



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



DESARROLLO DE SOFTWARE SEGURO

GRUPO C

INTEGRANTES:

- **ARIAS EDDY**
- **COLLAGUAZO SHIRLEY**
- **ESPINOZA MATEO**
- **JIMA JUAN**
- **VILLARREAL MATIAS**

DISEÑAR E IMPLEMENTAR UN SISTEMA WEB FUNCIONAL QUE PERMITA A UNA ORGANIZACIÓN REGISTRAR, CLASIFICAR, GESTIONAR Y HACER SEGUIMIENTO A INCIDENTES DE SEGURIDAD INFORMÁTICA, APLICANDO PRINCIPIOS DE DESARROLLO DE SOFTWARE SEGURO EN TODAS LAS FASES DEL CICLO DE VIDA.

PERIODO: 2025A PROYECTO SEGUNDO BIMESTRE

DESARROLLO DE SOFTWARE SEGURO



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Tabla de contenidos

Tabla de contenidos.....	2
Índice - Tablas	3
Tabla de figuras:.....	4
Desarrollo Primer Bimestre	6
Introducción.....	7
Marco Teórico	8
1. Security Development Lifecycle (SDL):	8
2. Gestión de Incidentes de Seguridad Informática:	9
3. Requerimientos de Seguridad en SDL:	9
4. Modelado de Amenazas y Análisis de Riesgos:	9
5. Control de Acceso:	9
6. Matriz de Trazabilidad de Requerimientos (RTM):.....	9
7. Prácticas Adicionales de Seguridad en SDL:	10
Desarrollo	10
Metodología: SDL.....	10
1. Entrenamiento	11
2. Requerimientos.....	11
3. Diseño	24
Árbol de ataques.....	24
1. Análisis y explicación del árbol de ataque - Completo del sistema.	25
2. Análisis y explicación del árbol de ataque – Denegación del servicio.	26
3. Análisis y explicación del árbol de ataque – Divulgación de información.....	27
Desarrollo Segundo Bimestre	28
Notas a contemplar para el Desarrollo de la aplicación.....	29
Elaboración	31
Requerimientos – Segundo Bimestre.....	31
Requerimientos de Seguridad – Tabla actualizada	31
Casos de Mal Uso – Identificados	34
Sistema de Control de Acceso – Actualizada.....	36
Almacenes de datos	37
Funcionalidad del Auditor	37
Funcionalidad del Sistema	40



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Usuario.....	40
Analista de Seguridad	44
Jefe de SOC	47
Auditor.....	51
Gerente de Riesgos	55
Conclusiones y Recomendaciones	63
Conclusiones	63
Recomendaciones	63
Referencias	64
Anexos	65
• Anexo A.....	65
• Anexo B.....	65
• Anexo C.....	65
• Anexo D.....	65
• Anexo E	65

Índice - Tablas

Tabla 1 US-01 Registrar Incidente	12
Tabla 2 US-02 Clasificar incidente	13
Tabla 3 US-03 Flujo de estado del incidente	14
Tabla 4 US-04 Alertas por correo	14
Tabla 5 US-05 Reportes Mensuales	15
Tabla 6 US-06 Exportar incidentes CSV/PDF	16
Tabla 7 NF-01 Disponibilidad 24 x 7	16
Tabla 8 NF-02 Tiempo de respuesta CRUD	17
Tabla 9 NF-03 Usabilidad responsiva	17
Tabla 10 NF-04 Cumplimiento – Logs 5 años	17
Tabla 11 RS-01 Confidencialidad (TLS 1.3 + AES-256)	18
Tabla 12 RS-02 Integridad de adjuntos	18
Tabla 13 RS-03 Disponibilidad frente a DoS	18
Tabla 14 RS-04 Trazabilidad inmutable.....	19
Tabla 15 RS-05 Privacidad – Anonimización.....	19
Tabla 16 CU-01.....	20
Tabla 17 CU-02.....	20
Tabla 18 CU-03.....	21
Tabla 19 CU-04.....	21
Tabla 20 MU-01	22
Tabla 21 MU-02	22



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Tabla 22 MU-03	22
Tabla 23 MU-04	23
Tabla 24 MU-05	23
Tabla 25 Requerimientos de Seguridad - Actualizados	32
Tabla 26 MU-06	34
Tabla 27 MU-07	34
Tabla 28 MU-08	35
Tabla 29 MU-09	35

Tabla de figuras:

Ilustración 1 Fases de la metodología SDL	10
Ilustración 2 Actividades del SDL para la Seguridad	10
Ilustración 3 Árbol de ataques	25
Ilustración 4 Subárbol denegación de servicio	26
Ilustración 5 Subárbol divulgación de información	27
Ilustración 6 Historial de Eventos (Logs) del Auditor	38
Ilustración 7 Detalle de un Log con Opciones de Exportación	39
Ilustración 8 Pantalla de Inicio de Sesión del Usuario	40
Ilustración 9 Registro de Usuario y Selección de Rol	41
Ilustración 10 Dashboard Principal del Usuario	41
Ilustración 11 Formulario de Creación de Incidente	42
Ilustración 12 Gestión de Incidentes del Usuario	43
Ilustración 13 Dashboard Actualizado tras Registro de Incidente	43
Ilustración 14 Creación de Cuenta para Analista de Seguridad	44
Ilustración 15 Dashboard del Analista de Seguridad	45
Ilustración 16 Gestión de Incidentes por el Analista	45
Ilustración 17 Reportes Mensuales de Incidentes	46
Ilustración 18 Detalles de un Incidente	47
Ilustración 19 Creación de Cuenta para Jefe de SOC	48
Ilustración 20 Dashboard del Jefe de SOC	48
Ilustración 21 Gestión de Incidentes por el Jefe de SOC	49
Ilustración 22 Reportes Mensuales Generados por el Jefe de SOC	50
Ilustración 23 Gestión de Usuarios desde el Perfil Jefe de SOC	50
Ilustración 24 Creación de cuenta del Auditor	51
Ilustración 25 Dashboard del Auditor	52
Ilustración 26 Gestión de Incidentes por parte del Auditor	52
Ilustración 27 Subida y revisión de evidencia	53
Ilustración 28 Detalle de un incidente	54
Ilustración 29 Reportes mensuales del Auditor	54
Ilustración 30 Logs de Auditoría	55
Ilustración 31 Creación de cuenta como Gerente de Riesgos	56
Ilustración 32 Dashboard del Gerente de Riesgos	56



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Ilustración 33 Gestión de Incidentes.....	57
Ilustración 34 Exportación de Reportes	58
Ilustración 35 Reportes Mensuales.....	58
Ilustración 36 Gestión de Usuarios	59
Ilustración 37 Configuración inicial del MFA.....	60
Ilustración 38 Escaneo del Código QR.....	61
Ilustración 39 Generación de clave secreta y validación.....	62



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Desarrollo Primer Bimestre



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



Introducción

En el panorama actual de la ciberseguridad, las organizaciones enfrentan una creciente ola de incidentes de seguridad informática, como ataques de ransomware, filtraciones de datos y denegaciones de servicio, que amenazan la integridad, confidencialidad y disponibilidad de sus activos digitales. Estos incidentes no solo generan pérdidas económicas, sino que también afectan la confianza de los usuarios y la reputación de las organizaciones. Para abordar esta problemática, es fundamental contar con sistemas robustos que permitan registrar, clasificar, gestionar y dar seguimiento a los incidentes de manera eficiente, garantizando al mismo tiempo la seguridad del sistema en sí. Este proyecto tiene como objetivo diseñar e implementar un sistema web funcional que facilite a una organización la gestión integral de incidentes de seguridad informática, aplicando los principios de desarrollo de software seguro a través de la metodología Security Development Lifecycle (SDL) en todas las fases del ciclo de vida del software.

El enfoque del primer bimestre se centra en las fases de requerimientos y diseño, siguiendo las prácticas establecidas por SDL para integrar la seguridad desde las etapas iniciales del desarrollo. En la fase de requerimientos, se definirán los requerimientos funcionales (como el registro y clasificación de incidentes), no funcionales (como escalabilidad y rendimiento) y de seguridad (como autenticación y control de acceso), incluyendo un modelo de control de acceso basado en roles (RBAC) y una actividad adicional de seguridad, como la clasificación de datos sensibles. En la fase de diseño, se elaborará un modelado de amenazas utilizando el marco STRIDE, un diagrama de flujo de datos (DFD) para visualizar el flujo de información, un análisis de riesgos para priorizar mitigaciones y una actividad adicional de seguridad, como la revisión de diseño seguro. Además, se generará una Matriz de Trazabilidad de Requerimientos (RTM) para asegurar que todos los requerimientos se aborden y se mantengan trazables a lo largo del proyecto, cumpliendo con los estándares de SDL.

La metodología SDL, desarrollada por Microsoft, proporciona un marco estructurado que garantiza la incorporación de prácticas de seguridad en cada etapa del desarrollo, desde la capacitación del equipo hasta la respuesta a incidentes post-lanzamiento. Este enfoque es especialmente relevante para sistemas que manejan información crítica, como los detalles de incidentes de seguridad, donde cualquier vulnerabilidad podría tener consecuencias graves.

Este informe documenta el proceso inicial de desarrollo, detallando las actividades realizadas, los artefactos generados y las medidas de seguridad aplicadas en las fases de requerimientos y diseño. Los resultados se presentarán en una exposición, con el objetivo de compartir los avances con los compañeros, promover la retroalimentación y fomentar el aprendizaje colaborativo. Este proyecto sienta las bases para un sistema seguro, escalable y alineado con las necesidades de la organización, preparando el terreno para las fases posteriores del desarrollo en el segundo bimestre.



Marco Teórico

El desarrollo de un sistema web para la gestión de incidentes de seguridad informática requiere un enfoque estructurado que integre prácticas de seguridad desde las primeras etapas del ciclo de vida del software. La metodología **Security Development Lifecycle (SDL)**, propuesta por Microsoft, ofrece un marco robusto para garantizar que el software sea seguro, confiable y resiliente frente a amenazas. A continuación, se presentan los conceptos teóricos fundamentales que sustentan el proyecto, incluyendo las etapas de SDL y su relevancia para las fases de requerimientos y diseño.

1. Security Development Lifecycle (SDL):

SDL es una metodología diseñada para incorporar seguridad en todas las fases del ciclo de vida del desarrollo de software (SDLC). Según Microsoft (2020), SDL abarca etapas como capacitación, definición de requerimientos, diseño, implementación, verificación, lanzamiento y respuesta a incidentes. En las fases de requerimientos y diseño, SDL enfatiza la identificación de requerimientos de seguridad, el modelado de amenazas y la aplicación de controles para mitigar riesgos desde el inicio. Los artefactos de SDL incluyen listas de verificación de seguridad, análisis de riesgos y especificaciones de diseño seguro.

Las etapas de SDL son las siguientes:

- **Entrenamiento:** Formación del equipo en prácticas de desarrollo seguro, incluyendo conceptos como OWASP Top 10, principios de seguridad y técnicas de mitigación de amenazas.
- **Definición de Requerimientos:** Identificación de requerimientos funcionales, no funcionales y de seguridad, asegurando que se establezcan controles como autenticación, autorización y protección de datos. Se utilizan listas de verificación basadas en estándares como **NIST SP 800-53**.
- **Diseño:** Creación de especificaciones de diseño seguro, incluyendo modelado de amenazas (**por ejemplo, STRIDE**), diagramas de flujo de datos (**DFD**) y análisis de riesgos para identificar y mitigar vulnerabilidades.
- **Implementación:** Desarrollo del software utilizando herramientas y prácticas seguras, como revisiones de código y el uso de bibliotecas validadas.
- **Verificación:** Pruebas de seguridad, como análisis estático y dinámico, para detectar vulnerabilidades antes del lanzamiento.
- **Lanzamiento:** Revisión final de seguridad y preparación para el despliegue, incluyendo planes de respuesta a incidentes.
- **Respuesta:** Monitoreo **post-lanzamiento** y gestión de incidentes de seguridad, con actualizaciones y parches según sea necesario.

Para este proyecto, las fases de requerimientos y diseño son el foco principal, con entregables como listas de verificación de seguridad, modelos de control de acceso, modelado de amenazas y DFD.



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



2. Gestión de Incidentes de Seguridad Informática:

Según ISO/IEC 27035, la gestión de incidentes de seguridad implica identificar, responder, mitigar y recuperarse de eventos que comprometan la seguridad de una organización. Un sistema de gestión de incidentes debe permitir registrar eventos, clasificarlos por tipo o severidad (**por ejemplo, ataque de malware, fuga de datos**), asignar responsables, realizar seguimiento de acciones correctivas y generar reportes para análisis. La seguridad del sistema es crítica para proteger datos sensibles, como detalles de incidentes o información de usuarios.

3. Requerimientos de Seguridad en SDL:

En la fase de definición de requerimientos de SDL, se identifican los requerimientos funcionales (**por ejemplo, registrar y clasificar incidentes**), no funcionales (**como rendimiento y disponibilidad**) y de seguridad (**como autenticación multifactor o cifrado de datos**). SDL exige el uso de listas de verificación para garantizar que los requerimientos cumplan con estándares de seguridad, como OWASP Top 10 o NIST SP 800-53. Un modelo de control de acceso, como RBAC (Control de Acceso Basado en Roles), es esencial para definir permisos basados en roles de usuario (**por ejemplo, administrador, analista de incidentes**), asegurando el principio de privilegio mínimo.

4. Modelado de Amenazas y Análisis de Riesgos:

En la fase de diseño de SDL, el modelado de amenazas utiliza frameworks como **STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)** para identificar posibles vulnerabilidades en el sistema. El análisis de riesgos evalúa la probabilidad e impacto de estas amenazas, priorizando medidas de mitigación. Los diagramas de flujo de datos (**DFD**) visualizan cómo los datos se mueven a través del sistema, identificando puntos de riesgo, como interfaces externas, almacenamiento de datos o interacciones con usuarios.

5. Control de Acceso:

El control de acceso es un pilar clave de la seguridad informática. Modelos como RBAC o ABAC (**Control de Acceso Basado en Atributos**) permiten definir permisos basados en roles o atributos, garantizando que los usuarios solo accedan a los recursos autorizados. En SDL, el diseño del control de acceso se valida durante la fase de diseño para cumplir con principios como el privilegio mínimo y la separación de funciones.

6. Matriz de Trazabilidad de Requerimientos (RTM):

La RTM es una herramienta que mapea los requerimientos del sistema con sus artefactos, casos de prueba y medidas de mitigación, asegurando que todos los requerimientos se aborden y verifiquen durante el desarrollo. En el contexto de SDL, la RTM también vincula los requerimientos de seguridad con las prácticas aplicadas en cada fase, facilitando el seguimiento y la auditoría.



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



7. Prácticas Adicionales de Seguridad en SDL:

- **Fase de Requerimientos:** Además del modelo de control de acceso, SDL recomienda actividades como la clasificación de datos para identificar información sensible (por ejemplo, detalles de incidentes o datos personales) y definir medidas de protección específicas, como cifrado o anonimización.
- **Fase de Diseño:** Además del modelado de amenazas y DFD, SDL promueve la revisión de diseño seguro, aplicando principios como defensa en profundidad, uso de componentes seguros y validación de entradas para prevenir vulnerabilidades como inyecciones SQL o XSS.

Desarrollo

Metodología: SDL

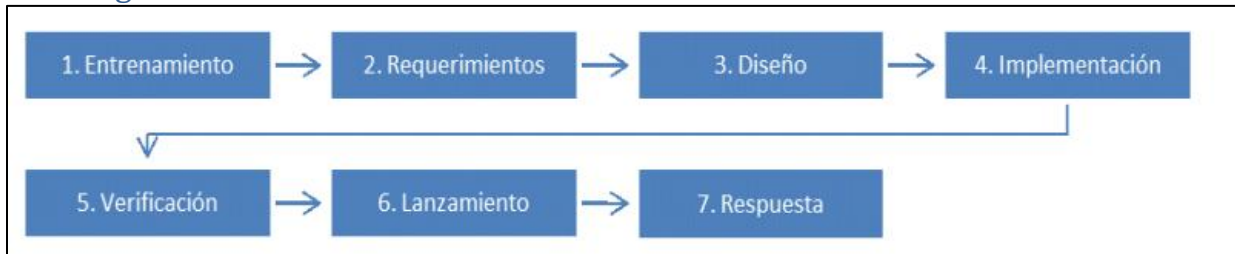


Ilustración 1 Fases de la metodología SDL

Actividades del SDL para la Seguridad	
1. Entrenamiento	5. Verificación
Entrenamiento de seguridad básica	Análisis dinámico
2. Requerimientos	Fuzz Testing
Establecer requerimientos de seguridad	Revisión de la superficie de ataques
Crear umbrales de calidad y límites de errores	6. Lanzamiento
Evaluación de los riesgos de seguridad y privacidad	Plan de respuesta a incidentes
3. Diseño	Revisión de seguridad final
Establecer requerimientos de diseño	Aprobar y archivar lanzamiento
Análisis de la superficie de ataques	7. Respuesta
Modelado de amenazas	Ejecutar el plan de respuesta a incidentes
4. Implementación	
Utilizar herramientas aprobadas	
Prohibir funciones no seguras	
Análisis estático	

Ilustración 2 Actividades del SDL para la Seguridad



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



1. Entrenamiento

Como parte fundamental del proceso de desarrollo de software seguro, todos los integrantes del equipo de desarrollo deben recibir una formación continua y actualizada en temas de seguridad informática y privacidad de la información. Esta capacitación tiene como objetivo garantizar que el equipo esté preparado para identificar, prevenir y mitigar amenazas durante todo el ciclo de vida del sistema.

De acuerdo con las buenas prácticas en ingeniería de software seguro, los miembros con funciones técnicas Estos entrenamientos deben cubrir conceptos esenciales como:

- Defensa en profundidad
- Principio de privilegios mínimos
- Modelos de análisis de riesgos
- Vulnerabilidades como saturaciones de búfer
- Inyecciones de código SQL
- Criptografía débil
- Evaluación de riesgos
- Procedimientos para el desarrollo orientado a la privacidad

2. Requerimientos

Requerimientos funcionales.

ID	Descripción
RF-01	Registrar incidentes con campos: fecha/hora, origen, activo afectado, criticidad preliminar, evidencia.
RF-02	Clasificar incidentes según ISO 27035 (evento, incidente, brecha).
RF-03	Flujo de estados: <i>Nuevo</i> → <i>En análisis</i> → <i>Contenido</i> → <i>Cerrado</i> .
RF-04	Alertar por correo cuando se cambie el estado o criticidad a <i>Alta</i> .
RF-05	Generar reportes mensuales.
RF-06	Exportar casos a PDF para la Superintendencia.

En la tabla 1 se presenta la historia de usuario enfocada en la **creación de un incidente** con todos los campos iniciales. Interviene principalmente el **Analista SOC**, quien registra la información y adjunta evidencias. Sirve para iniciar el flujo de gestión con trazabilidad y control de integridad de datos. Incluye criterios de aceptación para altas exitosas y validación de formularios.

Nro: US-01	Título: Registrar incidente	Prioridad: Alta Estimación: 12 horas
Historia de usuario: Como Analista de Centro de Operaciones de Seguridad quiero registrar un incidente con fecha/hora, origen, activo afectado, criticidad preliminar y evidencia para iniciar el flujo de gestión y seguimiento.		
Criterios de aceptación Escenario 1 – Registro exitoso		



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



<ul style="list-style-type: none">• Precondición: formulario completo.• Ejecución: clic en <i>Guardar</i>.• Resultado: incidente creado, estado <i>Nuevo</i> e ID generado. <p>Escenario 2 – Datos faltantes</p> <ul style="list-style-type: none">• Precondición: campo vacío.• Ejecución: clic en <i>Guardar</i>.• Resultado: mensaje de error; no se crea incidente.
<p>QSR (Quality-of-Service Requirement) y requisitos de seguridad</p> <ul style="list-style-type: none">• Clasificación PII(Personally Identifiable Information): Sí (datos de reportante).• Disponibilidad: 99,9 %.• Tamaño máximo de evidencia: 10 MB.• Trazabilidad: registrar acción en audit-log inmutable.
<p>Tareas de implementación (12 h)</p> <ol style="list-style-type: none">1. Maquetar formulario de alta (1 h)2. Crear entidad Incident y tabla (2 h)3. API POST /incidents + servicio (2 h)4. Validaciones de campos y 10 MB (1 h)5. Generar ID y estado inicial (0,5 h)6. Registrar en audit-log (1 h)7. Actualizar Threat Model (0,5 h)8. Tests BDD + unitarios (3 h)9. Documentar (1 h)

Tabla 1 US-01 Registrar Incidente

En la tabla 2 se detalla la funcionalidad de **asignar la categoría Evento, Incidente o Brecha** conforme a la norma ISO 27035. Participan el Analista SOC y, en casos de revisión, el Jefe SOC. Permite priorizar la respuesta y generar métricas basadas en la severidad formal. Los criterios de aceptación aseguran que solo se acepten valores válidos y que el cambio quede auditado.

Nro: US-02	Título: Clasificar incidente (ISO 27035)	Prioridad: Alta Estimación: 8 horas
<p>Historia de usuario: Como Analista de Centro de Operaciones de Seguridad quiero clasificar cada registro como Evento, Incidente o Brecha según ISO 27035 para estandarizar la severidad y priorizar la respuesta.</p>		
<p>Criterios de aceptación</p> <p>Escenario 1 – Clasificación correcta</p> <ul style="list-style-type: none">• Precondición: incidente en estado <i>Nuevo</i>• Ejecución: elegir tipo en lista ISO 27035 y guardar• Resultado: campo <i>Tipo</i> actualizado; se muestra en la vista de lista <p>Escenario 2 – Tipo no seleccionado</p> <ul style="list-style-type: none">• Precondición: campo <i>Tipo</i> vacío• Ejecución: clic en <i>Guardar</i>		



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



<ul style="list-style-type: none">• Resultado: mensaje de error «Debe seleccionar Evento, Incidente o Brecha»
QSR (Quality-of-Service Requirement) y requisitos de seguridad <ul style="list-style-type: none">• Solo roles Analista SOC o Jefe SOC pueden clasificar• Cambios se trazan en audit-log• Validar entrada contra valores fijos (lista blanca)
Tareas de implementación (8 h) <ol style="list-style-type: none">1. Añadir campo type y enum BD (1 h)2. Desplegar combo ISO 27035 en UI (1 h)3. Endpoint PUT /incidents/{id}/type (1 h)4. Validaciones de roles (1 h)5. Registro en audit-log (0.5 h)6. Pruebas de aceptación (2.5 h)

Tabla 2 US-02 Clasificar incidente

En la tabla 3 se describe el **cambio controlado de estados** dentro del ciclo de vida: Nuevo → En análisis → Contenido → Cerrado. El **Jefe SOC** es el actor clave para autorizar transiciones, garantizando procesos y cumplimiento de SLA. Evita saltos no permitidos y mantiene un historial inmutable que apoyará los informes de auditoría. Criterios de aceptación cubren transiciones válidas y bloqueos ante errores.

Nro: US-03	Título: Flujo de estados del incidente	Prioridad: Alta Estimación: 10 horas
Historia de usuario: Como Jefe de Centro de Operaciones de Seguridad quiero mover incidentes a través de los estados <i>Nuevo</i> → <i>En análisis</i> → <i>Contenido</i> → <i>Cerrado</i> para reflejar su progreso y generar métricas.		
Criterios de aceptación Escenario 1 – Transición válida <ul style="list-style-type: none">• Precondición: incidente en estado actual permitido• Ejecución: seleccionar siguiente estado y guardar• Resultado: estado actualizado y timestamp registrado Escenario 2 – Transición no permitida <ul style="list-style-type: none">• Precondición: intentar saltar de <i>Nuevo</i> a <i>Cerrado</i>• Ejecución: guardar• Resultado: mensaje «Transición no permitida»		
QSR (Quality-of-Service Requirement) y requisitos de seguridad <ul style="list-style-type: none">• Solo Jefe SOC puede cerrar incidentes• Historial de estados inmutable• Notificar cambio via audit-log		
Tareas de implementación (10 h) <ol style="list-style-type: none">1. Definir máquina de estados (1 h)2. Endpoint PATCH /incidents/{id}/state (2 h)3. Validar reglas de transición (2 h)		



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



4. UI de cambio de estado (1 h)
5. Registro en historial + audit-log (1 h)
6. Pruebas unitarias y BDD (3 h)

Tabla 3 US-03 Flujo de estado del incidente

En la tabla 4 se define la historia que **dispara notificaciones** cuando la criticidad sube a Alta o el estado pasa a Contenido. Intervienen sistemas externos y el Jefe SOC como receptor. Su objetivo es acelerar la reacción del equipo ante incidentes críticos. Incluye escenarios para verificar la entrega oportuna y el manejo de reintentos seguros.

Nro: US-04	Título: Alertas por correo	Prioridad: Media Estimación: 13 horas
Historia de usuario: Como Jefe de Centro de Operaciones de Seguridad quiero recibir alertas por correo cuando la criticidad se marque <i>Alta</i> o el estado cambie a <i>Contenido</i> para reaccionar oportunamente.		
Criterios de aceptación Escenario 1 – Alerta por criticidad <ul style="list-style-type: none">• Precondición: incidente criticidad <i>Media</i>• Ejecución: cambiar a <i>Alta</i>• Resultado: correo y mensaje Teams enviados en < 30 s Escenario 2 – Alerta por estado <ul style="list-style-type: none">• Precondición: incidente en <i>En análisis</i>• Ejecución: cambiar a <i>Contenido</i>• Resultado: notificaciones enviadas		
QSR (Quality-of-Service Requirement) y requisitos de seguridad <ul style="list-style-type: none">• Logs de entrega de notificaciones• Límite de 3 reintentos si falla envío		
Tareas de implementación (13 h) <ol style="list-style-type: none">1. Configurar servicio de correo SMTP seguro (1 h)2. Disparador en cambios de criticidad/estado (2 h)3. Plantillas de mensaje (1 h)4. Registro de intentos y reintentos (2 h)5. Pruebas con simulador (3 h)6. Documentar configuración (3 h)		

Tabla 4 US-04 Alertas por correo



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



En la tabla 5 se resume la capacidad de **visualizar métricas en tiempo real** y generar reportes PDF cada mes. El **Gerente de Riesgos** consulta tendencias y cumplimiento de objetivos. La tabla explica requisitos de rendimiento, firma digital y acceso seguro a la API de métricas. Criterios de aceptación validan la actualización en vivo y la generación correcta del informe.

Nro: US-05	Título: Reportes mensuales	Prioridad: Media Estimación: 18 horas
Historia de usuario: Como Gerente de Riesgos quiero ver y generar reportes mensuales PDF para evaluar tendencias y cumplimiento de SLA.		
Criterios de aceptación Escenario 1 – Reporte mensual <ul style="list-style-type: none">Precondición: usuario autenticado con rol Gerente, seleccionar mes a descargarEjecución: clic en <i>Generar PDF</i>Resultado: se descarga documento con indicadores (n.º incidentes, MTTR, top activos) y firma digital		
QSR (Quality-of-Service Requirement) y requisitos de seguridad <ul style="list-style-type: none">PDF firmado con certificado interno		
Tareas de implementación (18 h) <ol style="list-style-type: none">API agregación métricas (3 h)Gráficas (4 h)Servicio generación PDF (3 h)Firma digital y timestamp (2 h)Caché de métricas 30 s (1 h)Pruebas de rendimiento (3 h)Documentación de uso (2 h)		

Tabla 5 US-05 Reportes Mensuales

En la tabla 6 se expone la historia para **exportar registros** en formatos regulados, dirigida al **Auditor Externo**. Facilita el envío de datos a la Superintendencia con filtrado de columnas e integridad hash. Los criterios de aceptación cubren las descargas en ambos formatos y el registro de la acción en audit-log. Las tareas aseguran cumplimiento de límites de filas y sanitización de datos.

Nro: US-06	Título: Exportar incidentes CSV/PDF	Prioridad: Baja Estimación: 9 horas
Historia de usuario: Como Auditor Externo quiero exportar la lista de incidentes en CSV o PDF para remitirla a la Superintendencia conforme lo solicita la normativa.		
Criterios de aceptación Escenario 1 – Exportación CSV <ul style="list-style-type: none">Precondición: rol Auditor autenticadoEjecución: clic en <i>Exportar CSV</i>Resultado: descarga archivo con separador coma y cabeceras oficiales		



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Escenario 2 – Exportación PDF

- Precondición: rol Auditor autenticado
- Ejecución: clic en *Exportar PDF*
- Resultado: descarga PDF con sello de integridad y hash SHA-256

QSR (Quality-of-Service Requirement) y requisitos de seguridad

- Datos limitados a columnas autorizadas por la SBS
- Exportaciones registradas en audit-log
- Límite: 1 000 filas por exportación

Tareas de implementación (9 h)

1. Endpoint GET /incidents/export?format=csv (1.5 h)
2. Endpoint PDF (2 h)
3. Sanitizar y formatear datos (1 h)
4. Firma/hash de PDF (1 h)
5. UI de selección de formato (0.5 h)
6. Registro en audit-log (1 h)
7. Pruebas de formato y límite (2 h)

Tabla 6 US-06 Exportar incidentes CSV/PDF

Requerimientos no funcionales del sistema

- **Disponibilidad** (horario 24 × 7).
- **Tiempo de respuesta** para operaciones CRUD.
- **Usabilidad:** interfaz web responsiva (Node.js Angular).
- **Cumplimiento:** logs y retención 5 años (LOPD Art. 11).

En la tabla 7 se documenta el requisito de la disponibilidad este requisito enfrenta la necesidad operativa de que el servicio nunca “duerma”. Interviene principalmente el equipo de Operations/SRE, que configura y monitorea el SLA de 99,9 %. El objetivo es que los analistas puedan registrar incidentes a cualquier hora. Se valida con paneles de uptime y reportes mensuales.

ID	Tipo	Descripción	Métrica / Umbral	Prior.	Verificación	Evidencia	Estado
NF-01	NFR	El sistema debe estar disponible las 24 h los 7 días	SLA \geq 99,9 % mensual (\approx 43 min de caída)	Alta	Monitor de uptime	Reporte mensual de SLA	Propuesto

Tabla 7 NF-01 Disponibilidad 24 × 7



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



En la tabla 8 en el requisito de tiempo de respuesta participan Desarrolladores y QA para garantizar que todas las altas, bajas y consultas respondan en menos de 2 s (p95). Se busca evitar frustración del usuario y liberar recursos de servidor. Las pruebas de carga (Locust/JMeter) se integran al CI. Los resultados viajan en cada reporte de build.

ID	Tipo	Descripción	Métrica / Umbral	Prior.	Verificación	Evidencia	Estado
NF-02	NFR	Las operaciones CRUD deben responder rápido	Latencia $p95 \leq 2 \text{ s}$; $p50 \leq 0,5 \text{ s}$	Alta	Prueba de carga (Locust / JMeter) en CI	Informe de performance por build	Propuesto

Tabla 8 NF-02 Tiempo de respuesta CRUD

El equipo UX/Front-end lidera este requisito expuesto en la tabla 9, asegurando que la interfaz Angular se adapte a móvil, tablet y escritorio. La métrica se mide con Lighthouse & WCAG, persiguiendo una puntuación ≥ 90 . El fin es accesibilidad universal sin apps nativas. Se comprueba sprint a sprint en la demo de producto.

ID	Tipo	Descripción	Métrica / Umbral	Prior.	Verificación	Evidencia	Estado
NF-03	NFR	UI debe adaptarse a móvil, tablet y desktop	Lighthouse "Best Practices" ≥ 90 ; WCAG AA	Media	Test UX + Lighthouse en pipeline	PDF de resultados Lighthouse	Propuesto

Tabla 9 NF-03 Usabilidad responsiva

En la tabla 10 se observa la Seguridad, Legal y la mesa de datos velan por guardar registro por 60 meses según la LOPDP. Esto protege a la organización ante auditorías forenses. Se define un vault barato (S3-IA o Blob Archive) y un plan de restauración $\leq 24 \text{ h}$. Auditorías anuales generan la evidencia documental.

ID	Tipo	Descripción	Métrica / Umbral	Prior.	Verificación	Evidencia	Estado
NF-04	NFR	Conservar logs y metadatos 5 años	≥ 60 meses de retención; recuperación $\leq 24 \text{ h}$	Alta	Auditoría anual de retención	Certificado de auditoría	Propuesto

Tabla 10 NF-04 Cumplimiento – Logs 5 años



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Requerimientos de seguridad.

- **RS-01 Confidencialidad:** cifrado AES-256 en reposo.
- **RS-02 Integridad:** firma de integridad en adjuntos de evidencia.
- **RS-03 Disponibilidad:** protección DoS (WAF + rate-limit).
- **RS-04 Trazabilidad:** auditoría inmutable con hash encadenado.
- **RS-05 Privacidad:** anonimización de PII en los informes externos.

A continuación, se representaran los requisitos de seguridad el requisito cubre la capa de cifrado tanto “en vuelo” como “en reposo”. SecOps configura TLS 1.3 en el front y discos cifrados en el cloud. Así se asegura que terceros no lean ni bases de datos ni tráfico. Se certifica con escaneos SSL Labs y comprobaciones de políticas de clave, tal y como se observa en la tabla 11.

ID	Tipo	Descripción	Métrica / Umbral	Prior.	Verificación	Evidencia	Estado
RS-01	SEC	Cifrado AES-256 en reposo	100 % de endpoints HTTPS; discos cifrados	Alta	Qualys / SSL Labs scan + Infra check	Reporte de escaneo (evidencia objetiva)	Propuesto

Tabla 11 RS-01 Confidencialidad (TLS 1.3 + AES-256)

Desarrolladores añaden firmas SHA-256 a cada archivo de evidencia; QA valida que se verifiquen al descargar. El fin es detectar alteraciones o corrupción. Evita fraudes en procesos legales. Hashes se almacenan en BD y se revisan en pruebas unitarias de seguridad tal y como se observa en la tabla 12.

ID	Tipo	Descripción	Métrica / Umbral	Prior.	Verificación	Evidencia	Estado
RS-02	SEC	Firmar adjuntos de evidencia para evitar manipulación	Firma SHA-256; verificación OK al descargar	Alta	Prueba unitaria + revisión de código	Hashes almacenados en DB	Propuesto

Tabla 12 RS-02 Integridad de adjuntos

Infra & SecOps orquestan un WAF con rate-limit (≤ 100 req/s/IP) para frenar ataques de denegación de servicio. El beneficio es mantener la plataforma operativa aun bajo abuso. Pentesters ejecutan simulaciones de carga maliciosa. Logs del WAF y reportes de test son la evidencia tal y como se observa en la tabla 13.

ID	Tipo	Descripción	Métrica / Umbral	Prior.	Verificación	Evidencia	Estado
RS-03	SEC	Mitigar ataques de denegación de servicio	WAF activo + rate-limit ≤ 100 req/s/IP	Alta	Pentest de DoS controlado	Log WAF + reporte pentest	Propuesto

Tabla 13 RS-03 Disponibilidad frente a DoS

Auditoría y Dev kollaboran para encadenar hashes (tipo blockchain light) en el audit-log. Sirve de “caja negra” que nadie puede editar sin dejar huella. Garantiza no repudio y facilita investigación post-incidente. Scripts



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



de verificación periódica confirman consistencia tal y como se observa en la tabla 14.

ID	Tipo	Descripción	Métrica / Umbral	Prior.	Verificación	Evidencia	Estado
RS-04	SEC	Audit-log inmutable con hash encadenado	100 % eventos firmados; detección alteraciones	Media	Revisión de hash-chain + script verif.	Informe de consistencia	Propuesto

Tabla 14 RS-04 Trazabilidad inmutable

El DPO y el equipo de datos establecen reglas para eliminar o seudonimizar PII en reportes externos. La motivación es cumplir la LOPDP y el principio de minimización. Nombres se reemplazan por hashes, IDs por pseudónimos. Pruebas de salida y revisiones funcionales avalan el cumplimiento tal y como se observa en la tabla 15.

ID	Tipo	Descripción	Métrica / Umbral	Prior.	Verificación	Evidencia	Estado
RS-05	SEC	Ocultar datos personales en informes externos	Nombres → hash irreversible; IDs → pseudónimo	Alta	Test de salida + revisión funcional	Ejemplos de informe sin PII	Propuesto

Tabla 15 RS-05 Privacidad – Anonimización



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Casos de uso y mal uso

A continuación, se observan los casos de uso y de mal uso del sistema:

Casos de uso

Código	CU-01		
Nombre	Registrar Incidente	Actor	Analista SOC
Descripción	Permite al analista registrar un nuevo incidente de seguridad.		
Precondiciones	Usuario autenticado		
Flujo principal			
1. Accede al formulario.			
2. Ingresar los datos del incidente.			
3. El sistema valida los campos y tamaño de evidencia.			
4. Guarda el incidente con estado Nuevo.			
5. Registra en audit-log.			
Postcondición	Incidente registrado con ID generado y trazabilidad registrada.		

Tabla 16 CU-01

El caso de uso de la tabla 16 se permite iniciar el flujo de gestión de incidentes desde su creación por parte del analista de seguridad.

Código	CU-02		
Nombre	Clasificar Incidente	Actor	Analista SOC
Descripción	Permite clasificar un incidente según ISO 27035.		
Precondiciones	Incidente en estado Nuevo o En análisis.		
Flujo principal			
1. El analista accede al incidente. 2. Selecciona tipo (evento/incidente/brecha). 3. El sistema guarda el cambio y registra actividad.			
Postcondición	El incidente queda clasificado correctamente.		

Tabla 17 CU-02

El caso de uso de la tabla 17 se escribe el proceso mediante el cual un incidente es categorizado conforme a la norma ISO 27035.

Código	CU-03		
Nombre	Cambiar Estado del Incidente	Actor	Analista SOC
Descripción	Actualiza el estado del incidente a En análisis, Contenido o Cerrado.		
Precondiciones	Incidente no cerrado		



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Flujo principal	
1. Accede al incidente. 2. Cambia el estado. 3. Si la criticidad es alta, se notifica. 4. Se registra en el audit-log.	
Postcondición	Estado del incidente actualizado y alerta enviada si corresponde.

Tabla 18 CU-03

El caso de uso de la tabla 18 se define cómo el analista actualiza el estado del incidente y activa alertas si la criticidad lo requiere.

Código	CU-04		
Nombre	Exportar o Visualizar Reportes	Actor	Auditor / Administrador
Descripción	Permite generar reportes mensuales o exportar a CSV/PDF.		
Precondiciones	Usuario con permisos adecuados		
Flujo principal			
1. Aplica filtros de búsqueda.			
2. Elige formato (gráfico o archivo).			
3. Se anonimiza PII si aplica.			
4. El sistema genera el resultado.			
Postcondición	Reporte generado de forma segura y conforme a normas de privacidad.		

Tabla 19 CU-04

El caso de uso de la tabla 19 permite a usuarios autorizados generar reportes con anonimización de datos sensibles conforme a la LOPDP.

Casos de mal uso

Código	MU-01		
Nombre	Inyección SQL en Registro	Actor	Atacante autenticado
Descripción	Intenta insertar SQL malicioso en campos del formulario de incidente.		
Flujo del ataque			
1. Ingresa payload malicioso.			
2. El sistema valida entradas y usa consultas parametrizadas.			
3. Rechaza el intento y lo registra.			



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Resultado esperado	El sistema bloquea el ataque y alerta al administrador si es necesario.
--------------------	---

Tabla 20 MU-01

El caso de mal uso de la tabla 20 representa un intento de ataque mediante la inserción de código SQL malicioso en campos del formulario.

Código	MU-02		
Nombre	Manipulación de Evidencia	Actor	Usuario malicioso
Descripción	Intenta modificar un archivo de evidencia ya cargado.		
Flujo del ataque			
1. Intenta reemplazar archivo. 2. El sistema verifica integridad con firma. 3. Detecta alteración y bloquea el cambio.			
Resultado esperado	Evidencia protegida, intento registrado y alertado.		

Tabla 21 MU-02

El caso de mal uso de la tabla 21 expone el riesgo de modificación de archivos subidos y la validación de integridad mediante firma digital.

Código	MU-03		
Nombre	Escalada de Privilegios vía Token	Actor	Atacante autenticado
Descripción	Modifica su token de sesión para obtener acceso como administrador.		
Flujo del ataque			
1. Modifica el token localmente.			
2. El backend valida firma JWT.			
3. Acceso es denegado y se registra intento.			
Resultado esperado	Acceso bloqueado, sistema resiliente ante tokens manipulados.		

Tabla 22 MU-03

El caso de mal uso de la tabla 22 ilustra cómo un atacante intenta modificar su token para adquirir un rol no autorizado dentro del sistema.

Código	MU-04		
Nombre	Exposición de PII en Reportes	Actor	Auditor o Externo
Descripción	Intenta acceder a datos personales en reportes generados.		
Flujo del ataque			
1. Solicita reporte externo.			
2. Sistema aplica anonimización antes de exportar.			



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Resultado esperado	Información PII no expuesta; auditoría conforme a LOPDP.
--------------------	--

Tabla 23 MU-04

El caso de mal uso de la tabla 23 muestra cómo el sistema previene la divulgación de datos personales mediante anonimización previa.

Código	MU-05		
Nombre	Acceso No Autorizado a Logs	Actor	Usuario no autorizado
Descripción	Intenta acceder a registros de auditoría sin permiso.		
Flujo del ataque			
1. Intenta acceder a endpoint restringido. 2. Backend verifica permisos. 3. Rechaza acceso y registra intento.			
Resultado esperado	Acceso denegado (403) y evento registrado en audit-log.		

Tabla 24 MU-05

El caso de mal uso de la tabla 24 refleja el intento de un usuario sin permisos de acceder al registro de auditoría del sistema.

Modelo de control de acceso:

Modelo de Control de Acceso Basado en Roles con Restricciones Temporales (TRBAC)

Este modelo es una extensión del clásico RBAC (**Role-Based Access Control**) que añade la dimensión temporal a las reglas de acceso. Cada regla define qué puede hacer un rol, sobre qué recurso, y en qué horarios. La sintaxis general que usas es:

<Rol, Acción, Recurso, TiempoInicio, TiempoFin>

Usuario

Rol responsable de registrar incidentes, pero sin acceso a clasificación, estados ni reportes.

- <Usuario, Crear, Incidente, Lunes 08:00, Viernes 17:00>
- <Usuario, Ver, Incidentes, Lunes 08:00, Viernes 17:00>
- <Usuario, Editar, Incidentes, Lunes 08:00, Viernes 17:00>
- <Usuario, Adjuntar, Evidencia, Lunes 08:00, Viernes 17:00>

Analista de Seguridad

Encargado de la gestión activa de incidentes: clasificación, estado, reportes.

- <Analista de Seguridad, Ver, Todos los incidentes, Lunes 07:00, Viernes 19:00>
- <Analista de Seguridad, Editar, Incidente (excepto campos del Usuario), Lunes 07:00, Viernes 19:00>
- <Analista de Seguridad, Clasificar, Incidente (ISO 27035), Lunes 07:00, Viernes 19:00>



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



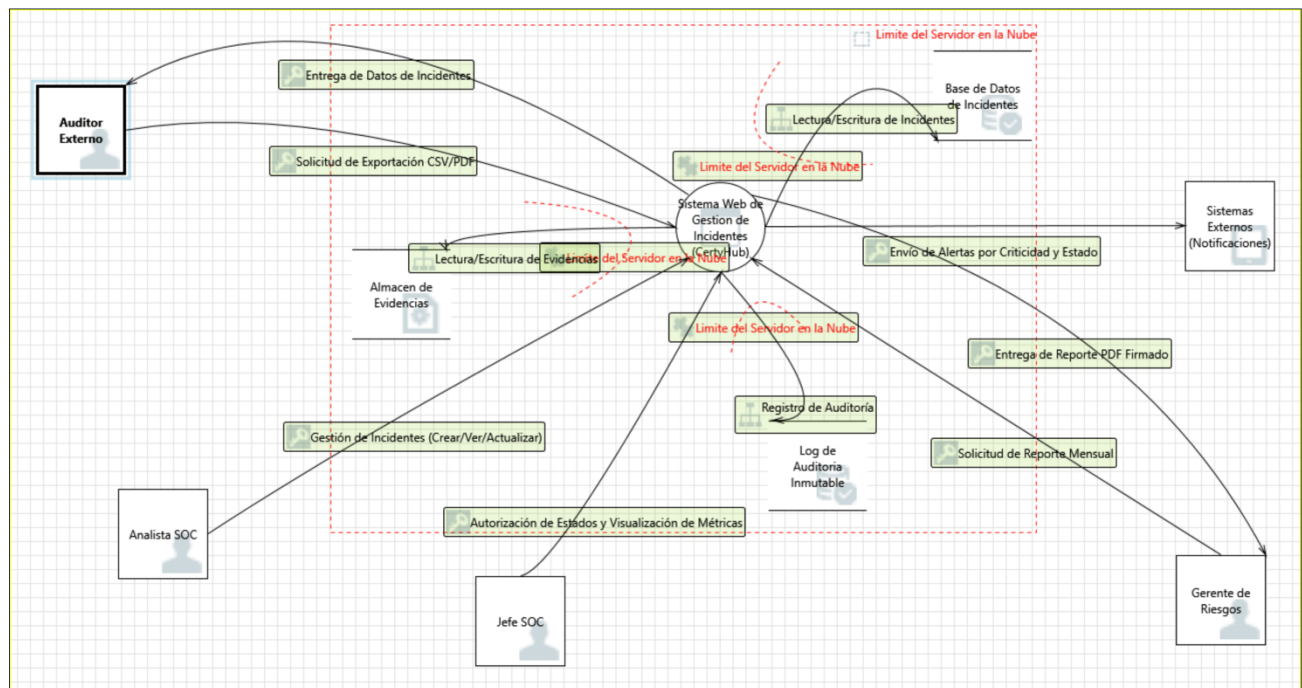
- <Analista de Seguridad, Cambiar estado, Incidente, Lunes 07:00, Viernes 19:00>
- <Analista de Seguridad, Enviar notificación, Cambio de estado o criticidad, Lunes 07:00, Viernes 19:00>
- <Analista de Seguridad, Generar, Reporte mensual, Último día del mes 17:00, Último día del mes 18:00>
- <Analista de Seguridad, Visualizar, Dashboard de incidentes, Lunes 07:00, Viernes 19:00>
- <Analista de Seguridad, Exportar, Incidentes a CSV/PDF, Lunes 07:00, Viernes 19:00>

Auditor

Rol solo de consulta. Puede auditar todas las acciones del sistema.

- <Auditor, Ver, Incidentes, Lunes 00:00, Domingo 23:59>
- <Auditor, Ver, Evidencias, Lunes 00:00, Domingo 23:59>
- <Auditor, Ver, Estados de incidentes, Lunes 00:00, Domingo 23:59>
- <Auditor, Ver, Reportes mensuales, Lunes 00:00, Domingo 23:59>
- <Auditor, Exportar, Casos a CSV/PDF, Lunes 00:00, Domingo 23:59>

3. Diseño



Árbol de ataques

El SGISI es un sistema web diseñado para registrar, clasificar, gestionar y hacer seguimiento a incidentes de seguridad informática dentro de una organización. El árbol de ataques identifica dos amenazas principales que comprometen su seguridad: Divulgación de Información (Information Disclosure) y Denegación de



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



Servicio (Denial of Service), cada una con subamenazas específicas y vectores de ataque detallados.

Completo del sistema:

La ilustración 3 presenta el árbol de ataques general del Sistema de Gestión de Incidentes y Seguridad (SGIS), destacando los riesgos principales de divulgación de información (impacto muy alto) y denegación de servicio (impacto muy bajo), con sus respectivas subamenazas y métodos de ataque, sirviendo como base para un análisis detallado de la seguridad del sistema.

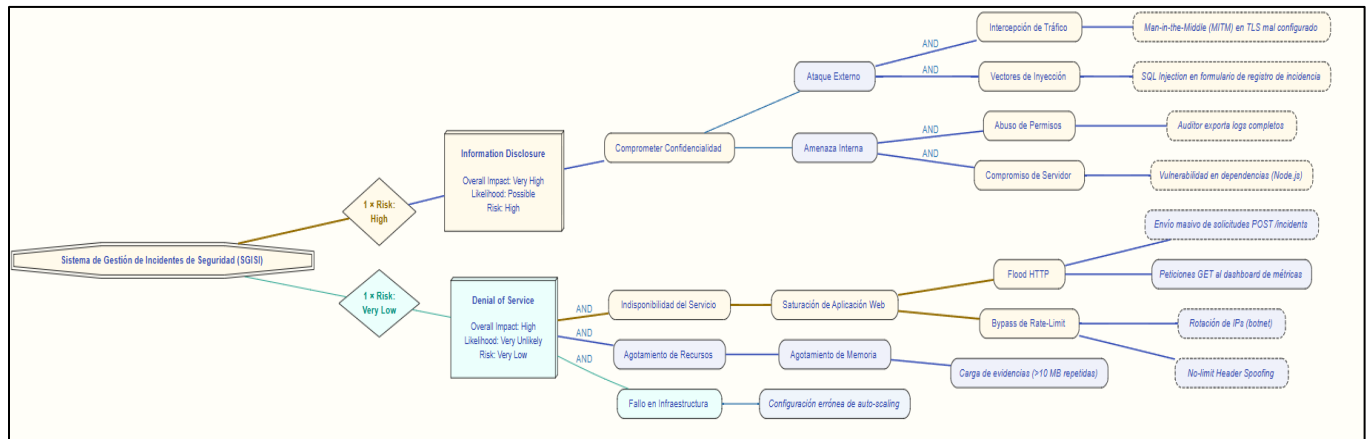


Ilustración 3 Árbol de ataques

1. Análisis y explicación del árbol de ataque - Completo del sistema.

El árbol de ataques para el "Sistema de Gestión de Incidentes y Seguridad (SGIS)" ofrece una visión integral de los riesgos asociados a este sistema crítico. Se identifican dos categorías principales de riesgo:

- **Divulgación de Información:** Clasificada con un impacto "Muy Alto" y un riesgo "Alto". Incluye amenazas como:
 - Compromiso de credenciales y ataques externos/internos.
 - Vulnerabilidades en aplicaciones (por ejemplo: inyecciones SQL, auditorías de código inseguro).
 - Compromiso de servidores debido a configuraciones débiles.
- **Denegación de Servicio:** Con un impacto "Muy Bajo" y riesgo "Bajo". Comprende interrupciones por saturación, agotamiento de recursos y fallos de infraestructura.

El árbol sugiere que la prioridad de mitigación debe centrarse en proteger la confidencialidad de la información, implementando controles de acceso robustos y parches de seguridad, mientras se refuerza la resiliencia contra ataques de denegación con tolerancia a fallos y escalabilidad adecuada.

Denegación de servicio:

En la ilustración 4 se detalla el subárbol de denegación de servicio del SGIS, ilustrando cómo la indisponibilidad del servicio, el agotamiento de recursos y los fallos de infraestructura, impulsados por ataques como Flood HTTP y bypass de rate-limit, generan un impacto alto con alta probabilidad, evidenciando áreas críticas para



la mitigación.

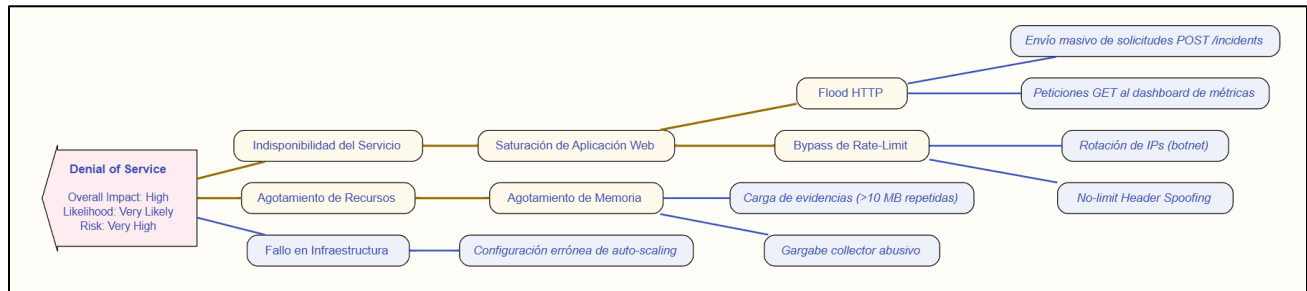


Ilustración 4 Subárbol denegación de servicio

2. Análisis y explicación del árbol de ataque – Denegación del servicio.

El subárbol de "Denial of Service" detalla las causas y métodos que pueden provocar la indisponibilidad del SGIS, con un impacto "Alto" y probabilidad "Muy Alta". Las ramas principales son:

- **Indisponibilidad del Servicio:** Este paso resulta de las siguientes causas observadas:
 - **Agotamiento de Recursos:** Incluye saturación de aplicaciones web (e.g., Flood HTTP) y agotamiento de memoria.
 - **Fallo en Infraestructura:** Provocado por configuraciones inadecuadas de autoescalado.
- **Métodos de Ataque:**
 - **Flood HTTP:** Sobrecarga mediante solicitudes masivas, incluyendo bypass de límites de tasa y carga de evidencia pesada (>10 MB repetida).
 - **Envío Masivo de Solicitudes POST:** Incluye peticiones al dashboard, rotación de IPs (botnets) y técnicas de header spoofing sin límite.
- **Implicaciones:** La saturación y el agotamiento de recursos pueden colapsar el sistema, mientras que los fallos de infraestructura amplifican el riesgo si el autoescalado no está optimizado.

Mitigaciones recomendadas incluyen límites de tasa estrictos, monitoreo de uso de recursos, y un diseño de autoescalado que responda dinámicamente a picos de tráfico.



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Divulgación de información

La ilustración 5 representa el subárbol de divulgación de información del SGIS, mostrando cómo los ataques externos (inyecciones SQL) y las amenazas internas (abuso de permisos) comprometen la confidencialidad con un impacto muy alto, subrayando la necesidad de controles robustos de seguridad.

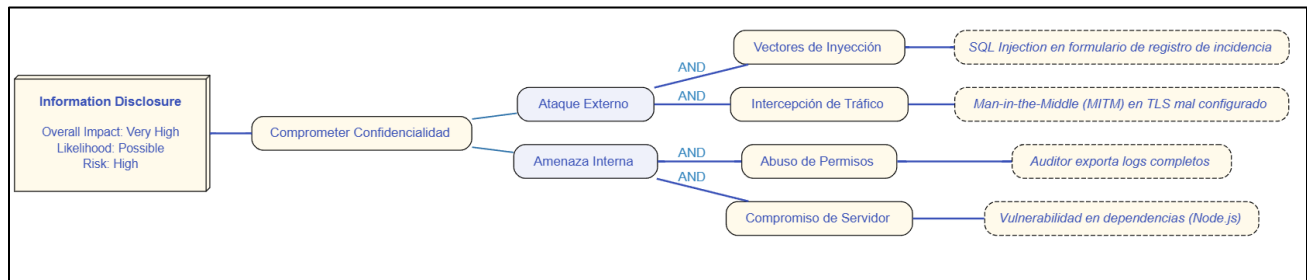


Ilustración 5 Subárbol divulgación de información

3. Análisis y explicación del árbol de ataque – Divulgación de información.

El subárbol de "**Information Disclosure**" aborda las amenazas que comprometen la confidencialidad del SGIS, con un impacto "Muy Alto" y riesgo "Alto". Las ramas clave son:

- **Compromiso de Credenciales:** Acceso no autorizado a datos sensibles, facilitado por ataques externos o internos.
- **Vulnerabilidades en Aplicaciones:** Incluyen inyecciones SQL y auditorías de código inseguro que exponen datos.
- **Compromiso de Servidor:** Resulta de configuraciones débiles o exploits específicos.

Métodos de Ataque:

- Inyección SQL para manipular bases de datos.
- Flood HTTP y bypass de límites para amplificar el acceso no autorizado.
- Header spoofing para engañar al sistema.
- El ataque que habitualmente pasa en la mayoría de programas que es el **Man in the middle**.

El enfoque de mitigación debe centrarse en cifrado de datos, autenticación multifactor, y revisiones regulares de código para eliminar vulnerabilidades. Además, los servidores deben estar protegidos con firewalls y parches actualizados.



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Desarrollo Segundo Bimestre



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Notas a contemplar para el Desarrollo de la aplicación.

FASE REQUERIMIENTOS:

- REQUERIMIENTOS DE SEGURIDAD
- CASOS DE MAL USO
- SISTEMA DE CONTROL ACCESO
 - RBAC + FECHAS
 - ROLES:
 - USUARIO: CREAR VER EDITAR INCIDENTES DE SEGURIDAD
 - ANALISTA DE SEGURIDAD:
 - AUDITOR
 - JEFE DE SOC
 - GERENTE DE RIESGOS... REPORTES MENSUALES

YO COMO USUARIO PUEDE VER TODOS LOS INCIDENTES
YO COMO USUARIO PUEDO EDITAR LOS QUE YO CREE
YO COMO USUARIO PUEDO ADJUNTAR EVIDENCIA

ANALISTA DE SEGURIDAD: VER INCIDENTES

ANALIZAR EL INCIDENTE
ACCIONES DE MITIGACIÓN

INCIDENTES SE CLASIFICAN: EVENTO INCIDENTE BRECHA

ANALISTA DE SEGURIDAD:

VER FLUJO DEL ESTADO: NUEVO, ANÁLISIS, CERRAR

ENVIAR NOTIFICACIÓN –

JEFE DE SOC – AUTORIZACIÓN DE ESTADOS
JEFE DE SOC – GENERACIÓN DE REPORTES

ANALISTA DE SEGURIDAD ENVIA NOTIFICACIÓN AL JEFE DE SOC
JEFE DE SOC NOTIFICA AL ANALISTA
ANALISTA NOTIFICA USUARIO

AUDITOR: REGISTRA TODAS LAS ACCIONES DE LOS USUARIOS
AUDITOR: GENERA REPORTES DE AUDITORIA

GERENTE DE RIESGOS



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



ALMACENES DE DATOS:

- INCIDENTES
- LOGS DE AUDITORIAS
- ALMACEN DE EVIDENCIA

ANALISTA SOC – GESTIÓN DE INCIDENTES

SPOOFING

- VALIDACIÓN DE ENTRADAS CON CHECKSUM Y LAS FIRMAS DIGITALES

ELEVACIÓN DE PRIVILEGIOS:

- INCLUIR MULTI FACTOR AUTENTICATION

DENEGACIÓN DE SERVICIOS:

- LIMITAR LOS RECURSOS
- AUTOESCALADO
- DIVULGACIÓN DE INFORMACIÓN NO AUTORIZADA
- CIFRAR DATOS + HASH + FIRMAS DIGITALES + ANONIMIZACIÓN
- FIREWALS



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Elaboración

En el segundo bimestre, se consolidan las fases de requerimientos y diseño del Sistema de Gestión de Incidentes y Seguridad (SGISI), enfocándose en la definición detallada de los requerimientos de seguridad, la identificación de casos de mal uso, y el diseño de un sistema de control de acceso basado en roles con restricciones temporales (TRBAC). Estas actividades se alinean con la metodología Security Development Lifecycle (SDL) para garantizar un sistema seguro, escalable y conforme a normativas como ISO 27035 y la Ley Orgánica de Protección de Datos Personales (LOPD). A continuación, se presentan las secciones correspondientes, detallando los artefactos generados, las medidas de seguridad aplicadas, y las verificaciones realizadas, acompañadas de explicaciones específicas para cada tabla que ilustran su propósito, implementación, beneficios y validación.

Requerimientos – Segundo Bimestre

Requerimientos de Seguridad – Tabla actualizada

A continuación, se representan los requerimientos de seguridad. Cada requerimiento aborda una capa crítica de protección, como el cifrado de datos, la integridad de evidencias, la disponibilidad frente a ataques, y la autenticación robusta. SecOps configura tecnologías como TLS 1.3, AES-256, firmas digitales SHA-256, y firewalls con rate-limiting, mientras que los desarrolladores implementan validaciones estrictas y anonimización de datos. Estas medidas aseguran que los datos sean confidenciales, inalterables y accesibles solo para usuarios autorizados, cumpliendo con LOPDP y protegiendo contra amenazas STRIDE. La verificación se realiza mediante escaneos de seguridad, pruebas automatizadas, y auditorías, como se detalla en la Tabla 25.

ID	Tipo	Descripción	Métrica / Umbral	Prior.	Verificación	Evidencia	Estado
RS-01	SEC	Cifrado AES-256 en reposo y TLS 1.3 en tránsito	100 % de endpoints HTTPS; discos cifrados	Alta	Escaneos Qualys/SSL Labs; revisión de configuración de infraestructura	Reporte de escaneo SSL Labs	Implementado
RS-02	SEC	Firma digital SHA-256 para adjuntos de evidencia	Firma verificada al descargar; hash almacenado en BD	Alta	Pruebas unitarias de integridad; revisión de código	Log de hashes en BD	Implementado
RS-03	SEC	Protección contra ataques de denegación de servicio (DoS)	WAF activo; rate-limit \leq 100 req/s/IP	Alta	Simulaciones de pentest DoS; revisión de logs WAF	Reporte de pentest y logs WAF	Implementado



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



RS-04	SEC	Audit-log inmutable con hash encadenado	100% eventos firmados; detección de alteraciones	Media	Script de verificación de hash-chain	Informe de consistencia de logs	Implementado
RS-05	SEC	Anonimización de PII en reportes externos	Nombres → hash irreversible; IDs → pseudónimo	Alta	Pruebas funcionales de reportes; revisión de salida	Ejemplo de informe anonimizado	Implementado
RS-06	SEC	Autenticación multifactor (MFA) para roles críticos	MFA obligatorio para Jefe SOC, Auditor, Gerente de Riesgos	Alta	Pruebas de acceso con MFA; auditoría de sesiones	Reporte de auditoría de sesiones	Propuesto
RS-07	SEC	Validación de entradas con checksum y listas blancas	100% de entradas validadas contra inyecciones SQL/XSS	Alta	Análisis estático (SAST); pruebas dinámicas (DAST)	Reporte SAST/DAST	Propuesto
RS-08	SEC	Protección contra elevación de privilegios	Validación estricta de tokens JWT; RBAC con restricciones temporales	Alta	Pruebas de seguridad en endpoints; revisión de RBAC	Reporte de pruebas de seguridad	Propuesto

Tabla 25 Requerimientos de Seguridad - Actualizados

Los requerimientos de seguridad del Sistema de Gestión de Incidentes de Seguridad Informática (SGIS) se definieron con base en el modelo STRIDE y las normas ISO/IEC 27035 y LOPDP:

Confidencialidad y Privacidad:

- Cifrado AES-256 en reposo y TLS 1.3 en tránsito.
- Anonimización de PII en reportes externos conforme a la LOPDP.
- Gestión de llaves criptográficas mediante HSM.

Integridad:

- Firmas digitales SHA-256 en todas las evidencias.
- Audit-log inmutable con hash encadenado.
- Validación de integridad con verificaciones periódicas de hash-chain.



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Disponibilidad:

- Protección DoS con WAF y rate-limit ≤ 100 req/s/IP.
- Autoescalado dinámico para picos de tráfico.
- SLA $\geq 99,9$ % con monitoreo continuo 24/7.

Autenticación y Autorización:

- Autenticación multifactor (MFA) para roles críticos.
- RBAC con restricciones temporales (TRBAC).
- Tokens JWT firmados y con expiración controlada.

Protección frente a STRIDE:

- **Spoofing:** MFA, validación de tokens, device fingerprint.
- **Tampering:** Evidencias y logs firmados digitalmente.
- **Repudiation:** Logs inmutables y encadenados.
- **Information Disclosure:** Cifrado, anonimización de PII y firewalls.
- **Denial of Service:** WAF, rate-limit, autoescalado.
- **Elevation of Privilege:** Principio de privilegios mínimos y MFA.

Los requerimientos de seguridad cubren la protección integral del SGIS, desde el cifrado de datos hasta la mitigación de ataques. SecOps configura TLS 1.3 para el tráfico de red y AES-256 para bases de datos y almacenamientos en la nube, asegurando que terceros no puedan interceptar ni leer datos sensibles. Los desarrolladores implementan firmas digitales SHA-256 para evidencias, garantizando su integridad. Para la disponibilidad, se despliega un WAF con rate-limiting, mientras que la anonimización protege la privacidad de datos personales. La autenticación multifactor (MFA) y la validación de tokens JWT previenen accesos no autorizados. Estas medidas se certifican con herramientas como Qualys/SSL Labs, pruebas SAST/DAST, simulaciones de pentest, y auditorías de configuración, proporcionando evidencia objetiva de cumplimiento, como se observa en la Tabla 25.



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Casos de Mal Uso – Identificados

El caso de mal uso de la tabla 26 describe cómo un atacante interno intenta alterar los registros de auditoría. El sistema lo previene mediante el uso de hash encadenado y revisiones periódicas, garantizando que los logs permanezcan íntegros y registrando cualquier intento fallido.

Código	MU-06		
Nombre	Manipulación de Logs	Actor	Atacante interno
Descripción	Intento de alterar registros de auditoría		
Flujo del ataque			
1. Hash encadenado + revisión periódica			
Resultado esperado	El intento es detectado y rechazado; el log permanece íntegro y se registra el intento fallido en el audit-log.		

Tabla 26 MU-06

El caso de mal uso de la tabla 27 muestra cómo un atacante externo intenta acceder con un token JWT robado. El sistema bloquea el acceso gracias a la autenticación multifactor, la expiración de sesiones y la validación de dispositivos, generando además una alerta de seguridad para el administrador.

Código	MU-07		
Nombre	Spoofing de Sesión	Actor	Atacante externo
Descripción	Uso de token JWT robado		
Flujo del ataque			
1. MFA, expiración de sesión 2. Validación de dispositivo			
Resultado esperado	El acceso es bloqueado; el token modificado se invalida y se genera alerta de seguridad al administrador.		

Tabla 27 MU-07



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



El caso de mal uso de la tabla 28 expone la situación en la que un usuario malicioso busca cargar evidencias infectadas o de tamaño excesivo. El sistema ejecuta un escaneo antivirus y valida las restricciones de formato y peso, rechazando el archivo y registrando el intento en el audit-log.

Código	MU-08		
Nombre	Subida de Evidencia Maliciosa	Actor	Usuario malicioso
Descripción	Adjuntar archivos infectados o con tamaño excesivo.		
Flujo del ataque			
1. Escaneo antivirus 2. Validación ≤ 10MB			
Resultado esperado	El archivo es rechazado; se notifica al usuario y el intento queda registrado en el audit-log.		

Tabla 28 MU-08

El caso de mal uso de la tabla 29 describe el intento de un usuario común por obtener permisos de Auditor. El backend valida los roles, aplica MFA y genera alertas de anomalías, bloqueando el acceso y registrando el intento en el audit-log.

Código	MU-09		
Nombre	Elevación de Privilegios	Actor	Usuario común
Descripción	Intento de obtener permisos de Auditor		
Flujo del ataque			
1. Validación backend + MFA + alertas de anomalías.			
Resultado esperado	El intento es bloqueado; se conserva el rol original del usuario y el evento queda registrado para auditoría.		

Tabla 29 MU-09



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Sistema de Control de Acceso – Actualizada

Modelo de Control de Acceso Basado en Roles con Restricciones Temporales (TRBAC)
Este modelo es una extensión del clásico RBAC (Role-Based Access Control) que añade la dimensión temporal a las reglas de acceso. Cada regla define qué puede hacer un rol, sobre qué recurso, y en qué horarios. La sintaxis general es:

<Rol, Acción, Recurso, TiempoInicio, TiempoFin>

Usuario

Rol responsable de registrar incidentes, pero sin acceso a clasificación, estados ni reportes.

- <Usuario, Crear, Incidente, Lunes 08:00, Viernes 17:00>
- <Usuario, Ver, Incidentes, Lunes 08:00, Viernes 17:00>
- <Usuario, Editar, Incidentes, Lunes 08:00, Viernes 17:00>
- <Usuario, Adjuntar, Evidencia, Lunes 08:00, Viernes 17:00>

Analista de Seguridad

Encargado de la gestión activa de incidentes: clasificación, estado, reportes.

- <Analista de Seguridad, Ver, Todos los incidentes, Lunes 07:00, Viernes 19:00>
- <Analista de Seguridad, Editar, Incidente (excepto campos del Usuario), Lunes 07:00, Viernes 19:00>
- <Analista de Seguridad, Clasificar, Incidente (ISO 27035), Lunes 07:00, Viernes 19:00>
- <Analista de Seguridad, Cambiar estado, Incidente, Lunes 07:00, Viernes 19:00>
- <Analista de Seguridad, Enviar notificación, Cambio de estado o criticidad, Lunes 07:00, Viernes 19:00>
- <Analista de Seguridad, Generar, Reporte mensual, Último día del mes 17:00, Último día del mes 18:00>
- <Analista de Seguridad, Visualizar, Dashboard de incidentes, Lunes 07:00, Viernes 19:00>
- <Analista de Seguridad, Exportar, Incidentes a CSV/PDF, Lunes 07:00, Viernes 19:00>

Auditor

Rol solo de consulta. Puede auditar todas las acciones del sistema.

- <Auditor, Ver, Incidentes, Lunes 00:00, Domingo 23:59>
- <Auditor, Ver, Evidencias, Lunes 00:00, Domingo 23:59>
- <Auditor, Ver, Estados de incidentes, Lunes 00:00, Domingo 23:59>
- <Auditor, Ver, Reportes mensuales, Lunes 00:00, Domingo 23:59>
- <Auditor, Exportar, Casos a CSV/PDF, Lunes 00:00, Domingo 23:59>

Jefe de SOC

Rol encargado de autorizar transiciones de estados y supervisar al equipo.

- <Jefe de SOC, Autorizar, Estados de incidente, Lunes 00:00, Domingo 23:59>
- <Jefe de SOC, Generar, Reportes críticos, Lunes 00:00, Domingo 23:59>
- <Jefe de SOC, Notificar, Analista de Seguridad, Lunes 00:00, Domingo 23:59>

Gerente de Riesgos

Encargado de evaluar métricas y cumplimiento de SLA.

- <Gerente de Riesgos, Ver, Reportes mensuales, Lunes 00:00, Domingo 23:59>
- <Gerente de Riesgos, Analizar, Tendencias SLA, Lunes 00:00, Domingo 23:59>



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



Almacenes de datos

- Incidentes: Base con campos estandarizados (ID, usuario, activo, criticidad, estado, fecha/hora, adjuntos).
- Logs de Auditoría: Registro inmutable con hash encadenado.
- Evidencias: Archivos cifrados AES-256 con firmas SHA-256 y validados contra malware.

Funcionalidad del Auditor

El sistema cuenta con una interfaz exclusiva para el rol Auditor, cuyo objetivo general es supervisar y analizar de forma segura el historial de eventos del sistema, identificando quién realizó cada acción y en qué momento, con la capacidad de profundizar en los incidentes y generar reportes descargables en formatos CSV y PDF.

Casos de uso principales

- **Ver lista de logs:** Pantalla con tabla paginada de eventos que incluye usuario, acción y fecha/hora.
- **Filtrar registros:** Posibilidad de búsqueda por usuario (email parcial), tipo de acción y rango de fechas.
- **Ver detalle de cada registro:** Modal con información ampliada del log (usuario, acción, fecha/hora, ID y título del incidente, criticidad, estado, activo afectado, enlace a evidencia).
- **Exportar un log:** Botones para descargar un registro individual en CSV o PDF, con sello de integridad y hash SHA-256.

Requerimientos de seguridad

- **Autenticación:** Uso de tokens JWT firmados con Supabase, enviados en cada petición con Authorization: Bearer <token>.
- **Autorización:** Aplicación de RBAC; solo el rol Auditor puede acceder a los endpoints /api/logs y exportaciones.
- **Integridad:** Cada entrada en audit_logs se protege mediante hash encadenado, evitando alteraciones no autorizadas.

Buenas prácticas:

- No exponer la clave de service_role en el frontend.
- Uso del cliente administrativo de Supabase solo en backend.
- Validación estricta de entradas y manejo seguro de errores.
- **CORS:** Configuración en Express para permitir solo cabeceras seguras y autorizadas.



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



Integración técnica

Backend (Node.js + Express + Supabase):

- Uso de authMiddleware.js para validar JWT y extraer metadatos de usuario.
- Registro de acciones con auditLogger.js, que encadena hashes y almacena en audit_logs.
- Rutas principales:
 - ✓ GET /api/logs → listado de logs.
 - ✓ GET /api/incidents/:id → detalle de incidente.
 - ✓ GET /api/logs/:id/export/csv y /export/pdf → exportación de registros.

Frontend (React + Material-UI + Axios):

- Página AuditLogPage.js con filtros interactivos, tabla de eventos y modal para detalles.
- Funcionalidad de descarga mediante Axios configurado con el token de autenticación.

La figura 6 muestra la vista principal del módulo de Auditoría, donde se despliega una tabla con el historial completo de eventos registrados en el sistema.

La interfaz permite aplicar filtros por usuario, tipo de acción y rango de fechas, ofreciendo al Auditor una visión clara y estructurada de quién realizó qué acción y en qué momento.

SDIS

Dashboard

Incidentes

Reportes

Logs de Auditoría

Sistema de Gestión de Incidentes de Seguridad

Auditor

S

Historial de Eventos (Logs)

Usuario

Ar.

Desde

dd/mm/aaaa

Hasta

dd/mm/aaaa

Limpiar

Usuario	Acción	Fecha y Hora
tewat63808@hostbyt.com	CREATE_INCIDENT	3/8/2025, 3:25:59 p. m.
shirley@gmail.com	CREATE_INCIDENT	3/8/2025, 3:13:52 p. m.
giso95479@hostbyt.com	CREATE_INCIDENT	3/8/2025, 1:19:56 p. m.
woxi20034@foboxs.com	CREATE_INCIDENT	3/8/2025, 9:37:48 a. m.
xfir33645@foboxs.com	UPDATE_INCIDENT	3/8/2025, 9:35:04 a. m.
xfir33645@foboxs.com	UPDATE_INCIDENT	3/8/2025, 9:34:59 a. m.

Ilustración 6 Historial de Eventos (Logs) del Auditor



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



La figura 7 presenta el modal de detalle de un registro de auditoría. En él se observa información clave del incidente asociado, incluyendo usuario, acción realizada, fecha y hora, criticidad, estado, activo afectado y enlace a la evidencia.

El Auditor puede exportar este registro individual en formatos **PDF** o **CSV**, con integridad garantizada mediante hash digital, facilitando así el cumplimiento de auditorías y reportes normativos.

Historial de Eventos (Loas)

Usuario

Usuario

tewat63808@hostbyt.com

shirley@gmail.com

giso95479@hostbyt.com

woxil20034@foboxs.com

xifir33645@foboxs.com

xifir33645@foboxs.com

Detalle del Log

Usuario: xifir33645@foboxs.com

Acción: UPDATE_INCIDENT

Fecha: 3/8/2025, 9:35:04 a. m.

ID de Incidente: 4

Título:

Activo Afectado: WebApp Server 01

Criticidad: Alta

Estado: En Progreso

Fuente: Firewall Logs

[Ver evidencia](#)

Exportar PDF

Exportar CSV

Cerrar

Ilustración 7 Detalle de un Log con Opciones de Exportación



Funcionalidad del Sistema

A continuación, se detallan los pasos realizados de la funcionalidad de nuestro sistema.

Usuario

Pantalla de Inicio de Sesión del Usuario

Explicación funcional: Este proceso garantiza que solo personal autorizado acceda al sistema. Además, permite la aplicación del control de acceso basado en roles (TRBAC), asegurando que cada usuario ingrese con los privilegios que le corresponden.

La figura 8 muestra el formulario de autenticación del **Sistema de Gestión de Incidentes de Seguridad (SGIS)**, donde el usuario debe ingresar su correo electrónico y contraseña.

Ilustración 8 Pantalla de Inicio de Sesión del Usuario

Registro de Usuario y Selección de Rol

Explicación funcional: Este flujo asegura que desde la creación de la cuenta se asignen correctamente los permisos, aplicando el principio de **mínimo privilegio** y reforzando la seguridad del sistema.

En la figura 9 se observa el formulario de creación de cuenta, que solicita correo electrónico, contraseña y la confirmación de esta, junto con la asignación de un rol específico: Usuario, Analista de Seguridad, Jefe de SOC, Auditor o Gerente de Riesgos.



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



SDIS - Sistema de Gestión de Incidentes

Crear Cuenta

Correo Electrónico *

juan.jima@gmail.com

Contraseña *

Confirmar Contraseña *

Rol

Usuario

Analista de Seguridad

Jefe de SOC

Auditor

Gerente de Riesgos

Ilustración 9 Registro de Usuario y Selección de Rol

Dashboard Principal del Usuario

Explicación funcional: El dashboard ofrece una visión general del estado de la seguridad, permitiendo al usuario acceder rápidamente a funciones como crear incidentes y revisar incidentes recientes, con la trazabilidad necesaria para la gestión segura.

La figura 10 presenta el tablero inicial del sistema tras un inicio de sesión exitoso. En él se muestran indicadores clave como: total de incidentes, incidentes abiertos, incidentes críticos y reportes del mes.

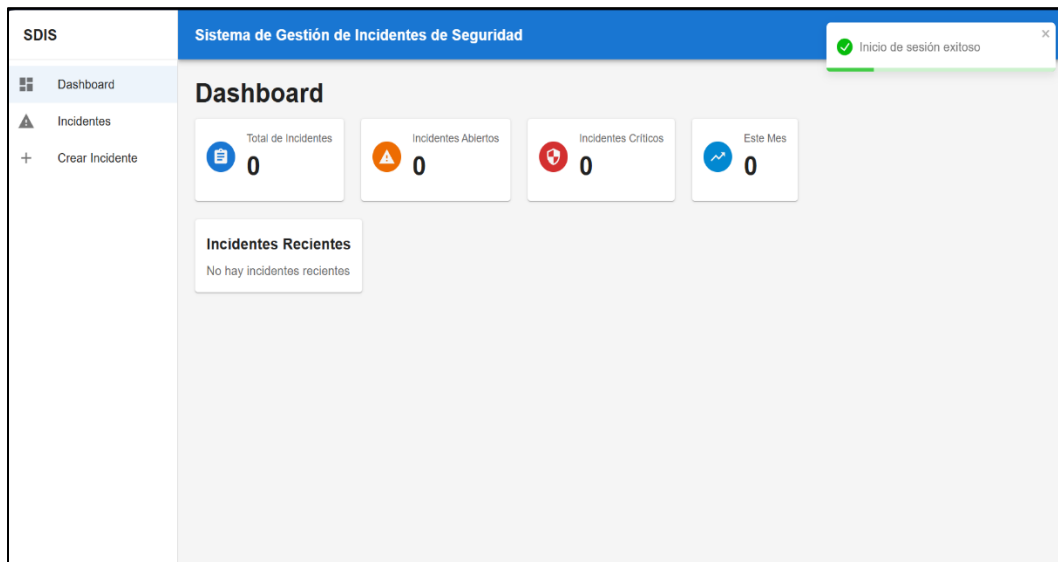


Ilustración 10 Dashboard Principal del Usuario



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



Formulario de Creación de Incidente

Explicación funcional: Esta funcionalidad permite al usuario documentar de manera estructurada los detalles de un evento de seguridad, garantizando la trazabilidad y facilitando el análisis posterior por parte de los analistas.

La figura 11 muestra la interfaz donde el usuario registra un nuevo incidente dentro del SGIS. Se incluyen campos como título, descripción, activo afectado, fuente del incidente, criticidad, clasificación y fecha de detección.

The screenshot shows the 'Crear Nuevo Incidente' (Create New Incident) form within the 'Sistema de Gestión de Incidentes de Seguridad' (SGIS) interface. The form is titled 'Crear Nuevo Incidente' and contains the following fields:

- Título del Incidente ***: Error en aplicacion
- Descripción ***: Detecté un error al intentar acceder a la aplicación SGIS a las 22:11 -05 del 03/08/2025, mostrando 'Acceso denegado'. Necesito asistencia para resolverlo.
- Activo Afectado ***: Servidor web
- Fuente del Incidente**: Usuario
- Criticidad ***: Media
- Clasificación ***: Evento
- Fecha y Hora de Detección**: 04/08/2025 03:09 a. m.

At the bottom right of the form are two buttons: 'Cancelar' and 'Crear Incidente'.

Ilustración 11 Formulario de Creación de Incidente

Gestión de Incidentes del Usuario

Explicación funcional: El módulo de gestión de incidentes facilita al usuario visualizar y dar seguimiento a los reportes realizados. Además, permite acceder al detalle de cada incidente y adjuntar evidencia adicional, contribuyendo a la continuidad en el manejo del caso.

En la figura 12 se presenta la lista de incidentes registrados por el usuario, mostrando información relevante como ID, título, activo afectado, criticidad, estado y fecha de creación.



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



SDIS	Sistema de Gestión de Incidentes de Seguridad						Usuario JJ
Dashboard	Gestión de Incidentes						Cambiar vista de rol + Crear Incidente
Incidentes	ID	Título	Activo Afectado	Criticidad	Estado	Fecha	Acciones
+ Crear Incidente	11	Error en aplicación	Servidor web	Medio	Nuevo	3 ago 2025	Ver Editar

Ilustración 12 Gestión de Incidentes del Usuario

Pantalla de Inicio de Sesión del Usuario

Explicación funcional: Esta actualización inmediata refuerza la transparencia y la confianza del usuario, mostrando en tiempo real que su incidente fue registrado correctamente y que será gestionado según el flujo definido en el sistema.

La figura 13 presenta el dashboard una vez creado un incidente. Se observa el aumento en el número total de incidentes y la aparición del nuevo caso en la sección de “Incidentes Recientes”.

SDIS	Sistema de Gestión de Incidentes de Seguridad				Usuario JJ
Dashboard	Dashboard				
Incidentes	Total de Incidentes	Incidentes Abiertos	Incidentes Críticos	Este Mes	
+ Crear Incidente	1	1	0	0	
	Incidentes Recientes				
	Error en aplicación Medio				
	Servidor web • hace unos segundos				
	Estado: Nuevo				

Ilustración 13 Dashboard Actualizado tras Registro de Incidente



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Analista de Seguridad

Creación de Cuenta para Analista de Seguridad

Explicación funcional: Este proceso garantiza que el acceso de los analistas quede definido desde la creación de la cuenta, permitiéndoles gestionar incidentes según el modelo TRBAC.

La figura 14 muestra el formulario de registro de un nuevo usuario con el rol **Analista de Seguridad**.

SDIS - Sistema de Gestión de Incidentes

Crear Cuenta

Correo Electrónico *
prueba@gmail.com

Contraseña *

Confirmar Contraseña *

Rol
Analista de Seguridad

Crear Cuenta

[¿Ya tienes una cuenta? Inicia sesión](#)

Ilustración 14 Creación de Cuenta para Analista de Seguridad

Dashboard del Analista de Seguridad

Explicación funcional: Permite al Analista obtener una visión global del estado actual de los incidentes, priorizando aquellos de mayor criticidad para su pronta atención.

En la figura 15 se observa el tablero principal para el Analista, con indicadores del total de incidentes, abiertos, críticos y recientes.



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE

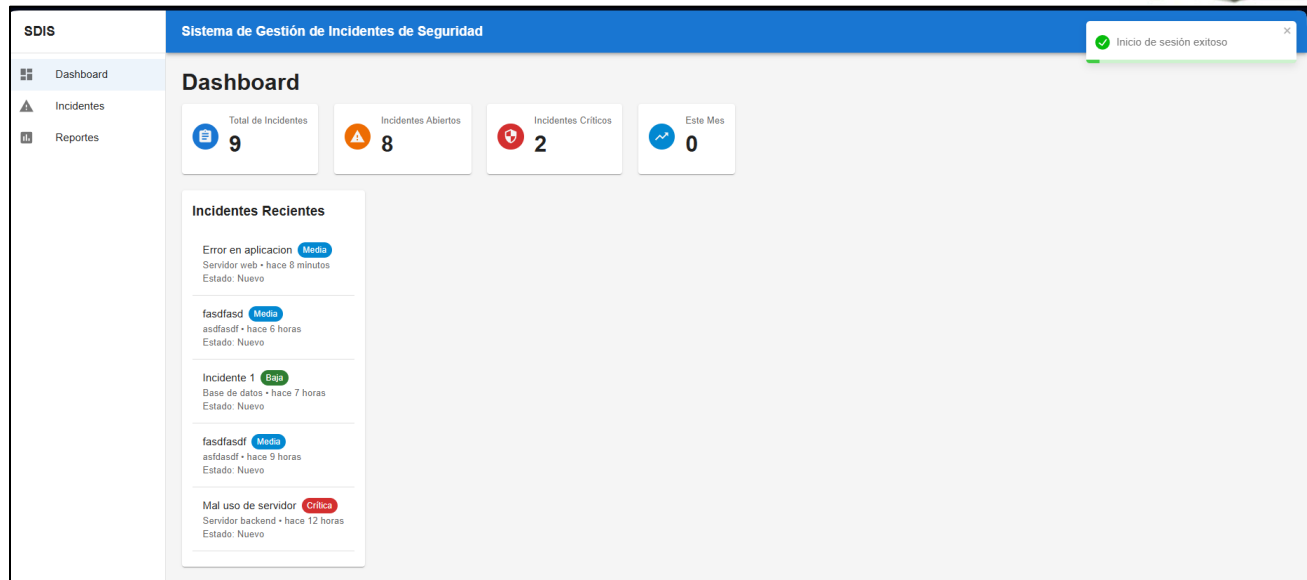


Ilustración 15 Dashboard del Analista de Seguridad

Gestión de Incidentes por el Analista

Explicación funcional: El analista puede acceder a incidentes reportados, clasificarlos, modificar su estado y tomar acciones de mitigación. Esto asegura la continuidad en la gestión del ciclo de vida del incidente.

La figura 16 presenta la lista de incidentes gestionada por el Analista de Seguridad, mostrando ID, título, activo afectado, criticidad, estado y fecha.

Sistema de Gestión de Incidentes de Seguridad						
ID	Título	Activo Afectado	Criticidad	Estado	Fecha	Acciones
3	Unauthorized Access Attempt Detected	WebApp Server 01	Media	En analisis	22 jul 2025	
4	Unauthorized Access Attempt Detected 2	WebApp Server 01	Alta	En Progreso	24 jul 2025	
7	Mal uso de servidor	Servidor backend	Crítica	Nuevo	3 ago 2025	
8	fasdfasdf	asfdasfd	Media	Nuevo	3 ago 2025	
9	Incidente 1	Base de datos	Baja	Nuevo	3 ago 2025	
10	fasdfasd	asfdasfd	Media	Nuevo	3 ago 2025	
5	hlaadd	fsfaltdads	Media	En Progreso	3 ago 2025	
6	holaasfd	fsfaltdads	Baja	Cerrado	3 ago 2025	
11	Error en aplicación	Servidor web	Media	Nuevo	3 ago 2025	

Ilustración 16 Gestión de Incidentes por el Analista



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



Reportes Mensuales de Incidentes

Explicación funcional: Esta funcionalidad permite generar análisis estadísticos sobre los incidentes registrados, facilitando la toma de decisiones y el cumplimiento de auditorías periódicas.

La figura 17 evidencia la sección de reportes mensuales, con métricas de distribución por criticidad y estado.

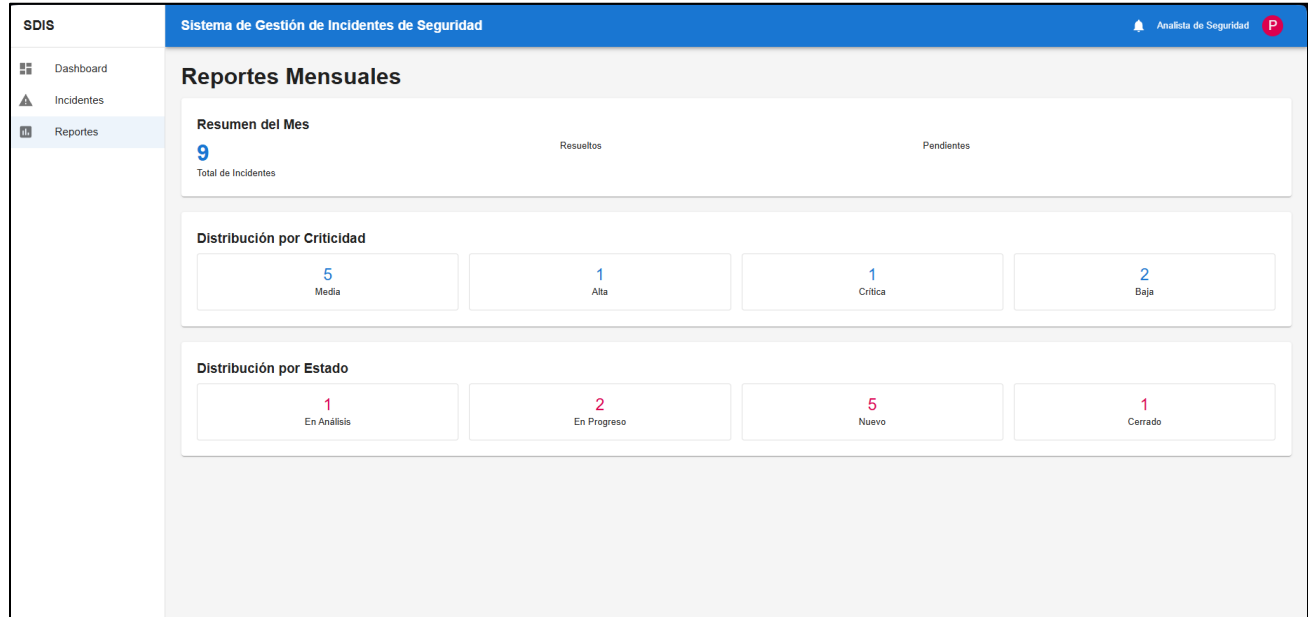


Ilustración 17 Reportes Mensuales de Incidentes

Detalles de un Incidente

Explicación funcional: El analista puede revisar en profundidad cada caso, verificar la evidencia adjunta y actualizar el estado o la clasificación del incidente, asegurando la trazabilidad y el registro completo del evento.

La figura 18 muestra la vista detallada de un incidente específico, incluyendo título, descripción, activo afectado, criticidad, estado, clasificación y evidencia asociada.



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE

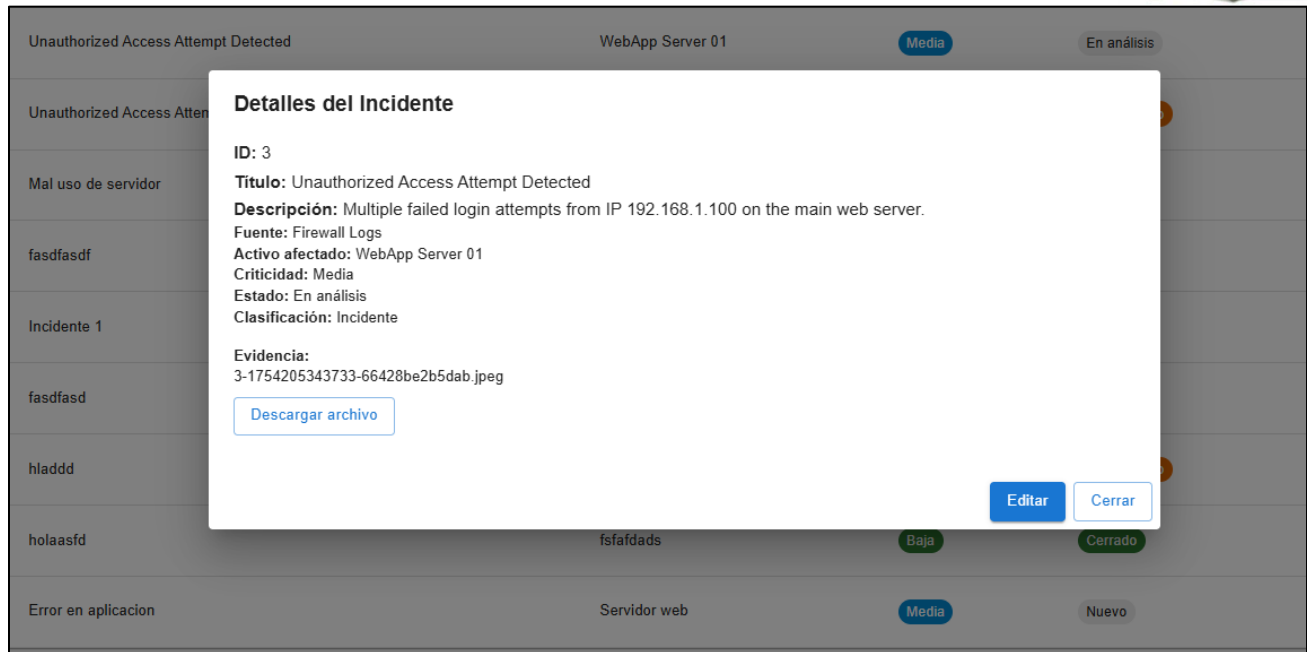


Ilustración 18 Detalles de un Incidente

Jefe de SOC

Creación de Cuenta para Jefe de SOC

Explicación funcional: El rol de Jefe de SOC requiere privilegios elevados para supervisar, autorizar cambios de estado y generar reportes estratégicos. La creación de una cuenta con este rol garantiza que el acceso quede restringido únicamente al personal designado con responsabilidades de liderazgo en el centro de operaciones de seguridad.

En la imagen 19 observa el formulario de registro de un nuevo usuario con rol *Jefe de SOC*, ingresando correo electrónico y credenciales seguras para su autenticación posterior.



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



SDIS - Sistema de Gestión de Incidentes

Crear Cuenta

Correo Electrónico *

Mateo@gmail.com

Contraseña *

Confirmar Contraseña *

Rol

Jefe de SOC

Crear Cuenta

[¿Ya tienes una cuenta? Inicia sesión](#)

Ilustración 19 Creación de Cuenta para Jefe de SOC

Dashboard del Jefe de SOC

Explicación funcional: El tablero del Jefe de SOC ofrece una visión consolidada de los incidentes y su distribución mensual por estado y criticidad, permitiéndole tomar decisiones estratégicas y priorizar recursos en función de la severidad de los eventos.

En la figura 20 se visualizan indicadores de incidentes totales, abiertos y críticos, además de un resumen mensual con la cantidad de incidentes por estado (en análisis, en progreso, nuevos, cerrados) y por nivel de criticidad.

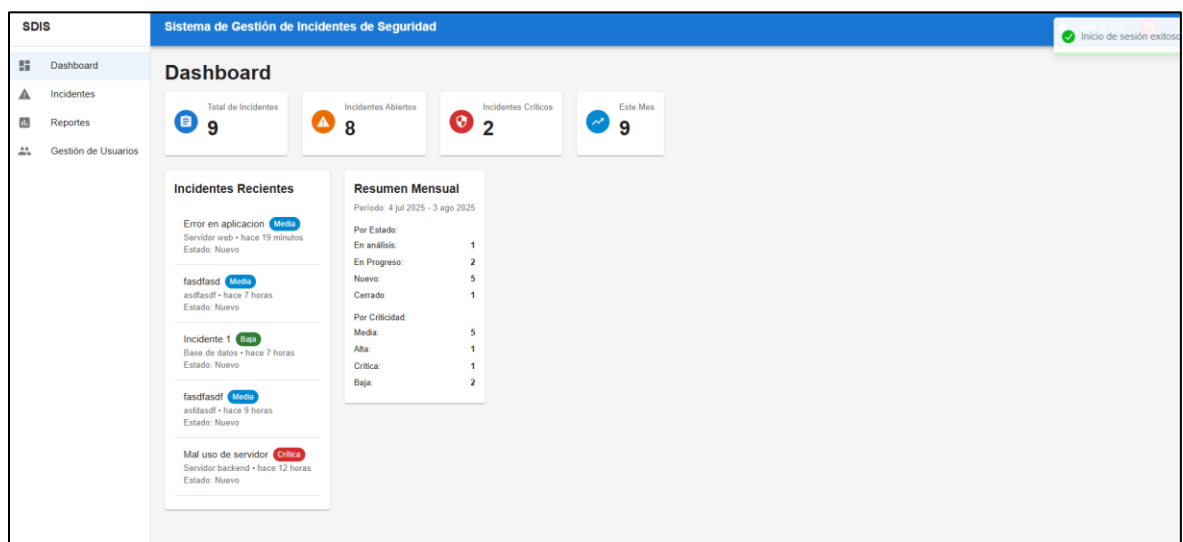


Ilustración 20 Dashboard del Jefe de SOC



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



Gestión de Incidentes por el Jefe de SOC

Explicación funcional: El Jefe de SOC puede acceder al listado completo de incidentes registrados, supervisar su avance y validar el correcto manejo por parte de los analistas, autorizando los cambios de estado cuando corresponde.

En la figura 21 se muestra una tabla con incidentes identificados por ID, título, activo afectado, criticidad, estado actual y fecha, junto con acciones para visualizar o editar la información del caso.

SDIS	Sistema de Gestión de Incidentes de Seguridad						Jefe de SOC
Dashboard	Gestión de Incidentes						Cambiar vista de rol
Incidentes	ID	Título	Activo Afectado	Criticidad	Estado	Fecha	Acciones
Reportes	3	Unauthorized Access Attempt Detected	WebApp Server 01	Media	En análisis	22 jul 2025	
Gestión de Usuarios	4	Unauthorized Access Attempt Detected 2	WebApp Server 01	Alta	En Progreso	24 jul 2025	
	7	Mal uso de servidor	Servidor backend	Crítica	Nuevo	3 ago 2025	
	8	fasdfasdf	asdfasdf	Media	Nuevo	3 ago 2025	
	9	Incidente 1	Base de datos	Baja	Nuevo	3 ago 2025	
	10	fasdfasd	asdfasdf	Media	Nuevo	3 ago 2025	
	5	hladdd	fsfaldads	Media	En Progreso	3 ago 2025	
	6	holaasfd	fsfaldads	Baja	Cerrado	3 ago 2025	
	11	Error en aplicación	Servidor web	Media	Nuevo	3 ago 2025	

Ilustración 21 Gestión de Incidentes por el Jefe de SOC

Reportes Mensuales Generados por el Jefe de SOC

Explicación funcional: Esta sección permite al Jefe de SOC generar reportes mensuales con métricas clave, fundamentales para auditorías internas y presentación a la gerencia de riesgos.

En la figura 22 se presentan métricas de distribución de incidentes por criticidad y estado, con un resumen de resultados y pendientes del periodo.



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE

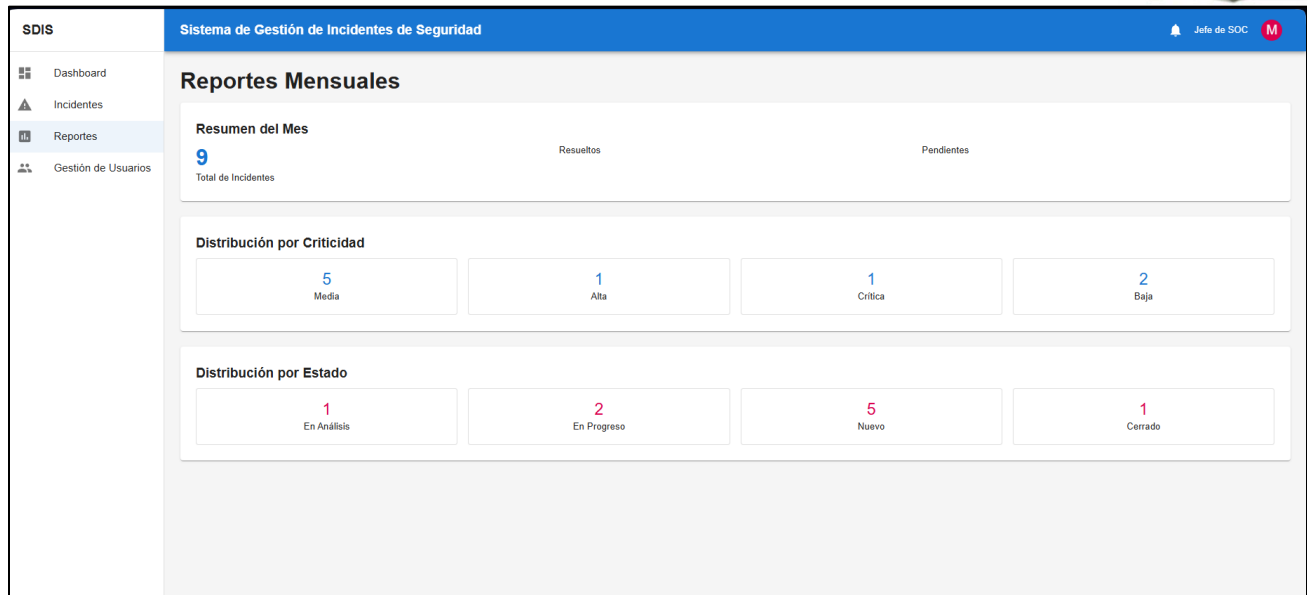


Ilustración 22 Reportes Mensuales Generados por el Jefe de SOC

Gestión de Usuarios desde el Perfil Jefe de SOC

Explicación funcional: Una de las facultades exclusivas del Jefe de SOC es la administración de usuarios, lo que incluye la visualización de cuentas, roles asignados y su estado de actividad, reforzando el control de accesos.

En la figura 23 se observa la tabla de gestión de usuarios, listando el identificador único, correo electrónico, rol asignado y estado de cada cuenta dentro del sistema.

SDIS

Sistema de Gestión de Incidentes de Seguridad

Jefe de SOC

M

Dashboard

Incidentes

Reportes

Gestión de Usuarios

Gestión de Usuarios

ID	Email	Rol	Estado
ec97dca8-aecf-4a6f-971e-c223c722d23c	mateo@gmail.com	Jefe de SOC	Activo
dtd89044-bfc9-448b-8c42-fd58aa7e6773	prueba@gmail.com	Analista de Seguridad	Activo
b3684dcd-519c-4668-9908-4e5b50bec450	datemeh239@foboxs.com	Analista de Seguridad	Activo
11987463-504e-4781-a5aa-8dce4508d11	juan.jima@gmail.com	Usuario	Activo
4ae40b02-e311-4810-a91e-8fb0d48a2533	a@a.com	Gerente de Riesgos	Activo
bd68a9b1-e600-430e-b058-cb12598ad383	domase6783@foboxs.com	Auditor	Activo
f6e9a8d8-664f-4489-89cc-0575a11c59d2	rakajig228@hostbyt.com	Auditor	Activo
61fa1205-d431-46ee-b5b7-3660ed70b12a	xerilop978@foboxs.com	Auditor	Activo
367d316c-d675-4467-bb8c-e92a22b55803	joha@gmail.com	Auditor	Activo
626fd295-4582-43ad-9e01-a8527c897105	shir@gmail.com	Usuario	Activo
25cd2b93-50d1-4c26-8680-078a4131969f	kegak58795@hostbyt.com	Auditor	Activo
2d6d937f-108d-4e60-91b1-32aa75d4aa95	pasebat568@foboxs.com	Gerente de Riesgos	Activo
d54800ec-fa08-4675-a40a-7ae7d649896a	seyeyin587@hostbyt.com	Usuario	Activo
b8352c04-ab2b-46a3-b84a-b118996b1adc	toyhiv522@foboxs.com	Usuario	Activo

Ilustración 23 Gestión de Usuarios desde el Perfil Jefe de SOC



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Auditor

Creación de cuenta del Auditor

Explicación funcional: El auditor se registra en el sistema seleccionando el rol correspondiente. Su cuenta le permitirá acceder a la plataforma con privilegios de solo lectura y verificación, garantizando la independencia en sus revisiones.

La figura 24 muestra la interfaz de creación de cuenta, donde se ingresan correo, contraseña y confirmación, y se selecciona el rol Auditor.

SDIS - Sistema de Gestión de Incidentes

Crear Cuenta

Correo Electrónico *
Maria@gmail.com

Contraseña *

Confirmar Contraseña *

Rol
Auditor

Crear Cuenta

[¿Ya tienes una cuenta? Inicia sesión](#)

Ilustración 24 Creación de cuenta del Auditor

Dashboard del Auditor

Explicación funcional: Una vez que inicia sesión, el auditor accede al dashboard principal. Desde aquí puede visualizar un resumen general de los incidentes registrados, diferenciando los abiertos, críticos y recientes. Esto le permite tener una visión global del estado de la seguridad y evaluar el nivel de riesgo actual de la organización.

La figura 25 muestra el dashboard con estadísticas: total de incidentes, incidentes abiertos, críticos y recientes, con detalles como título, criticidad, activo afectado y estado.



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE

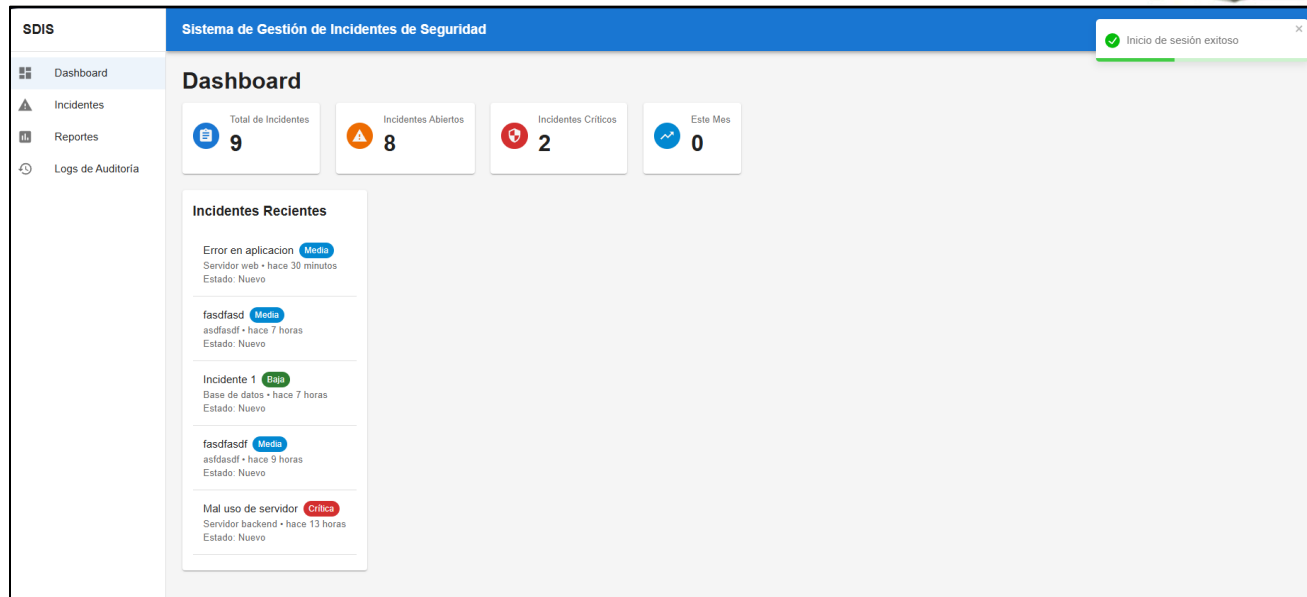


Ilustración 25 Dashboard del Auditor

Gestión de Incidentes por parte del Auditor

Explicación funcional: El auditor revisa la lista completa de incidentes registrados en el sistema. Puede observar el detalle de cada incidente, incluyendo título, activo afectado, criticidad, estado y fecha. Su función principal es validar la integridad de la información y garantizar que los registros estén completos, consistentes y trazables.

La figura 26 muestra la sección de Gestión de Incidentes, con una tabla que contiene múltiples registros de incidentes, mostrando criticidad y estado actual.

ID	Título	Activo Afectado	Criticidad	Estado	Fecha	Acciones
3	Unauthorized Access Attempt Detected	WebApp Server 01	Medio	En análisis	22 jul 2025	
4	Unauthorized Access Attempt Detected 2	WebApp Server 01	Alta	En Progress	24 jul 2025	
7	Mal uso de servidor	Servidor backend	Crítica	Nuevo	3 ago 2025	
8	fasdfasf	asfdasf	Medio	Nuevo	3 ago 2025	
9	Incidente 1	Base de datos	Baja	Nuevo	3 ago 2025	
10	fasdfasf	asfdasf	Medio	Nuevo	3 ago 2025	
5	hladd	fsafds	Medio	En Progress	3 ago 2025	
6	holaasf	fsafds	Baja	Cerrado	3 ago 2025	
11	Error en aplicacion	Servidor web	Medio	Nuevo	3 ago 2025	

Ilustración 26 Gestión de Incidentes por parte del Auditor



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



Subida y revisión de evidencia

Explicación funcional: El sistema permite que el auditor verifique las evidencias relacionadas con los incidentes, asegurando que cada registro esté respaldado por documentación adecuada. Aunque el auditor no tiene permisos de modificación, puede visualizar o descargar la evidencia para fines de validación y control.

La figura 27 muestra la ventana para subir o visualizar evidencia de un incidente, con la opción de seleccionar archivos relacionados al evento reportado.

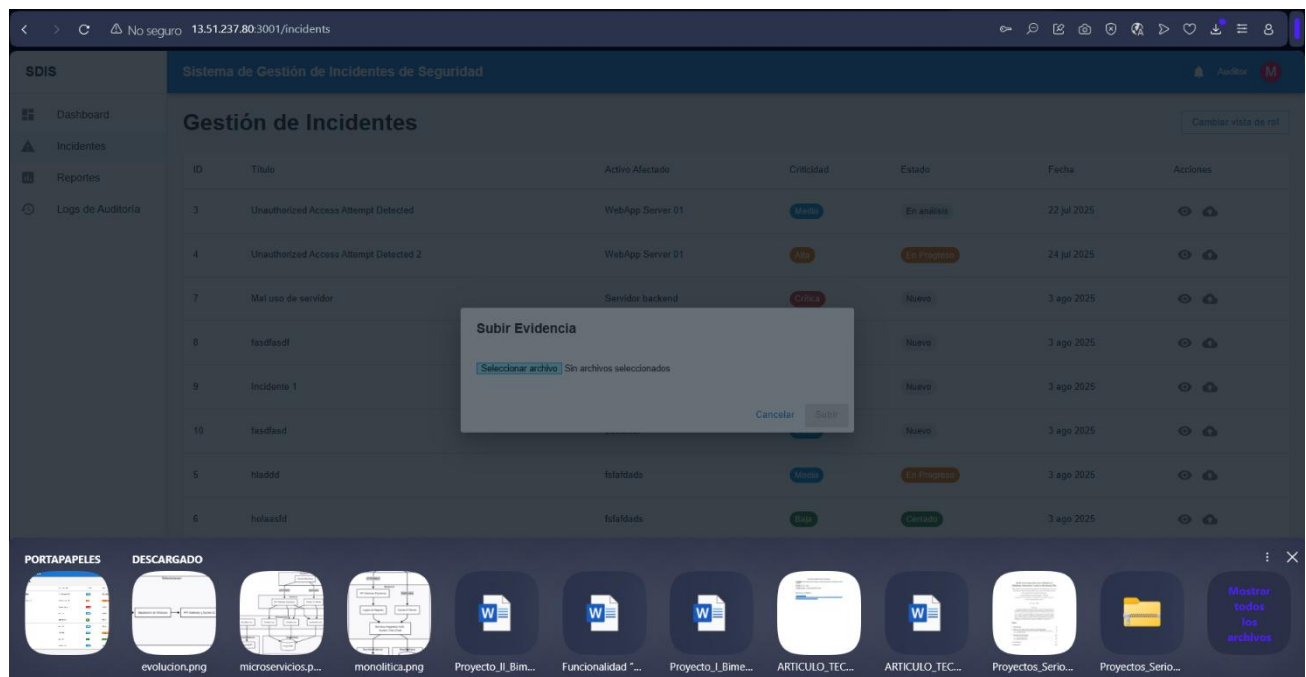


Ilustración 27 Subida y revisión de evidencia

Detalle de un incidente

Explicación funcional: El auditor accede a la vista detallada de un incidente, lo que le permite revisar la descripción, fuente, activo afectado, criticidad, estado, clasificación y evidencia adjunta. De esta manera, valida que el registro cumpla con los parámetros establecidos en las auditorías internas y externas.

La figura 28 muestra una ventana emergente con el detalle completo del incidente, incluyendo ID, título, descripción, fuente, activo afectado, criticidad, estado y enlace para descargar la evidencia.



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



SDIS	Sistema de Gestión de Incidentes de Seguridad						
Dashboard	Gestión de Incidentes						
Incidentes							
Reportes							
Logs de Auditoría							
ID	Título	Activo Afectado	Criticidad	Estado	Fecha	Acciones	
3	Unauthorized Access Attempt Detected	WebApp Server 01	Media	En análisis	22 jul 2025		
4	Unauthorized Access Attempt				24 jul 2025		
7	Mal uso de servidor				3 ago 2025		
8	fasdfasdf				3 ago 2025		
9	Incidente 1				3 ago 2025		
10	fasdfasdf				3 ago 2025		
5	hiaddd				3 ago 2025		
6	holaasfd	Infraestructura	Baja	Cerrado	3 ago 2025		
11	Error en aplicación	Servidor web	Media	Nuevo	3 ago 2025		

Ilustración 28 Detalle de un incidente

Reportes mensuales del Auditor

Explicación funcional: La sección de reportes mensuales brinda al auditor un análisis de la distribución de incidentes por criticidad y estado. Esta información permite identificar tendencias, medir la efectividad de los controles aplicados y evaluar el desempeño de la gestión de seguridad en un período específico.

La figura 29 muestra un reporte mensual con el total de incidentes y su distribución clasificada por criticidad (Media, Alta, Crítica, Baja) y por estado (En Análisis, En Progreso, Nuevo, Cerrado).

SDIS

Dashboard

Incidentes

Reportes

Logs de Auditoria

Sistema de Gestión de Incidentes de Seguridad

Auditor

M

Reportes Mensuales

Resumen del Mes

9

Total de Incidentes

Resueltos

Pendientes

Distribución por Criticidad

5

Media

1

Alta

1

Crítica

2

Baja

Distribución por Estado

1

En Análisis

2

En Progreso

5

Nuevo

1

Cerrado

Ilustración 29 Reportes mensuales del Auditor



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



Logs de Auditoría

Explicación funcional: El módulo de Logs de Auditoría permite al auditor supervisar todas las acciones realizadas en el sistema, como la creación y actualización de incidentes, detallando fecha, hora y usuario responsable. Esto asegura trazabilidad, transparencia y cumplimiento con las normas de auditoría de seguridad.

La figura 30 muestra una tabla de historial de eventos donde se registran acciones de usuarios (ejemplo: CREATE_INCIDENT, UPDATE_INCIDENT), junto con fecha, hora y correo electrónico del actor.

The screenshot shows the 'SDIS Sistema de Gestión de Incidentes de Seguridad' interface. On the left is a sidebar with navigation links: Dashboard, Incidentes, Reportes, and Logs de Auditoría (selected). The main area is titled 'Historial de Eventos (Logs)' and contains a table of events. Above the table are filters for 'Usuario', 'Desde' (dd/mm/aaaa), and 'Hasta' (dd/mm/aaaa), along with a 'Limpiar' button.

Usuario	Acción	Fecha y Hora
Juan.jima@gmail.com	CREATE_INCIDENT	3/8/2025, 10:13:02 p.m.
datemah239@foboxs.com	UPDATE_INCIDENT	3/8/2025, 9:58:05 p.m.
xerilop978@foboxs.com	UPDATE_INCIDENT	3/8/2025, 8:02:11 p.m.
xerilop978@foboxs.com	UPDATE_INCIDENT	3/8/2025, 8:02:08 p.m.
tewat63808@hostbyt.com	CREATE_INCIDENT	3/8/2025, 3:25:59 p.m.
shirley@gmail.com	CREATE_INCIDENT	3/8/2025, 3:13:52 p.m.
gsox95479@hostbyt.com	CREATE_INCIDENT	3/8/2025, 1:19:56 p.m.
woxi20034@foboxs.com	CREATE_INCIDENT	3/8/2025, 9:37:48 a.m.
xifr33645@foboxs.com	UPDATE_INCIDENT	3/8/2025, 9:35:04 a.m.
xifr33645@foboxs.com	UPDATE_INCIDENT	3/8/2025, 9:34:59 a.m.
xifr33645@foboxs.com	UPDATE_INCIDENT	3/8/2025, 9:34:40 a.m.
xifr33645@foboxs.com	CREATE_INCIDENT	3/8/2025, 1:51:38 a.m.
teriro9765@foboxs.com	CREATE_INCIDENT	3/8/2025, 12:11:18 a.m.

Ilustración 30 Logs de Auditoría

Gerente de Riesgos

Creación de cuenta como Gerente de Riesgos

Explicación funcional: El Gerente de Riesgos se registra en el sistema para obtener credenciales y así acceder a las funciones ejecutivas, enfocadas en supervisar la seguridad organizacional y generar reportes estratégicos.

Lo que muestra la figura 31 es un formulario de creación de cuenta en el que se ingresa el correo, contraseña y se selecciona el rol Gerente de Riesgos.



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



SDIS - Sistema de Gestión de Incidentes

Crear Cuenta

Correo Electrónico *

Michelle@gmail.com

Contraseña *

.....

Confirmar Contraseña *

.....

Rol

Gerente de Riesgos

Crear Cuenta

[¿Ya tienes una cuenta? Inicia sesión](#)

Ilustración 31 Creación de cuenta como Gerente de Riesgos

Dashboard del Gerente de Riesgos

Explicación funcional: El Gerente accede a un tablero ejecutivo con indicadores globales de los incidentes, lo que le permite evaluar el panorama general de la seguridad y el desempeño de la gestión de riesgos.

Lo que muestra la figura 32 el dashboard con tarjetas que indican el total de incidentes, abiertos, críticos y del mes, junto a un resumen mensual por estado y criticidad.

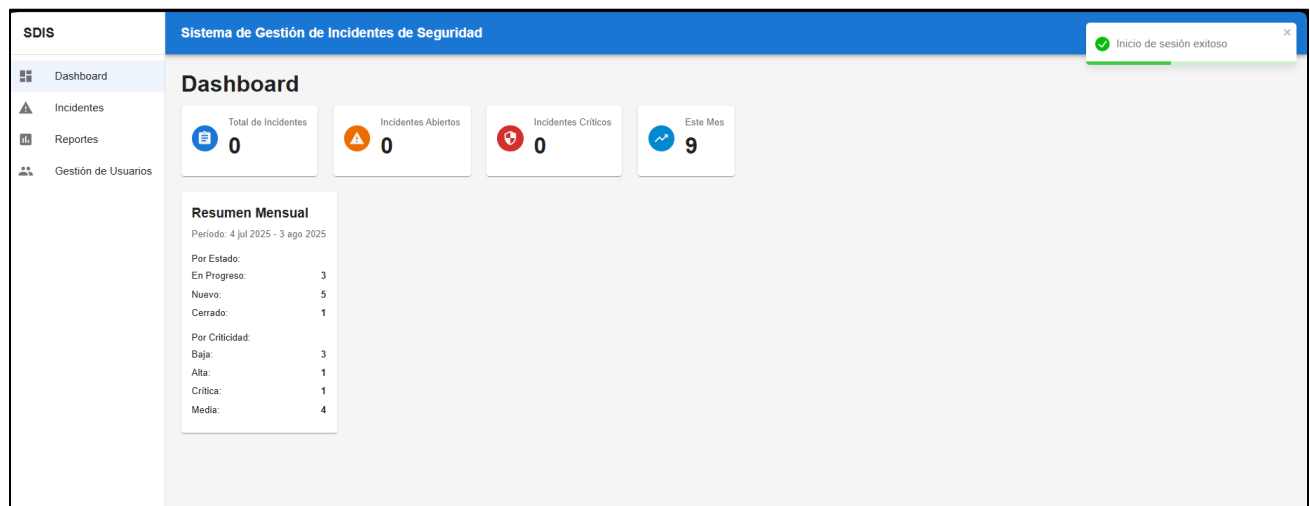


Ilustración 32 Dashboard del Gerente de Riesgos



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



Gestión de Incidentes

Explicación funcional: El Gerente revisa la lista de incidentes para analizar su distribución y estado actual. También tiene la opción de exportar la información en PDF o CSV, facilitando la elaboración de reportes para juntas directivas o auditorías.

Lo que muestra la figura 33 es una tabla con incidentes que incluye ID, título, activo afectado, criticidad, estado, fecha y acciones, junto con botones de exportación de reportes.

SDIS	Sistema de Gestión de Incidentes de Seguridad						Gerente de Riesgos
Dashboard	Gestión de Incidentes						Cambiar vista de rol Exportar PDF Exportar CSV
Incidentes	ID	Título	Activo Afectado	Criticidad	Estado	Fecha	Acciones
Reportes	3	Unauthorized Access Attempt Detected	WebApp Server 01	Baja	En Progreso	22 jul 2025	O
Gestión de Usuarios	4	Unauthorized Access Attempt Detected 2	WebApp Server 01	Alta	En Progreso	24 jul 2025	O
	7	Mal uso de servidor	Servidor backend	Crítica	Nuevo	3 ago 2025	O
	8	fasdfasdf	asfdasdf	Medio	Nuevo	3 ago 2025	O
	9	Incidente 1	Base de datos	Baja	Nuevo	3 ago 2025	O
	10	fasdfasd	asfdasdf	Medio	Nuevo	3 ago 2025	O
	5	hladd	fsfadsd	Medio	En Progreso	3 ago 2025	O
	6	holaasfd	fsfadsd	Baja	Cerrado	3 ago 2025	O
	11	Error en aplicación	Servidor web	Medio	Nuevo	3 ago 2025	O

Ilustración 33 Gestión de Incidentes

Exportación de Reportes

Explicación funcional: El Gerente genera reportes descargables para respaldar la documentación y análisis de la gestión de incidentes, lo que garantiza la trazabilidad y evidencia en procesos de auditoría.

Lo que muestra la figura 34 es la ventana de descargas con archivos generados del sistema en formatos Excel (CSV) y PDF, que contienen el detalle de incidentes.



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



ID	Título	Activo Afectado	Criticidad	Estado	Fecha	Acciones
3	Unauthorized Access Attempt Detected	WebApp Server 01	Baja	En Progreso	22 jul 2025	
4	Unauthorized Access Attempt Detected 2	WebApp Server 01	Alta	En Progreso	24 jul 2025	
7	Mal uso de servidor	Servidor backend	Crítica	Nuevo	3 ago 2025	
8	fasdfasdf	asfdasdf	Media	Nuevo	3 ago 2025	
9	Incidente 1	Base de datos	Baja	Nuevo	3 ago 2025	
10	fasdfasd	asfdasdf	Media	Nuevo	3 ago 2025	

Nombre	Fecha de modificación	Tipo	Tamaño
incidents_export	03/08/2025 10:56 p. m.	Microsoft Excel Co...	1 KB
reporte_incidentes	03/08/2025 10:56 p. m.	Microsoft Edge PD...	3 KB

Ilustración 34 Exportación de Reportes

Reportes Mensuales

Explicación funcional: El Gerente accede a un informe mensual para evaluar tendencias, criticidad y estados de los incidentes, facilitando la toma de decisiones estratégicas y la definición de planes de mitigación.

Lo que muestra la figura 35 es el reporte con la distribución de incidentes por criticidad (baja, media, alta, crítica) y por estado (en progreso, nuevo, cerrado).

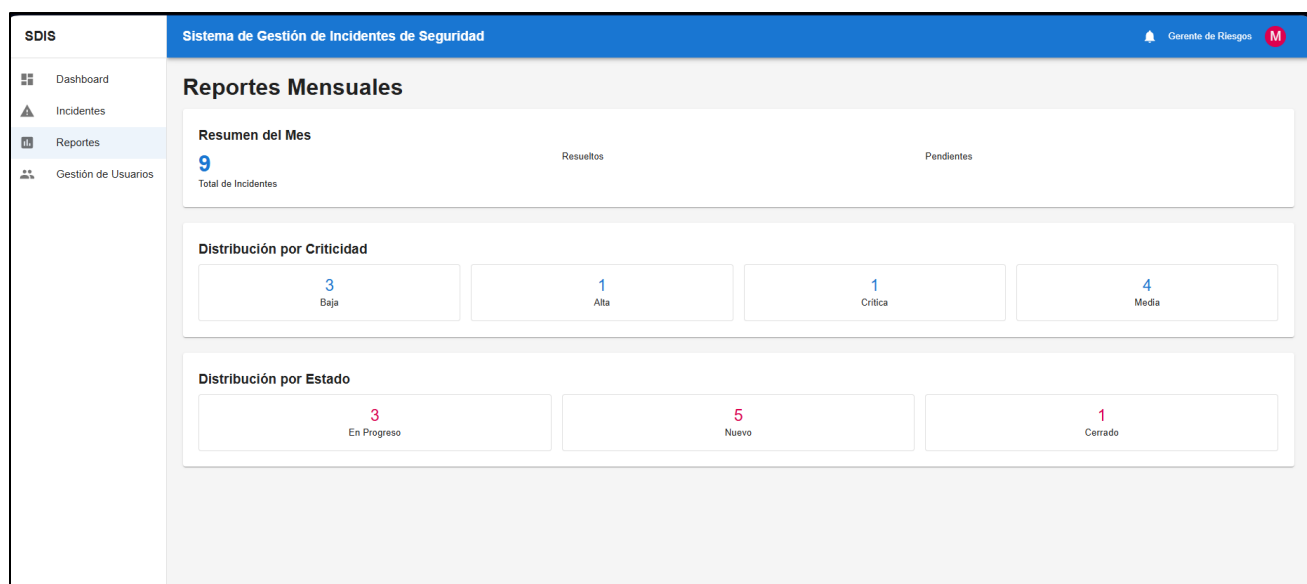


Ilustración 35 Reportes Mensuales



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



Gestión de Usuarios

Explicación funcional: El Gerente supervisa la correcta asignación de roles y estados de los usuarios registrados, asegurando el control de accesos y la coherencia con la política de seguridad.

Lo que muestra la figura 36 es una lista de usuarios con ID, correo electrónico, rol y estado, que permite verificar quiénes tienen acceso y en qué condición se encuentran.

SDIS	Sistema de Gestión de Incidentes de Seguridad			Gerente de Riesgos
Dashboard	Gestión de Usuarios			
Incidentes				
Reportes				
Gestión de Usuarios				
ID	Email	Rol	Estado	
f18028a1-b8c5-48ff-92e5-4a1792cfd9fc	michelle@gmail.com	Gerente de Riesgos	Activo	
aec33bfc-5ac3-42d5-b76b-d5ca1142b74a	dicetj837@foboxs.com	Usuario	Activo	
2195071a-b675-4c61-9f77-b2d8370fa529	maria@gmail.com	Auditor	Activo	
ec97dca8-aecf-4a6f-971e-c223c722d23c	mateo@gmail.com	Jefe de SOC	Activo	
dfd89044-bfc9-448b-8c42-fd58aa7e67f3	prueba@gmail.com	Analista de Seguridad	Activo	
b3684dcd-519c-4668-9908-4e5b50bec450	datemeh239@foboxs.com	Analista de Seguridad	Activo	
11987463-504e-4781-a5aa-8f6ce4508d11	Juan.jima@gmail.com	Usuario	Activo	
4ae40bf2-e311-4810-a91e-8fb0d48a2533	a@a.com	Gerente de Riesgos	Activo	
bd68a9b1-e600-430e-b058-cb12598ad383	domase6783@foboxs.com	Auditor	Activo	
f6e9a8d8-664f-4489-89cc-0575a11c59d2	rakajg228@hostbyt.com	Auditor	Activo	
61fa1205-d431-46ee-b5b7-3660ed70b12a	xerlop978@foboxs.com	Auditor	Activo	
367d316c-d675-4467-bb8c-e92a22b55803	joha@gmail.com	Auditor	Activo	
626fd295-4582-43ad-9e01-a8527c897105	shir@gmail.com	Usuario	Activo	

Ilustración 36 Gestión de Usuarios



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE



Configuración MFA

Configuración inicial del MFA

Explicación funcional: En esta primera etapa, el sistema invita al usuario a activar la Autenticación de Doble Factor. Esta medida añade una capa adicional de seguridad para evitar accesos no autorizados, incluso si las credenciales principales son comprometidas. El usuario deberá contar con una aplicación de autenticación (como Google Authenticator o Authy) para generar códigos dinámicos.

Lo que muestra la figura 37 es la interfaz para el paso de Configurar MFA, indicando que el usuario debe iniciar la configuración para continuar. Se muestran las opciones de "Iniciar Configuración" o posponerla ("Configurar más tarde").

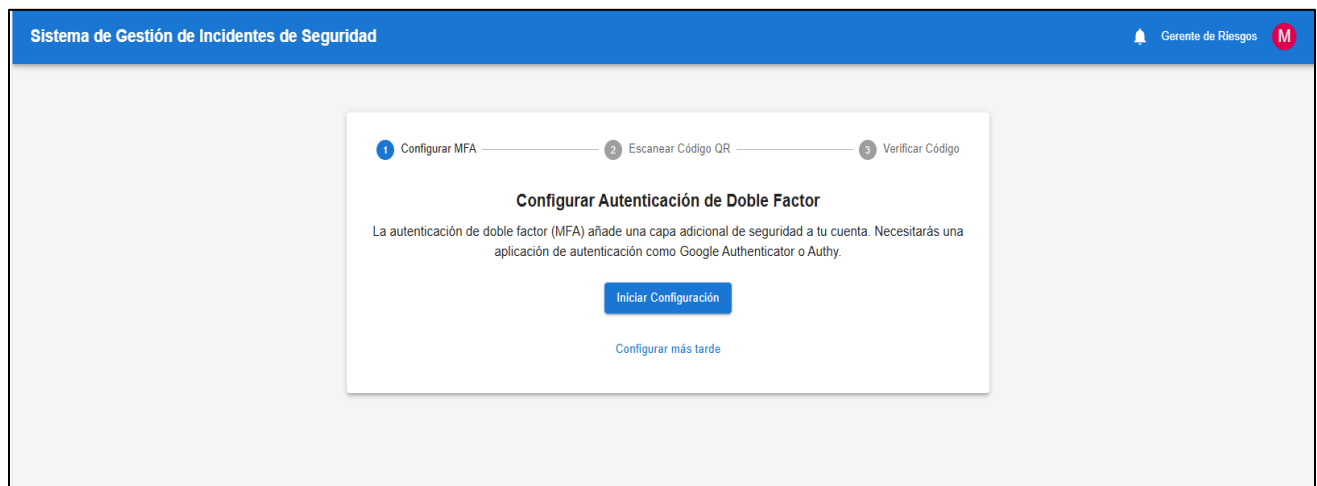


Ilustración 37 Configuración inicial del MFA

Escaneo del Código QR

Explicación funcional: En este paso, el sistema genera un código QR único asociado a la cuenta del usuario. El usuario debe escanearlo desde su aplicación de autenticación para vincularla con el sistema. Una vez realizado el escaneo, la aplicación comenzará a generar códigos de verificación temporales de 6 dígitos, válidos por 30 segundos.

Lo que muestra la figura 38 es la pantalla indica el paso Escanear Código QR, mostrando el código a ser leído por la aplicación de autenticación. Además, se incluye un campo para ingresar el código de verificación generado por la app.



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE




Sistema de Gestión de Incidentes de Seguridad

Gerente de Riesgos

1 Configurar MFA 2 Escanear Código QR 3 Verificar Código

Escanear el Código QR

Abre tu aplicación de autenticación y escanea el siguiente código QR:



data:image/svg+xml;utf-8,

Una vez escaneado, tu aplicación generará códigos de 6 dígitos cada 30 segundos.

Código de Verificación (6 dígitos) *

Verificar Código

[Configurar más tarde](#)

Ilustración 38 Escaneo del Código QR

Generación de clave secreta y validación

Explicación funcional: Luego del escaneo, se genera una clave secreta única vinculada al usuario. Esta clave se almacena de forma segura en la aplicación autenticadora y permite crear códigos dinámicos (TOTP). El usuario debe ingresar uno de estos códigos en el campo de verificación para confirmar la configuración del MFA.

Lo que muestra en la figura 39 es la cadena `otpauth://totp/...`, que contiene parámetros como el correo electrónico del usuario, el algoritmo (SHA1), la longitud del código (6 dígitos), el período de validez (30 segundos) y la clave secreta. Esto confirma que la aplicación ya está generando los códigos necesarios para la autenticación.



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SOFTWARE

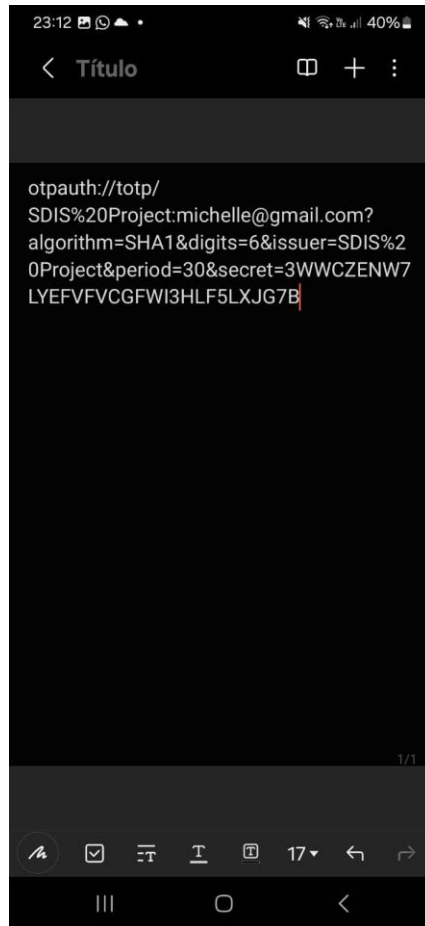


Ilustración 39 Generación de clave secreta y validación



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Conclusiones y Recomendaciones

Conclusiones

- La implementación del SDIS permitió establecer un sistema estructurado para la gestión de incidentes de seguridad, garantizando la trazabilidad, clasificación y seguimiento de cada evento reportado.
- La asignación de roles específicos (Usuario, Analista de Seguridad, Auditor, Jefe de SOC y Gerente de Riesgos) asegura la correcta segregación de funciones y la aplicación de controles de acceso basados en el principio de menor privilegio.
- La funcionalidad de reportes mensuales proporciona una visión clara de la criticidad y estado de los incidentes, facilitando la toma de decisiones estratégicas y operativas para la mitigación de riesgos.
- La inclusión de la opción para adjuntar y descargar evidencias en cada incidente fortalece la capacidad de análisis y documentación, apoyando la auditoría forense y el cumplimiento normativo.
- La activación de la Autenticación de Doble Factor (MFA) incrementa significativamente el nivel de seguridad del sistema, reduciendo el riesgo de accesos no autorizados y cumpliendo con estándares internacionales de ciberseguridad.
- El módulo de logs de auditoría permite monitorear todas las acciones realizadas por los usuarios, aportando transparencia y asegurando la detección temprana de actividades anómalas.

Recomendaciones

- Brindar entrenamientos periódicos a todos los roles del sistema para garantizar el uso correcto de las funcionalidades y la adecuada gestión de incidentes.
- Establecer reglas claras de clasificación, priorización y escalamiento de incidentes, alineadas con las normativas ISO/IEC 27001 y 27005.
- Auditar regularmente la asignación de roles para evitar privilegios innecesarios o caducados, reforzando el control de acceso.
- Garantizar que todos los usuarios activen la autenticación de doble factor y evaluar la adopción de métodos adicionales, como llaves de seguridad físicas (FIDO2).
- Implementar alertas automáticas en tiempo real para incidentes críticos, mejorando la capacidad de respuesta del equipo de seguridad.
- Establecer mecanismos de respaldo de la base de datos y pruebas periódicas de recuperación ante desastres, para garantizar la disponibilidad del sistema.



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



- Considerar la integración del SDIS con una solución de Gestión de Información y Eventos de Seguridad (SIEM) para mejorar el análisis correlacional de incidentes.

Referencias

- [1] Microsoft, "Microsoft Security Development Lifecycle (SDL)," 2024. [Online]. Available: <https://learn.microsoft.com/en-us/compliance/assurance/assurance-microsoft-security-development-lifecycle>
- [2] Security Compass, "Security Development Lifecycle (SDL) & Best Practices," 2025. [Online]. Available: <https://www.securitycompass.com/blog/security-development-lifecycle-best-practices/>
- [3] Tenacy, "What is ISO 27035?," [Online]. Available: <https://www.tenacy.io/en/resources/iso-27035/>
- [4] J. Vargas, "Manejo de Incidentes de Seguridad con ISO 27035 - 2023," LinkedIn, 2024. [Online]. Available: <https://www.linkedin.com/pulse/manejo-de-incidentes-seguridad-con-iso-27035-2023-vargas>
- [5] Beagle Security, "Understanding OWASP top 10: How to use it as a standard," LinkedIn, 2024. [Online]. Available: <https://www.linkedin.com/pulse/understanding-owasp-top-10-how-use-standard-beaglesecurity-4wz3c>
- [6] Sprinto, "List of NIST SP 800-53 Controls Families," 2024. [Online]. Available: <https://sprinto.com/blog/nist-800-53-control/>
- [7] IriusRisk, "Threat Modeling Methodology: STRIDE," 2023. [Online]. Available: <https://www.iriusrisk.com/resources-blog/threat-modeling-methodology-stride>



ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS
INGENIERÍA EN SOFTWARE



Anexos

- **Anexo A**
Matriz RTM para seguimiento de requerimientos:
[Requirements-Traceability-Matrix-ProyectoIB GrupoC.xlsx](#)
- **Anexo B**
Matriz Analisis de riesgo:
[Risk-Analysis ProyectoIB GrupoC.xlsx](#)
- **Anexo C**
AttackTree

[attacktree ProyectoIB GrupoC.json](#)
- **Anexo D**
Modelado de amenazas
[Informe.htm](#)
- **Anexo E**
Repositorio de GitHub
<https://github.com/eddyarias/ProyectoDSSGrupoC.git>