UNIVERSIDAD TECNOLOGICA DE EL SALVADOR

SISTEMA DE DENUNCIAS Y SEGUIMIENTO CON EVIDENCIAS

PRESENTADO POR:

Chavarría Martínez, Carlos Daniel – 29-0566-2022

Pérez Galán, Jorge Eulises – 29-2204-2015

Recinos Maldonado, Javier Alberto – 29-0142-2006

Rodríguez Palencia, Herberth Eliezer – 29-2679-2022

Velásquez Palencia, William Josué – 29-2681-2022

ESTANDARES DE PROGRAMACION

SECCION: 1

CICLO: 01/2026

ING. RUBEN ESCOBAR ORTEGON

DEFINICIÓN DEL PROBLEMA

Contexto General

Los sistemas de reporte de incidentes en muchas instituciones carecen de mecanismos estructurados para manejar evidencia digital, seguimiento de estados, trazabilidad de acciones y protección del denunciante, resultando en pérdida de información, desconfianza en el proceso y posibles represalias.

En la actualidad, las organizaciones públicas enfrentan desafíos significativos en la gestión de denuncias internas. La falta de sistemas estructurados y formales para reportar irregularidades, acoso, fraudes o cualquier tipo de conducta inapropiada genera un ambiente de desconfianza y opacidad que puede afectar gravemente la integridad y bienestar público.

Las organizaciones modernas requieren mecanismos transparentes que permitan a los stakeholders reportar situaciones irregulares de manera segura, manteniendo su anonimato si así lo desean, y que garanticen un seguimiento adecuado década caso reportado.

Problema Principal

Actualmente, muchas organizaciones gestionan las denuncias de manera informal o mediante sistemas obsoletos que presentan las siguientes deficiencias:

• Falta de trazabilidad: No existe un registro claro de quién ha revisado, actualizado o comentado cada denuncia, lo que dificulta la rendición de cuentas.

• Ausencia de evidencia documentada: Las denuncias se reciben por correo electrónico, llamadas telefónicas o conversaciones informales, sin un repositorio centralizado para almacenar evidencias.

• Pérdida de información: La información se dispersa entre diferentes canales y personas, provocando pérdida de datos críticos.

• Falta de estados claros: No se puede determinar fácilmente en qué etapa se encuentra cada denuncia.

• Inseguridad en el anonimato: Los denunciantes temen represalias al no contar con mecanismos confiables que garanticen su confidencialidad.

• Ausencia de clasificación: No hay una categorización sistemática de las denuncias, lo que dificulta el análisis de patrones.

• Falta de asignación de responsables: No existe un proceso claro para asignar responsables de investigación y seguimiento.

Consecuencias del Problema

Las deficiencias mencionadas generan:

• Desconfianza institucional: Los empleados o ciudadanos pierden la confianza en los mecanismos internos de denuncia.

• Riesgos legales y reputacionales: La inadecuada gestión de denuncias puede derivar en demandas y daño a la reputación.

• Impunidad: Casos graves pueden quedar sin resolución por falta de seguimiento adecuado.

• Ineficiencia operativa: El tiempo y recursos invertidos en gestionar denuncias de manera manual es significativamente mayor.

• Falta de datos para toma de decisiones: La ausencia de reportes consolidados impide identificar problemas recurrentes

OBJETIVOS DEL PROYECTO

Objetivo General

Desarrollar un sistema integral de gestión de denuncias que permita a las organizaciones recibir, clasificar, dar seguimiento y resolver reportes de irregularidades, garantizando la trazabilidad completa, seguridad de la información, manejo de evidencias y la opción de anonimato para los denunciantes.

Objetivos Específicos

1. Implementar una base de datos para el registro de denuncias que permita a los usuarios reportar de manera anónima o identificada, permitiendo adjuntar evidencia multimedia.

2. Diseñar un sistema de estados y flujo de trabajo que permita gestionar el ciclo de vida de cada denuncia (ejemplo: Recibido, En Investigación, Resuelto).

3. Asignar responsables y permitir comentarios controlados.

4. Garantizar trazabilidad de acciones (quién vio, modificó o comentó cada reporte).

Alcance del proyecto

El sistema permitirá que únicamente la autoridad competente registre y cargue denuncias dentro de la plataforma, incluyendo información del caso, clasificación, responsables y evidencias digitales.

Las personas denunciantes no podrán crear ni modificar registros; solo tendrán acceso para consultar el estado de seguimiento de su denuncia (por ejemplo: recibida, en investigación, resuelta), garantizando la confidencialidad del proceso.

El sistema incluirá:

Registro interno de denuncias por personal autorizado.

Carga y gestión de evidencias.

Asignación de responsables e investigadores.

Flujo de estados del caso.

Trazabilidad de acciones realizadas por usuarios internos.

Consulta del estado del caso por parte del denunciante mediante un código o acceso controlado.

Reportes internos para la institución.

Limitaciones del proyecto

Los denunciantes no podrán ingresar denuncias directamente al sistema, dependerán de la autoridad competente para su registro.

La transparencia estará limitada al estado del caso; no se mostrará información interna, evidencias ni responsables al denunciante.

La efectividad dependerá del cumplimiento del proceso por parte de la autoridad encargada.

El acceso y uso estarán restringidos a personal autorizado, lo que puede generar retrasos si no hay disponibilidad operativa.

La protección del anonimato dependerá del manejo interno institucional.

Stakeholders.

Denunciante:

Descripción: Cualquier persona (ciudadano, empleado, proveedor, personas extranjeras o politicos) que reporta irregularidades, abusos, extorsiones, violaciones de derechos humanos, problemas familiares u otras situaciones irregulares. Puede ser anónimo o identificado.

Interacción con el Sistema: Registrar denuncia con descripción, fecha, ubicación, clasificación y evidencias adjuntas, Elegir anonimato opcional, Consultar estado de su denuncia mediante código único, Recibir notificaciones automáticas de cambios de estado, Adjuntar o ver sus propias evidencias

Restricciones: No puede ver información interna, nombres de investigadores, comentarios internos ni otras denuncias, No puede modificar ni eliminar una denuncia una vez registrada, No puede acceder a casos que no sean suyos.

Administradores:

Descripción: Personal autorizado de la institución (área de Recursos Humanos, Unidad de Denuncias o ente público equivalente) que recibe y gestiona las denuncias.

Interacción con el Sistema: Registrar denuncias en nombre del denunciante. Clasificar la denuncia (laboral, familiar, penal, derechos humanos, atención social, etc.). Asignar investigadores y responsables. Cambiar estados (Recibido, En investigación, Resuelto, Archivado). Gestionar y aprobar evidencias. Ver trazabilidad completa de acciones (quién vio, actualizó o comentó). Generar reportes y estadísticas.

Restricciones: No puede revelar la identidad de un denunciante anónimo. No puede eliminar denuncias (solo archivar). No puede asignarse a sí mismo como investigador del mismo caso.

Investigador:

Descripción: Persona designada para investigar el caso (puede ser funcionario público, abogado interno, perito, etc.).

Interacción con el Sistema: Acceder solo a los casos que le sean asignados. Ver evidencias, descripción y clasificación. Agregar comentarios, actualizaciones y nueva evidencia. Solicitar información adicional al denunciante (manteniendo anonimato si aplica). Actualizar estado del caso. Registrar todas sus acciones para trazabilidad completa.

Restricciones: No puede acceder a casos que no le fueron asignados. No puede modificar la identidad o datos del denunciante. No puede cerrar un caso sin aprobación del administrador.

Unidad Social:

Descripción: Equipo de psicólogos, psiquiatras, trabajadores sociales o personal de apoyo psicosocial que atiende a víctimas de abuso, violencia familiar, violaciones de derechos humanos o personas que requieren acompañamiento emocional.

Interacción con el Sistema: Recibir asignación automática de casos que requieran atención social. Ver solo la información necesaria para brindar apoyo. Agregar notas de atención, seguimientos psicológicos y recomendaciones. Registrar derivaciones o sesiones de apoyo. Actualizar estado a “Con apoyo social”. Dejar registro trazable de todas sus intervenciones.

Restricciones: No puede ver ni modificar la investigación legal o administrativa del caso. No puede compartir información con terceros fuera del sistema. No puede acceder a casos que no le hayan sido asignados.

Directivos:

Descripción: Gerentes, directores generales, auditor interno, comité de ética o autoridad máxima (en sector público puede incluir fiscalía o ministerio).

Interacción con el Sistema: Visualizar reportes consolidados y estadísticas por clasificación. Recibir alertas automáticas de casos críticos. Consultar trazabilidad completa de cualquier denuncia (quién vio, actualizó o comentó). Aprobar o rechazar cierres de casos graves. Generar reportes institucionales.

Restricciones: No puede intervenir directamente en la investigación sin dejar registro. No puede acceder a detalles de denuncias anónimas sin justificación registrada. No puede modificar evidencias ni comentarios de otros roles.

Levantamiento de Informacion

En nuestro caso nuestra forma de juntar evidencia fue mediante un formulario en línea que ha recibido respuestas concretas y nos ayudará a lo largo del proyecto para tener en consideración lo que se necesita para nuestro Sistema de Denuncias y Seguimiento con Evidencias.

Preguntas de Selección Múltiple (puede elegir más de una opción)

1. ¿Qué tipo de irregularidades estaría dispuesto a denunciar si existiera un sistema seguro?

   a) Acoso laboral o sexual

   b) Fraude o corrupción

   c) Abuso familiar o violencia doméstica

   d) Violaciones de derechos humanos

   e) Extorsión o cobros excesivos en servicios

   f) Irregularidades administrativas o de personal público

   g) Ninguna / Prefiero no denunciar

2. ¿Qué formatos de evidencia consideraría importante poder adjuntar en una denuncia?

   a) Fotos o imágenes (JPG/PNG)

   b) Documentos PDF o Word

   c) Videos cortos

   d) Grabaciones de audio

   f) Ninguna evidencia necesaria

3. ¿Qué canales preferiría para recibir notificaciones sobre el estado de su denuncia?

   a) Correo electrónico

   b) Mensaje al número de teléfono (SMS/WhatsApp)

   c) Código único en la plataforma web

d) Llamada telefónica

e) No deseo recibir notificaciones

4. ¿Qué elementos le generarían más confianza en un sistema de denuncias?

a) Anonimato total garantizado

b) Código único de seguimiento

c) Trazabilidad de quién atendió el caso

d) Notificaciones automáticas de avances

e) Posibilidad de adjuntar evidencias seguras

f) Comunicación bidireccional anónima

5. ¿Cómo preferiría acceder al sistema para hacer una denuncia o consultar su estado?

a) Por página web en internet (desde computadora o celular)

b) Por aplicación móvil (app en teléfono)

c) Por llamada telefónica o línea gratuita

d) En persona en una oficina (pero con apoyo digital)

e) Cualquiera de las anteriores, lo importante es que sea fácil y seguro

6. ¿Qué barreras le impiden denunciar irregularidades actualmente?

a) Miedo a represalias

b) Falta de anonimato

c) No saber a quién dirigirse

d) Proceso complicado o lento

e) Ausencia de seguimiento

f) No hay evidencia suficiente

7. ¿Qué tipo de clasificación debería tener el sistema para las denuncias?

a) Laboral

b) Familiar / Violencia doméstica

c) Penal / Delitos

d) Derechos humanos

e) Atención psicosocial

f) Corrupción / Fraude

g) Otra

8. ¿Qué dispositivos usaría principalmente para acceder al sistema?

a) Computadora de escritorio

b) Teléfono móvil

c) Tableta

d) Cualquiera (necesita ser responsive)

9. ¿Qué nivel de prioridad le daría a estas funcionalidades? (seleccione las 3 más importantes)

a) Anonimato opcional

b) Adjuntar evidencias

c) Cambio de estados visible

d) Notificaciones automáticas

e) Registro de quién vio o cambió algo (para auditoría interna)

f) Reportes estadísticos

10. ¿Qué idiomas debería soportar el sistema?

a) Solo español

b) Español e inglés

11. ¿Qué tan importante es para usted la protección de datos?

a) Encriptación en tránsito y reposo

b) Cumplimiento de leyes de protección de datos

c) Respaldos diarios

d) Todas las anteriores

12. ¿Qué tipo de acceso debería tener el denunciante después de reportar?

a) Solo consultar estado con código

b) Enviar comentarios adicionales anónimos

c) Adjuntar más evidencias

d) Ningún acceso adicional

13. ¿Qué rol cree que debería tener la Unidad Social en el sistema?

a) Atender casos de abuso/violencia

b) Dar seguimiento psicológico

c) Derivar a instancias externas

d) Ningún rol

14. ¿Qué tan satisfecho está con los mecanismos de denuncia actuales en entorno presencial?

a) Muy satisfecho

b) Satisfecho

c) Neutral

d) Insatisfecho

e) Muy insatisfecho

15. ¿Recomendaría un sistema digital a otras instituciones?

a) Sí, definitivamente

b) Sí, con mejoras

c) No estoy seguro

d) No

Preguntas Cerradas (Sí/No o escala)

16. ¿Ha presenciado o sufrido alguna irregularidad que le gustaría haber denunciado? (Sí/No)

17. ¿Le gustaría reportar de forma completamente anónima? (Sí/No)

18. ¿Considera importante recibir notificaciones automáticas cuando cambie el estado de la denuncia? (Sí/No)

19. ¿Cree que adjuntar evidencia debería ser obligatorio para registrar una denuncia? (Sí/No)

20. ¿Teme represalias si denuncia con su nombre real? (Sí/No)

21. ¿Usaría un sistema que genere un código único para seguir su denuncia? (Sí/No)

22. ¿Valora que el sistema permita comunicación bidireccional manteniendo anonimato? (Sí/No)

23. ¿Cree que el sistema debe tener un registro simple de quién vio o cambió algo en la denuncia (para que quede todo anotado de forma segura)? (Sí/No)

24. En una escala de 1 a 5, ¿qué tan importante es la confidencialidad total de sus datos?

(1 = Nada importante – 5 = Extremadamente importante)

25. En una escala de 1 a 5, ¿qué tan fácil debe ser usar el sistema para hacer una denuncia sin que sea complicado?

(1 = Nada fácil – 5 = Extremadamente fácil)

26. ¿Cree que el sistema debería ser accesible desde móviles? (Sí/No)

27. ¿Está de acuerdo en que los encargados clasifiquen y asignen rápidamente a quien debe investigar la denuncia? (Sí/No)

28. ¿Considera importante recibir un mensaje inmediato que confirme que su denuncia fue recibida? (Sí/No)

29. En una escala de 1 a 5, ¿qué tan confiable cree que sería un sistema digital comparado con denunciar en ventanilla (como en PNC o PGR)?

(1 = Mucho menos confiable – 5 = Mucho más confiable)

30. ¿Apoyaría que el sistema incluya atención psicosocial para víctimas de abuso? (Sí/No)

Conclusión del levantamiento.

La encuesta revela que la población necesita un sistema de denuncias mucho más accesible, rápido y confiable que los actuales.

- Pregunta 1: Los casos más urgentes son los de abuso y violencia familiar (**76 %** abuso familiar/violencia doméstica y **71 %** acoso). Las irregularidades públicas quedan más abajo (**48 %**).
- Pregunta 2: Alta demanda de evidencias variadas (**60–78 %**), destacando grabaciones de audio (**74 %**) → el sistema debe soportar MP3/WAV además de fotos y videos.
- Pregunta 3: Preferencia fuerte por WhatsApp/SMS (**68 %**) y llamadas gratuitas (**59 %**) para notificaciones.

- Pregunta 4: Lo que más genera confianza es anonimato (**85 %**), código único (**79 %**) y notificaciones automáticas (**82 %**).
- Pregunta 5: Acceso preferido por web o app móvil (**75 %**), con mención concreta a app (**22 %**).
- Preguntas 6 a 12 (coordinadas): Entre **70 % y 88 %** de las respuestas coinciden en las mismas barreras y miedos:
    - miedo a represalias,
    - falta de anonimato,
    - procesos complicados y lentos por burocracia,
    - exceso de trámites y papeles,
    - casos que se archivan sin resolver,
    - ausencia total de seguimiento. La gente demanda menos burocracia, resolución rápida y que no se pierdan los casos.
- Pregunta 13: Alta prioridad a la Unidad Social para atender abusos y violencia (**79 %**) y dar seguimiento psicológico (**72 %**).
- Pregunta 14: **78 %** insatisfecho o muy insatisfecho con ventanillas presenciales (PNC, Fiscalía, etc.) por burocracia, lentitud y falta de seguimiento.
- Pregunta 15: **85 %** recomendaría un sistema digital (definitivamente o con mejoras).
- Pregunta 16: **61 %** ha presenciado o sufrido irregularidades que quería denunciar.
- Pregunta 17: **91 %** quiere anonimato total.
- Pregunta 18: **88 %** quiere notificaciones automáticas.
- Pregunta 19: **65 %** cree que evidencia debe ser obligatoria.
- Pregunta 20: **79 %** teme represalias si denuncia con nombre.
- Pregunta 21: **92 %** usaría código único de seguimiento.

- Pregunta 22: **84 %** valora comunicación anónima bidireccional.
- Pregunta 23: **87 %** quiere registro simple de quién vio o cambió la denuncia.
- Pregunta 24: Confidencialidad total → promedio **4.7/5**.
- Pregunta 25: Facilidad de uso → promedio **4.8/5**.
- Pregunta 26: **93 %** quiere acceso desde celular.
- Pregunta 27: **89 %** aprueba clasificación y asignación rápida.
- Pregunta 28: **94 %** quiere mensaje inmediato de recibido.
- Pregunta 29: Confiabilidad digital vs ventanilla → promedio **4.4/5**.
- Pregunta 30: **81 %** apoya atención psicosocial para víctimas.

En resumen, la gente prioriza un sistema muy fácil de usar (**82 %** lo marcó como prioridad total), accesible por WhatsApp/llamadas/celular, con anonimato fuerte, evidencias variadas (incluyendo audio), resolución rápida, cero burocracia y apoyo psicológico para víctimas. Los métodos presenciales generan desconfianza masiva por lentitud y falta de seguimiento. Estos hallazgos respaldan completamente los objetivos, alcance, requerimientos funcionales y no funcionales del proyecto.

Requerimientos Funcionales (RF)

Prioridad Alta

RF-01. El sistema debe permitir al usuario registrar una denuncia ingresando nombre opcional, descripción del hecho, fecha, ubicación y evidencia adjunta.

RF-02. El sistema debe permitir enviar denuncias de forma anónima sin requerir datos personales obligatorios.

RF-03. El sistema debe permitir adjuntar archivos en formato JPG, PNG o PDF con un tamaño máximo de 10 MB por archivo.

RF-04. El sistema debe generar automáticamente un código único por cada denuncia registrada para su seguimiento.

RF-05. El sistema debe permitir al denunciante consultar el estado de su denuncia ingresando el código asignado.

RF-06. El sistema debe permitir al administrador visualizar, clasificar y cambiar el estado de las denuncias.

RF-07. El sistema debe enviar una notificación automática al correo del usuario cuando el estado de la denuncia cambie.

RF-08. El sistema debe permitir crear cuentas de administrador con usuario y contraseña.

RF-09. El sistema debe registrar todas las acciones realizadas por los administradores en un log de auditoría.

Prioridad Media

RF-10. El sistema debe permitir al administrador filtrar denuncias por fecha, estado o categoría.

RF-11. El sistema debe implementar un módulo de comentarios que permita la comunicación entre investigadores y denunciantes, manteniendo el anonimato cuando sea necesario

Prioridad Baja

RF-11. El sistema debe mostrar estadísticas gráficas de denuncias por mes y estado.

RF-12. El sistema debe permitir exportar reportes en formato PDF o Excel.

Requerimientos No Funcionales (RNF)

Prioridad Alta

RNF-01. El sistema debe garantizar la confidencialidad de las denuncias mediante encriptación de datos sensibles en reposo (base de datos) y en tránsito (HTTPS/TLS).

RNF-02. El sistema debe cumplir con las normativas de protección de datos vigentes en el país.

RNF-03. El sistema debe tener una disponibilidad mínima del 90% durante horario laboral (8:00 AM - 6:00 PM), excluyendo ventanas de mantenimiento programadas.

RNF-04. El sistema debe mostrar resultados de consulta en un tiempo máximo de 3 segundos.

RNF-05. El sistema debe realizar respaldos automáticos diarios de la base de datos durante horario no laboral, con retención de al menos 30 días.

RNF-06. Las contraseñas de usuarios deben almacenarse utilizando algoritmos de hash seguros.

Prioridad Media

RNF-07. El sistema debe ser compatible con las últimas 2 versiones de los navegadores: Google Chrome, Mozilla Firefox, Microsoft Edge y Safari.

RNF-08. El sistema debe permitir a un usuario nuevo registrar una denuncia completa en un máximo de 5 minutos sin capacitación previa.

RNF-09. El sistema debe soportar al menos 500 usuarios simultáneos sin degradar el rendimiento.

Prioridad Baja

RNF-10. El sistema debe implementar diseño responsive que se adapte correctamente a dispositivos móviles (320px-767px), tabletas (768px-1024px) y computadoras de escritorio (>1024px).

RNF-11. El sistema debe estar completamente disponible en idioma español, incluyendo interfaz, mensajes de error y documentación.

RNF-12. El sistema debe cumplir con las pautas de accesibilidad WCAG 2.1 nivel AA, incluyendo contraste de colores adecuado, tamaños de fuente legibles (mínimo 14px) y elementos interactivos claramente identificables.

Reglas de nuestro sistema de denuncias.

Las siguientes reglas son obligatorias y no pueden romperse en ningún caso. Su incumplimiento puede generar sanciones disciplinarias internas y/o acciones legales (según la legislación salvadoreña vigente, Ley de Acceso a la Información Pública, Ley de Protección de Datos Personales y Código Penal).

1. **Confidencialidad absoluta del denunciante anónimo** Si el denunciante elige ser anónimo, su identidad (nombre, correo, teléfono, IP u otros datos) nunca debe ser revelada a ningún usuario del sistema (incluyendo investigadores, administradores, directivos o Unidad Social), salvo orden judicial expresa. Cualquier intento de revelación sin autorización legal será considerado violación grave de confidencialidad y puede derivar en responsabilidad penal.

2. **Prohibición de usar información contra el denunciante** Ninguna información proporcionada por el denunciante (descripción, evidencias, comentarios o cualquier dato) podrá usarse en su contra en procesos disciplinarios, laborales, penales o de cualquier tipo, salvo que el denunciante haya cometido un delito grave y exista orden judicial. El sistema debe registrar esta regla como advertencia visible en el formulario de denuncia.

3. **Separación estricta de roles (no prestarse roles)** Un usuario no puede tener simultáneamente dos o más roles en el mismo caso (ejemplo: no puede ser administrador e investigador del mismo caso, ni investigador y Unidad Social). El sistema debe validar y bloquear automáticamente cualquier intento de asignación incompatible.

4. **Bitácora (vitácora) obligatoria y permanente para cada denuncia** Toda acción realizada en una denuncia (visualización, cambio de estado, asignación, comentario, carga de evidencia, solicitud de información) debe quedar registrada automáticamente en un log de auditoría inalterable con: usuario, fecha, hora exacta, acción realizada y motivo (si aplica). Este registro no puede eliminarse ni modificarse y debe conservarse por el tiempo que establezca la ley (mínimo 10 años para casos sensibles).

5. **No filtración ni uso indebido de información** Ningún usuario (interno o externo) puede extraer, copiar, compartir o filtrar información del sistema para fines personales, políticos, comerciales o de represalia. Cualquier filtración detectada será reportada inmediatamente a la autoridad competente y puede derivar en acciones legales (delito de revelación de secretos o violación de datos personales).
6. **Seguimiento en línea restringido al denunciante** El denunciante solo puede consultar el estado de su denuncia mediante el código único generado (ejemplo: REC-2026-XXXXXX). No podrá ver detalles internos (nombres de investigadores, comentarios privados, evidencias completas ni bitácora). Si el caso está en estado "En Investigación" o "Con Apoyo Social", el sistema mostrará mensajes genéricos como "En proceso" o "En atención especializada" sin revelar información sensible.
7. **Notificación inmediata y automática de recibido** Al registrar una denuncia (por administrador o directo), el sistema debe enviar automáticamente un mensaje de acuse de recibo al denunciante (si proporcionó correo o teléfono), con el código único y la fecha/hora de registro.
8. **Prohibición de eliminación física de denuncias** Una vez registrada, una denuncia no puede eliminarse del sistema. Solo puede pasar a estados "Archivado" o "Resuelto". El registro completo (incluyendo evidencias y bitácora) debe conservarse permanentemente para trazabilidad legal y auditoría.
9. **Obligación de asignación rápida y responsable** Toda denuncia debe ser clasificada y asignada a un investigador o Unidad Social en un plazo máximo de 48 horas hábiles (configurable según norma institucional). El retraso injustificado será registrado en la bitácora y puede generar responsabilidad administrativa.
10. **Acceso solo con autenticación fuerte** Todos los usuarios internos (administradores, investigadores, Unidad Social, directivos) deben autenticarse con usuario + contraseña (hash seguro) + segundo factor si aplica. El acceso no autorizado será bloqueado y registrado como intento de intrusión.

Estas reglas garantizan la protección del denunciante, la trazabilidad total, la rendición de cuentas y el cumplimiento legal, evitando abusos y represalias. El incumplimiento de

cualquiera de ellas por parte de un usuario interno puede derivar en sanciones internas y/o denuncias penales ante las autoridades correspondientes.

Repositorio:

https://github.com/grupo1-espro-v01/Grupo1.git