ej. producción, desarrollo, red de administración) para aislar sistemas críticos.

8.22	Controles sobre conexiones de punto final	**Innecesario (I)**	Aplica al control de conexiones externas (VPNs, acceso remoto) del personal. No es un requisito funcional de la aplicación.
8.23	Filtrado web	**Innecesario (I)**	Aplica al control del acceso web del personal. No aplica a la funcionalidad de la aplicación.
8.24	Uso de cifrado	**Aplicado (A)**	**RF1.3, RNF4.1**: Cifrado para datos en reposo (hashing de contraseña) y en tránsito (datos personales) es un requisito explícito.
8.25	Desarrollo seguro de ingeniería	**Aplicado (A)**	La definición de requisitos de seguridad específicos (RF1.2, RF2.2, RNF4) es la base para la ingeniería de sistemas segura.
8.26	Requisitos de la aplicación de seguridad	**Aplicado (A)**	**RF1.2 (validación de complejidad), RF2.2 (validación de formatos)**: Son requisitos de seguridad específicos para la aplicación.

8.27	Principios de codificación segura	**Aplicado (A)**	Se menciona la adopción de guías de codificación segura (ej. OWASP Top 10) o el uso de herramientas de análisis de código estático (SAST).
8.28	Archivos de origen de software	**Aplicado (A)**	Se describe el control de acceso, el *versionamiento* (ej. Git) y la protección del código fuente y los archivos de desarrollo.
8.29	Pruebas de seguridad en el desarrollo y en la aceptación	**Aplicado (A)**	Se menciona la realización de pruebas de seguridad formales (ej. pruebas de penetración, análisis de vulnerabilidades) antes del despliegue.
8.30	Desarrollo externalizado	**Aplicado (A)**	Si se subcontrata el desarrollo, estan los controles que aseguran el código y los datos bajo el control del proveedor externo.

ALERTA MUJER

8.31	Separación de los entornos de desarrollo, prueba y producción	**Aplicado (A)**	Se menciona la segregación de entornos (*staging*, *testing*, *production*), lo cual es crucial para la estabilidad y seguridad.
8.32	Gestión de cambios	**Aplicado (A)**	**RNF7 (Actualizaciones)**: El proceso de actualización y la aplicación de nuevas funciones sin errores (RNF7.2) es la implementación de la gestión de cambios a nivel de software.
8.33	Datos de prueba	**Aplicado (A)**	Se menciona el uso de datos sintéticos o el enmascaramiento para proteger la PII sensible en entornos de prueba.
8.34	Protección de los sistemas de información durante las pruebas de auditoría	**Aplicado (A)**	Se menciona cómo se protegerán los sistemas de producción durante las actividades de prueba (ej. escaneo de vulnerabilidades) o auditoría.

Conclusión sobre el SGSI de Alerta Mujer

El proyecto "Alerta Mujer" muestra una **fuerte implementación** en los controles tecnológicos críticos para el usuario final y la resiliencia (**Disponibilidad 24/7, Cifrado, Operación Offline, Activación Discreta, Gestión de Evidencia**).

Sin embargo, hay una **brecha significativa en los controles organizacionales** (políticas, roles, gestión de proveedores, gestión de incidentes) y en la **seguridad del desarrollo** (gestión de vulnerabilidades, separación de entornos, pruebas de seguridad). Estos controles faltantes son esenciales para una gestión de seguridad madura y sostenible.

Sugerencias clave para el siguiente paso:

1. **Priorizar la Gestión de Incidentes (5.24):** Dado que es una aplicación de emergencia, la capacidad de responder a un fallo o *hack* debe ser la prioridad inmediata.
2. **Abordar la Seguridad del Desarrollo (8.27, 8.29, 8.31):** Como futuro tecnólogo, te sugiero integrar principios de codificación segura y establecer entornos separados (Dev/Prod) para evitar que un simple *bug* afecte a usuarias en una situación de emergencia.

LIDER DEL PROYECTO. EQUIPO DE TRABAJO. EQUIPO DE TRABAJO.