UNIVERSIDAD PANAMERICANA

Facultad de Ingeniería y Ciencias Aplicadas

Ingeniería en Sistemas y Tecnologías de la Información y la Comunicación

Sistema informático para el control de activos de tecnología y gestión de incidentes para la dirección de análisis criminal del ministerio público

(Tesis de Licenciatura)

Roberto Guillermo Lavagnino Rodríguez

Guatemala de la Asunción, marzo 2020.

Sistema informático para el control de activos de tecnología y gestión de incidentes para la dirección de análisis criminal del ministerio público

(Tesis de Licenciatura)

Roberto Guillermo Lavagnino Rodríguez

MSc. Ernesto Rene González Guzmán

Asesor

MSc. Dora Leonor Urrutia de Morales.

Revisora

Guatemala de la Asunción, marzo 2020

Autoridades de la Universidad Panamericana

M. Th. Mynor Augusto Herrera Lemus
Rector

Dra. HC. Alba Aracely Rodríguez de González
Vicerrectora Académica

M.A. Cesar Augusto Custodio Cóbar
Vicerrector Administrativo

EMBA Adolfo Noguera Bosque
Secretario General

Autoridades de la Facultad de Ingeniería y Ciencias Aplicadas

MSc. MBA César Augusto Cuevas Guerra
Decano

M.A. Mónica Lissette Alcázar Serralde
Coordinadora

Guatemala de la asunción, noviembre de 2019

Señores

Facultad de Ingeniería y Ciencia Aplicadas

Presente

Por este medio doy fe que soy autor el articulo científico titulado "**Sistema informático para el control de activos de tecnología y gestión de incidentes para la Dirección de Análisis Criminal**" y confirmo que respeté los derechos de autor de las fuentes consultadas y consigné las citas correspondientes.

Acepto la responsabilidad como autor del contenido de este Artículo científico y para efectos legales soy el único responsable de sus contenidos.

Atentamente,

Roberto Guillermo Lavagnino Rodriguez

Ingeniería en sistemas y Tecnologías de la información y la Comunicación

Carné No. 201803199

UPANA 2.0
Universidad Panamericana
UNA MEJOR VERSIÓN DE NOSOTROS

Guatemala, 01 de junio de 2,020

Ref. FICA-PF-013/2020

Facultad de Ingeniería y Ciencias Aplicadas

Campus Central, Guatemala

De acuerdo con el dictamen rendido por el Ingeniero Ernesto René González Guzmán, revisor de la tesis denominada **Sistema informático para el control de activos de tecnología y gestión de incidentes para la dirección de análisis criminal del Ministerio Público,** presentado por el estudiante Roberto Guillermo Lavagnino Rodríguez, quien se identifica con ID 000014182 y, la aprobación de la Evaluación de Competencias Profesionales (ECP), según consta en el Acta No. 2020 - 04, de fecha 26 de mayo de 2,020; por lo tanto, se **AUTORIZA LA IMPRESIÓN**, previo a conferirle el título de Licenciado en Ingeniería en Sistemas y Tecnologías de la Información y la Comunicación.

M. Sc., MBA Ing. César Augusto Cuevas Guerra

Decano

Facultad de Ingeniería y Ciencias Aplicadas

Ing. César Augusto Cuevas Guerra
Decano de Ingeniería y Ciencias Aplicadas

Diagonal 34, 31-43 zona 16
2506-3600 | 1779
upana.edu.gt

UPANA 2.0
Universidad Panamericana
UNA MEJOR VERSIÓN DE NOSOTROS

Guatemala, 01 de junio de 2,020
Ref. FICA012/2020

Licenciada
Ana Marina Yol
Directora de Biblioteca
Universidad Panamericana
Presente

Estimada Licenciada Yol,

Por medio de la presente, hago entrega a la Biblioteca de la Universidad Panamericana un (1) disco compacto con su respectiva cajilla y carátula en archivo único formato PDF correspondiente a la Facultad de Ingeniería y Ciencias Aplicadas con la siguiente información:

Título: Sistema informático para el control de activos de tecnología y gestión de incidentes para la dirección de análisis criminal del Ministerio Público.

Autor: Roberto Guillermo Lavagnino Rodríguez.

No. ID: 000014182.

El alumno Roberto Guillermo Lavagnino Rodríguez, pertenece a Facultad de Ingeniería y Ciencias Aplicadas, previo a obtener el grado académico de Licenciatura en Ingeniería en Sistemas y Tecnologías de la Información y la Comunicación.

Sin otro particular, me suscribo,

M.A. Mónica Alcázar Serralde
Coordinadora
Facultad de Ingeniería y Ciencias Aplicadas
Universidad Panamericana

Licda. Mónica Lissette Alcázar Serralde
Coordinadora de Ingeniería y Ciencias Aplicadas

Vo.Bo. M.SC MBA César Augusto Cuevas Guerra
Decano
Facultad de Ingeniería y Ciencias Aplicadas
Universidad Panamericana

Ing. César Augusto Cuevas Guerra
Decano de Ingeniería y Ciencias Aplicadas

Diagonal 34, 31-43 zona 16
2506-3600 | 1779
upana.edu.gt

UPANA 2.0
Universidad Panamericana
UNA MEJOR VERSIÓN DE NOSOTROS

Guatemala, 01 de junio de 2,020

Ref. FICA-PF-014/2020

DICTAMEN DEL REVISOR DE TESIS

Nombre del estudiante:	Lavagnino Rodríguez, Roberto Guillermo.
Título de la tesis:	Sistema informático para el control de activos de tecnología y gestión de incidentes para la dirección del análisis criminal del Ministerio Público.
Revisor de la tesis:	Ing. Ernesto René González Guzmán.

Considerando,

Primero: Que previo a la otorgársele el grado académico de Licenciado en Ingeniería en Sistemas y Tecnologías de la Información y la Comunicación, el estudiante, Roberto Guillermo Lavagnino Rodríguez quien se identifica con ID 000014182, ha desarrollado el trabajo de Tesis denominado **"Sistema informático para el control de activos de tecnología y gestión de incidentes para la dirección de análisis criminal del Ministerio Público".**

Segundo: Que el profesional Ing. Ernesto René González Guzmán, ha leído el informe de tesis donde consta que el trabajo de tesis realizado por el estudiante en mención reúne las cualidades necesarias de un trabajo profesional universitario de Licenciatura.

Por tanto,

En su calidad de revisor del proyecto de tesis se emite **DICTAMEN FAVORABLE** para que continúe con los trámites de rigor.

Ing. Ernesto René González Guzmán
Revisor de Tesis

M.A Mónica Lissette Alcázar Serrañe
Coordinadora Facultad de Ingeniería y Ciencias Aplicadas

Lcda. Mónica Lissette Alcázar Serrañe
Coordinadora de Ingeniería y Ciencias Aplicadas

M. Sc., MBA César Augusto Cuevas Guerra
Decano Facultad de Ingeniería y Ciencias Aplicadas

Ing. César Augusto Cuevas Guerra
Decano de Ingeniería y Ciencias Aplicadas

UNIVERSIDAD PANAMERICANA
FACULTAD DE CIENCIAS APLICADAS

Agradecimientos

A JESUCRISTO MI DIOS	Gracias a su misericordia, gracia y sabiduría estoy completando un ciclo de mi vida, para Él sea toda la gloria.
A mis Padres	Gracias al apoyo incondicional que me dieron desde mi niñez.
A mi Esposa e Hijos	Greis Jemina, Estaban Antonio y Daniela Alejandra, por el apoyo y la paciencia en estos últimos años.
A mis hermanos	Gracias al ejemplo que ellos me dieron de seguir adelante no importando las consecuencias.
A la Universidad Panamericana	Por creer en mí y ayudarme en mi formación.

Contenido

Tabla de Ilustraciones v
Resumen i
Introducción ii
Capítulo 1 1
Marco Contextual 1
1.1 Antecedentes 1
1.2 Planteamiento del problema 2
1.3 Justificación 4
1.4 Objetivos 4
Objetivo general 4
Objetivos específicos 4
1.5 Alcances 5
1.6 Limites 5
Capítulo 2 6
Marco Teórico 6
2.1 Antecedentes 6
2.2 Fundamento Teórico 7
2.2.1 Inventario 7
Inventario de activos 8
Activo Fijo 8
Activos de tecnología 8
2.2.2 Sistema de gestión de inventario 8
Funciones del control de inventario 9
2.2.3 Sistema de gestión de incidentes 9
Soporte de Servicio 9
Gestión de incidentes 9
Incidente 10
Pasos para la gestión de incidentes 10

2.2.4 Sistema de información 10
Ciclo de vida de un sistema de información 11
Componentes de un sistema de información 11
Diseño de un sistema de información 14
Diagrama de casos de usos 15
Diagrama de actividades 16
Diagrama de estados 16
Diagrama de clases 17
Diagrama de Secuencia 17
Diagrama de componentes 18
Metodología de gestión Kanban 18
Metodología de Desarrollo Modelo en cascada 19
Datos persistentes 19
2.2.5 Glosario 20
Capítulo 3 22
Marco Metodológico 22
3.1 Planificación del proyecto 22
Kanban 23
3.2 Diseño 24
3.2.1 UML 24
Diagrama de Caso de usos 24
Diagrama de actividades 31
Diagrama de Clase 37
Diagrama de estados 40
Diagrama de componentes 41
3.2.2 Infraestructura 42
Contenedores 43
Contenedores de MongoDB 44
3.2.3 Comunicación 45
Estructura de los mensajes 45
Estatus 46

Mensaje 46
Cuerpo 46
3.2.4 Seguridad 47
Encriptación 47
3.2.5 Datos Persistentes 48
Sigeind 48
Sigeinv 49
3.2.6 Estructura Código 51
Backend - NodeJS 51
Frontend – AngularJs/ionic 51
3.2.7 Interfaz de Usuario 52
Login 52
Principal 53
Reportes 54
3.2.8 Sistema de archivos 55
3.2.9 Pruebas 55
FrontEnd 55
Backend 56
Seguridad 56
Capítulo 4 58
Conclusiones y Recomendaciones 58
4.1 Conclusiones 58
4.2 Recomendaciones 60
Base de datos 60
Manejo de Activos 60
Incidentes 61
Capítulo 5 62
Anexos 62
5.1 Catálogos 62
Motivos de egresos 62
Motivos de devolución 62

Tipos de activos de tecnologías 62
Tipos de incidente 63
Complejidad del incidente 63
Impacto del negocio 63
Estado del incidente 63
Donantes 63
Nivel de seguridad 64
5.2 Códigos HTTP 64
5.3 Objetivos de control y controles de referencia ISO/IEC 27002:2013 66
Gestión de Activos 66
5.4 Uso del sistema 67
Inicio de sesión 67
Pantalla principal 68
Buzón Activos de tecnología 69
Activos de tecnología 70
Operaciones de los activos de tecnología 74
Incidente 79
Ingreso de incidente 80
5.5 Seguridad 83
Bibliografía 85

Tabla de Ilustraciones

Ilustración 1: Leyenda caso de usos UML 16
Ilustración 2 Leyenda de diagrama de actividades 16
Ilustración 3: Leyenda de diagrama de estados 17
Ilustración 4: Leyenda de diagrama de clases 17
Ilustración 5: Leyenda de diagrama de secuencia 18
Ilustración 6: Leyenda de diagrama de componente 18
Ilustración 7: Distribución beta 23
Ilustración 8: Tablero de Kanban para la gestión de tareas de planificación de tareas 24
Ilustración 9: Caso de uso de ingreso de un activo de tecnología 26
Ilustración 10 Caso de uso del egreso de un activo de tecnología 27
Ilustración 11: Caso de uso de préstamo de activos de tecnología 28
Ilustración 12: Caso de uso de devolución de activos de tecnología 29
Ilustración 13: Caso de Uso de registro de incidente y sus soluciones. 29
Ilustración 14 Caso de uso de generación de reportes 30
Ilustración 15 Diagrama de actividades del ingreso de activos de tecnología 31
Ilustración 16 Diagrama de actividad del egreso de un activo de tecnología 32
Ilustración 17 Diagrama de actividad de Préstamo de activo 33
Ilustración 18: Diagrama de actividad de devolución de un activo de tecnología 34
Ilustración 19: Diagrama de actividad de ingreso de un incidente 35
Ilustración 20 Diagrama de actividad de solución de un incidente 36
Ilustración 21: Diagrama de clases de activos de tecnología 39
Ilustración 22: Diagrama de clases de incidente 40
Ilustración 23 Diagrama de estado del objeto activo de tecnología 41
Ilustración 24: Diagrama de componentes 41
Ilustración 25: Infraestructura de contenedores 43
Ilustración 26: Contenedor Sicogind 44
Ilustración 27: Estructura de directorio de los contenedores 45

Ilustración 28: Construcción de esponja para funciones HASH (Guido Bertoni J. D., 2019) 48
Ilustración 29: Pagina de ingreso del sistema 52
Ilustración 30: Modulo principal 53
Ilustración 31: modo de acceso a los archivos FTP 55
Ilustración 32: Pantalla de inicio de sesión 67
Ilustración 33: Pantalla de inicio 68
Ilustración 34: Creación de un incidente desde el listado de activos de tecnología 69
Ilustración 35: Parte superior del detalle de activo 70
Ilustración 36: Menú de tipo de activo 71
Ilustración 37: Menú de nivel de seguridad 71
Ilustración 38: Menú de donantes 72
Ilustración 39: Parte inferior del detalle de activo 73
Ilustración 40: Crear una nueva ubicación 74
Ilustración 41: Botón para crear un activo de tecnología 74
Ilustración 42: Pantalla de creación de activo de tecnología 75
Ilustración 43: Activo recién creado 76
Ilustración 44: Activo en estado de disponible 77
Ilustración 45: Pantalla con listado de usuarios 78
Ilustración 46: Activo Prestado 79
Ilustración 47: Activo en problemas 80
Ilustración 48: Ingreso de un incidente 81
Ilustración 49: Menú tipo de incidentes 81
Ilustración 50: Menú de complejidad 82
Ilustración 51: Menú de usuarios que reportan el incidente 82
Ilustración 52: Incidente sobre un activo de tecnología 83

Resumen

En el presente documento es un registro del análisis, diseño y desarrollo del sistema informático para el control de activos de tecnología y gestión de incidentes para la Dirección de Análisis Criminal del Ministerio Público de Guatemala.

Entre los registros se encuentra la documentación del proyecto desde la concepción, planeación, ejecución y la gestión de todos estos pasos con metodologías agiles.

El objetivo principal del proyecto es desarrollar un sistema informático que permita llevar el control de activos informáticos y sus incidentes. Esta necesidad surge debido a que, en la actualidad, la Dirección de Análisis Criminal lleva los controles en hojas de papel, hoja de cálculo y tiene poco control de estos, existe la posibilidad de pérdida de activos.

Se diseñó el sistema utilizando el estándar UML, se crearon los diagramas de casos de usos, actividades, clases, estados y componentes.

El sistema está dividido en tres aplicaciones: una es la encargada de llevar el registro y operaciones de los activos, la otra es encargada de llevar el control de los incidentes y por último está la encargada de proveer una interfaz de usuario amigable y entendible. Debido a la necesidad que la aplicación se ejecute en teléfonos móviles y computadoras de escritorio, se creó un sistema hibrido que pueda correr en cualquier sistema operativo moderno.

Introducción

La Dirección de Análisis Criminal cuenta con equipo y licencias de software que entra como donación, dado a la burocracia y trámites para generar un código en el sistema integrado de administración financiera del Ministerio de Finanzas Públicas se ha decidido utilizar estos activos de tecnología sin un control apropiado.

En el presente documento se encontrará el análisis, diseño y desarrollo de una solución informática para el registro de activos de tecnología, que ayude a llevar control de los activos de tecnología que además pueda generar reportes en tiempo real del uso de estas.

El documento tiene la siguiente división:

Capítulo 1 el marco contextual, se encuentra registrado el análisis que contiene la justificación, objetivos, antecedentes y funciones del sistema.

Capítulo 2 el marco teórico, se encuentra el registro teórico, se basa en el diseño y desarrollo del sistema.

Capítulo 3 el marco metodológico, contiene el diseño y patrón de desarrollo del sistema.

Capítulo 4 se registran las conclusiones y recomendaciones acerca del tema desarrollado.

Capítulo 5 se encuentran los catálogos y listados que apoyan el diseño y desarrollo del sistema.

Capítulo 1

Marco Contextual

1.1 Antecedentes

La Dirección de Análisis Criminal (DAC) es una dirección que pertenece al Ministerio Público el cual se está expandiendo al área metropolitana y al interior del país. Dado este crecimiento una cantidad significativa de equipo de cómputo (servidores, computadoras, portátiles, teléfonos, impresoras monitores entre otros) y licencias de software ingresan a la dirección, éstos carecen de controles del sistema SICOIN. Debido a que el trámite para ingresarlos es lento, se decide poner en funcionamiento los equipos o licencias sin que estén registrados en alguna base de datos central, debido que estos son necesarios para ejecutar las tareas diarias de los analistas.

Estos equipos, licencias u otros activos informáticos llevan un control (registro de quién es responsable, de dónde vino, entre otros) que se lleva en papel físico, hojas de cálculos y en muchas ocasiones no se tiene ningún registro. Esta situación deriva muchas veces en extravío de equipo o licencias de software. Se necesita un reporte de inventario de los equipos o licencias que son donadas por parte de instituciones internacionales. Este reporte se entrega en un período de cinco a siete días, esto se debe a que para generarlo se necesita revisar máquina por máquina e ir buscando los documentos de registro en el archivo físico.

Este factor influye directamente en el rendimiento del personal del soporte técnico debido a que el costo en términos de tiempo es muy alto por tratarse de una tarea repetitiva y se ha comprobado que existe pérdida de información de todos los eventos que existen sobre esos activos informáticos, actualmente no se tiene registro de los incidentes.

Los registros y datos de los activos de tecnología de la DAC están siendo llevados en hojas de papel físico, tales como el listado de equipos que están en situación de préstamo, es un riesgo que

la información se deteriore o extravíe, conlleva a la pérdida del equipo. Después de devolver el equipo, las hojas de papel se archivan en gavetas que una vez al mes son empaquetadas y enviadas a un departamento encargado de resguardar los documentos físicos, perdiendo así la oportunidad de recuperar información histórica del equipo o incidentes.

Las licencias, servidores y equipo de telecomunicaciones se encuentran guardados en hojas de trabajo de Excel o en la nube pública, lo cual constituye una fisura de seguridad importante y están siendo guardados en cuentas personales. Las hojas de trabajos que están creadas en Excel están guardadas en diferentes equipos sin ninguna política de respaldo, lo cual hace que la información sea vulnerable y se pierda.

En la gestión de los incidentes, los cuales son los distintos problemas que un equipo puede presentar, actualmente existe un sistema que registra tales incidentes junto con su resolución, pero no se tiene un registro íntegro de cada equipo específico que permita obtener el historial de éste y permite proporcionar la utilidad a la hora de la toma de decisiones, por ejemplo, cuando un equipo necesita cambio y se debe de hacer el requerimiento de compra.

1.2 Planteamiento del problema

A la fecha, en la Dirección de Análisis Criminal del Ministerio Público no posee un sistema informático para el control de activos de tecnología y gestión de incidentes. El sistema informático de control de activos de tecnología y gestión de incidentes es un sistema informático que permite llevar el control de los registros de activos de tecnología que además contiene el registro de todos los incidentes que ocurren en dichos activos de tecnología.

Se considera activos informáticos los siguientes bienes:

- Software
    - Licencias de software
    - Sistemas informáticos creados internamente.

- Hardware
    - Equipos de cómputo
    - Computadoras Personales
    - Computadoras Portátiles
    - Monitores
    - Discos Duros
    - Memorias Flash
    - Teclados
    - Mouse
    - Lectores CD/DVD
    - Audífonos
    - Mochilas para Computadoras portátiles
- Impresoras
- Servidores
- Switch
- Insumos
    - Cables
    - CD/DVD en blanco

Por la sensibilidad de la información que se maneja en esta dirección, el sistema informático como buena práctica se tomarán en cuenta los cuadros de controles de la norma ISO 27001-2013 en el apartado de Gestión de Activos para poder garantizar la confidencialidad, integridad, disponibilidad y la autenticidad de la información.

Los datos como medida de seguridad se guardarán con métodos criptográficos en la base de datos, con llaves públicas y privadas los cuales se encuentran guardados en la dirección.

1.3 Justificación

Es necesario contar con un sistema informático para el control de los activos informáticos, que permita tener un inventario actualizado de todos los bienes para tener un control de qué usos se le están dando a estos bienes. Se necesita generar informes a los distintos donantes donde se les garantiza que se les está dando el uso adecuado a los bienes que fueron donados. Por la seguridad que se maneja dentro de la dirección, se necesita una solución transparente en cuanto el funcionamiento del sistema (qué datos se están registrando, cuáles se están transmitiendo, entre otros) y además sea amigable y se adapte a las necesidades puntuales que se tiene dentro de la dirección de análisis criminal.

Este sistema facilitará todas las operaciones de soporte técnico, ayudando a encontrar soluciones rápidas que registrarán todos los incidentes en los activos informáticos, además de ayudar en la planificación del mantenimiento preventivo.

1.4 Objetivos

Objetivo general

Analizar, diseñar y desarrollar un sistema informático que permita llevar el control de activos informáticos y sus incidentes para la dirección de análisis criminal que garantice la confidencialidad, la integridad, la disponibilidad y la autenticidad de la información gestionada por medio del mismo.

Objetivos específicos

- Automatizar el control de inventario de activos de tecnología.
- Digitalizar todos los controles que se llevan en hojas de papel
- Unificar todos los controles de activos informáticos

1.5 Alcances

El alcance de esta investigación es el análisis, diseño y desarrollo de un sistema informático para el control de activos de tecnología y gestión de incidentes para la Dirección de Análisis Criminal, el cual llevará el registro y control de los activos de tecnología. Los controles que se incluirán dentro del sistema son los siguientes:

- Inventario de los bienes: control de los bienes con que cuenta.
- Propiedad de los bienes: control de quién tiene asignado activos informáticos
- Devolución de los bienes: control de la devolución de bienes
- Incidencia de los bienes: control de todos los incidentes
- Gestión de medios removibles: control de discos duros u otro medio que pueda llevar información
- Las fases del sistema que se realizarán:
    - Análisis
    - Diseño
    - Desarrollo

En este proyecto no se contempla la fase de implementación ni el despliegue de los contenedores de los diferentes módulos.

1.6 Limites

El sistema contará con un módulo para registrar datos de activos de tecnología que incluirá datos de los incidentes. Los datos que no se registrarán en el sistema son:

- Activos ajenos a las tecnologías
- Materiales de oficina
- Incidentes ajenos a los activos de tecnología

El sistema no incluirá las siguientes funciones:

- Control de usuarios (existente en la Dirección de Análisis Criminal)
- Repositorio de archivos (existente en la Dirección de Análisis Criminal)
- Importación de datos en papel o en hojas electrónicas.

- Implementación del sistema.
- La creación, mantenimiento y gestión de los contenedores
- Manual de usuario

Capítulo 2
Marco Teórico

2.1 Antecedentes

En los tiempos actuales es importante no solo limitarse a desarrollar la calidad de todos los procesos, sino que se debe incrementar la eficiencia de la producción utilizando sistemas informáticos En la actualidad la función principal de estos sistemas informáticos es presentar o procesar la información. Los sistemas informáticos se refieren al conjunto de elementos que se utilizan para reunir, almacenar y procesar la información con el objetivo de disminuir costos o hacer funciones especializadas de manera eficiente.

Un sistema informático que lleve el control del inventario con gestión de incidentes no solo ayuda a gestionar el control de los activos informáticos (hardware y software) también ayuda a generar los informes detallados de inventario de manera inmediata. Este sistema informático es crítico, ya que se necesita tener un control de los registros, eventos e incidentes de los activos informáticos. Este sirve para tomar decisiones de compra, planificar el mantenimiento preventivo y control de tarjetas de responsabilidad entre otros.

La Dirección de Análisis Criminal del Ministerio Publico (DAC) está en proceso de ampliación, no solo en la ciudad de Guatemala sino también en el interior de la república, siendo necesario un control de todo el inventario de activos de tecnología a través de un sistema de información que sea capaz de agilizar el proceso de entrega, devolución y baja de los mismos, los cuales incluyen Hardware y Software.

Actualmente existe en el mercado una variedad de sistema de información Open Source que permiten el control del inventario, pero ninguno de estos cubre el 100% de necesidades de la Dirección de Análisis Criminal, entre estas:

- Encriptación de datos
- Acceso a dispositivos periféricos:
  - Lector de Huella
  - Lector de código de barras
  - Lector de códigos QR
- Buenas prácticas en la gestión de incidentes.
- Fácil integración con los sistemas de informáticos creados en la Dirección de Análisis Criminal.
- Documentación apegada a las buenas prácticas.
- Pruebas de seguridad de OWASP.
- La escalabilidad y prevenir la orfandad de software (Que los autores abandonen el proyecto y dejen de corregir las fallas, principalmente fallas de seguridad).
- Construcción de nuevos módulos.
- Aplicación hibrida.

2.2 Fundamento Teórico

2.2.1 Inventario

"*Valoración contable de las mercancías y bienes productivos existentes en una empresa*." (Diccionario Enciclopédico Vox 1, 2009) Los inventarios son listados que se lleva de manera detallada todos aquellos bienes que forman parte de una empresa o institución.

Es necesario controlar un inventario para saber cuáles son las necesidades de una empresa o institución, en este control se tiene que tomar en cuenta todos los movimientos y actividades que se tienen de dicho inventario para tener un historial y además para tener información actualizada, correcta y para tomar las mejores decisiones para la empresa o institución.

Inventario de activos

Es un listado o registros de todos aquellos bienes que posean una empresa o institución. Estos bienes tienen un valor para la empresa. Pueden ser de tres tipos:

- Circulante: estos activos son los que se pueden convertir en efectivo en un corto plazo.
- Fijo: estos activos son aquellos que son duraderos y son necesarios para que la empresa o institución funcione.
- Diferido: son los activos por el cual la empresa o institución ya ha realizado el pago, pero no han sido utilizados.

Activo Fijo

Son todos aquellos bienes que una empresa o instrucción necesita para su funcionamiento y es parte del capital e inversión para la operación de ésta. Pueden ser:

- Tangible: Son todos los activos que tienen una forma física es decir que se puedan ver y tocar.
- Intangible: Son todos los activos que no están representados de forma fisica.

Activos de tecnología

El inventario informático son todos los bienes (tangibles e intangibles) que posee una empresa o institución que forma parte la gestión de la información (seguridad, resguardo, comunicación, (otros).

2.2.2 Sistema de gestión de inventario

Es un proceso en el cual una empresa o institución registra y administra todos los movimientos que tienen sus activos informáticos tangibles e intangibles para así gestionar de manera eficiente el flujo de la información que surge a partir de los movimientos que se tienen de este.

Funciones del control de inventario

Las funciones que tiene un sistema de control de inventario son:

- Tener un registro de todos los activos informáticos que cuenta la empresa o institución. Esta se debe de encontrar actualizado.
- Control de existencias, para conocer de manera rápida y eficiente las carencias de los bienes que necesita de la empresa o institución para su correcto funcionamiento.
- Identificar anomalías de los bienes que pertenecen a la empresa o institución como por ejemplo el robo o pérdida.
- Generación de Información para la gerencia acerca de la situación de los bienes de la empresa.
- Revisar si se están cumpliendo las políticas de seguridad en los equipos.
- Control para reasignar recursos o licencias no utilizados para reducir costos.
- Gestionar el entorno informático.

2.2.3 Sistema de gestión de incidentes

Es un conjunto de procedimientos independiente de la infraestructura y de los diferentes proveedores que ayudan a gestionar los distintos incidentes para lograr calidad centrándose en la mejora continua en los sistemas informáticos.

Soporte de Servicio

Es un conjunto de mejores prácticas que tiene como objetivo que los usuarios tengan accesos y disponibilidad a todos los servicios de las empresas o instituciones.

Gestión de incidentes

Es un área que pertenece a la gestión de servicios de tecnologías de la información. Tiene como objetivo principal de mantener el correcto funcionamiento de todos los servicios y reducir los impactos que se tengan derivados a problemas de índole informático para así mantener la disponibilidad y calidad de los diferentes servicios.

Incidente

"Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción de este o una reducción de la calidad de dicho servicio. El objetivo de es reiniciar el funcionamiento normal tan rápido como sea posible con el menor impacto para el negocio y el usuario con el menor coste posible." (ITIL Incident Management, s.f.).

Los incidentes son frutos de errores en la infraestructura y se puede corregir de manera rápida y sin ninguna inversión extra a través de una reparación o cambio. Si existe la reincidencia, se crea un problema, es una diferente gestión y se utiliza un diferente equipo para poder revisarlo y corregirlo.

Pasos para la gestión de incidentes

Los pasos para la gestión de incidentes son los siguientes:

- Detección: Puede ser que afecte a los usuarios o por los monitoreos regulares.
- Registro: Se crea un registro del incidente.
- Clasificación:
    - Impacto: Nivel que afecta el servicio
    - Urgencia: Tiempo máximo para la resolución del problema
- Diagnóstico: Identificación y análisis del problema para verificar el análisis
- Escalamiento: Por falta de conocimiento, herramientas u otros motivos se pasa a otro equipo para la solución.
- Solución: Es la resolución del problema
- Cierre: Verificación de la resolución del problema
- Monitoreo: Revisión de la resolución correcta del problema.

2.2.4 Sistema de información

Es una serie de elementos que tienen como objetivo organizar, tratar y gestionar la información y su creación se basa en una necesidad que inicia con la definición del proyecto hasta la presentación de este.

Los componentes de un sistema de información son:

- Datos
- Hardware
- Software
- Redes
- Usuarios

En los sistemas de información existen actividades que transforman los datos a información que necesita una empresa o institución para su funcionamiento y su correcta toma de decisiones, estas actividades son:

- Almacenamiento de datos
- Distribución de datos
- Procesamiento de datos
- Recopilación de datos

Ciclo de vida de un sistema de información

Existen varios elementos que se consideran en el ciclo de vida de un sistema de información las básicas son**:**

- Codificación
- Conocimiento del entorno y sus propuestas para solucionar ese problema
- Diseño del sistema
- Identificación del problema
- Implementación
- Mantenimiento
- Propuesta del sistema

Componentes de un sistema de información

Back-End: es la parte de un sistema de información encargada de procesar toda la información, es decir que revisa todas las reglas del negocio para el correcto funcionamiento del sistema. Esta se encarga de comunicarse con el manejador de base de datos para registrar la información o para

solicitar la información requerida. También es encargada de la seguridad de la información, revisando si el usuario que está solicitando dicha información tiene acceso a ella.

NodeJs: es un entorno de ejecución y de javascript que está dirigida para eventos asíncronos, la versión actual es 10.16.3 LTS. Trabaja en base al motor V8 creado por Google que permite la ejecución del lado del servidor de una manera rápida y eficiente. Sus principales características son:

- Arquitectura orientada a eventos
- Asíncrono
- De un solo hilo, esto permite responder desde el servidor sin necesidad de bloqueos lo que le hace altamente escalable.
- Sin buffer

Base de datos**:** una base de datos es una colección de datos que se encuentran organizados, almacenados y relacionados entre ellos mismos para que puedan ser utilizados por un sistema de información de una empresa o institución Sus características son:

- Redundancia
- Integridad de los datos
- Seguridad de acceso
- Acceso concurrente

Los tipos de la base de datos son:

Base de Conocimiento: es un conjunto de registros o documentos que contienen información de conocimiento de todas las áreas o departamentos de una empresa o institución. Estas están diseñadas para que los usuarios puedan acceder a todos los conocimientos acumulados de las empresas o instituciones.

Base de datos Relacionales: son todas las bases de datos que tiene un modelo relacional es decir que permite establecer relaciones entre los datos a través de un conjunto de registros llamados tablas. Estos tienen como restricción que los nombres no pueden ser el mismo, y sus registros son

un conjunto de filas y columnas, cada registro debe tener un identificador único en una tabla y a esta se le llama llave primaria, y se relaciona con otros registros a través de la llave foránea. Para consultas se utiliza el lenguaje SQL.

Base de datos no relacionales: son todas las bases de datos que no necesariamente utilizar el lenguaje SQL, y no se rigen por las reglas de las tablas y relaciones. Además, estas no soportan las operaciones JOIN, estas tienen las siguientes características:

- Consistencia Eventual: para obtener un mejor rendimiento, los cambios realizados no son propagados a todos los nodos de manera inmediata.
- Flexibilidad en el esquema: los documentos pueden tener diferente forma, así solo se guarda los atributos que necesita.
- Escalabilidad horizontal: se puede aumentar el rendimiento solo añadiendo más servidores o nodos.

Existen diferentes tipos de argumentos para elegir una base de datos no relacional, pero las más importantes son las siguientes:

- Guardar información de gran tamaño que tenga poco o nada de estructura
- Obtener mayor beneficio de computación en la nube
- Aumentar la velocidad de desarrollo
- Facilitar la escalabilidad horizontal

Express: “Express es una infraestructura de aplicaciones web Node.js mínima y flexible que proporciona un conjunto sólido de características para las aplicaciones web y móviles.” (Express, s.f.) Express posee un conjunto de métodos que manejan las peticiones http (get, post, set) y la URL. Estas peticiones pueden ser leer o escribir en la base de datos o al manejador de archivos y crear html dinámico entre otros.

Front-End: Es la capa de presentación de los sistemas de información encargado de recopilar y presentar la información a los usuarios de manera entendible y amigable. Uno de las más utilizados es Angular.

Manejador de base de datos: es un software que se dedica a controlar el acceso a los datos entre la base de datos y las aplicaciones que son utilizados por los usuarios de una empresa o institución. Y esta se compone de los siguientes lenguajes:

- Definición de datos
- Manipulación de datos
- Consulta de datos

Y sus principales funciones son:

- Creación de las bases de datos
- Organización de las bases de datos
- Registrar el uso de la base de datos
- Relación con el manejador de archivos
- Respaldo de los datos
- Recuperación de los datos
- Control de concurrencia
- Seguridad de los datos
- Integridad de los datos

Diseño de un sistema de información

El diseño de un sistema de información es el proceso de definir la arquitectura, los componentes, módulos y la gestión de los datos con el fin de satisfacer los requerimientos de un sistema. Para el diseño se utiliza un lenguaje estandarizado llamado UML (Lenguaje unificado de modelado).

UML (Unified Modeling Language) es un lenguaje para modelar software, se utiliza para visualizar, especificar, construir y documentar un sistema. Este permite crear un plano estándar del sistema que abarca los procesos, funciones, esquemas de base de datos y compuestos reciclados entre otros. Los tipos de diagramas que existen en UML son:
Comportamiento: son todos los diagramas que muestran el comportamiento dinámico de actividades. Entre estos se encuentran los siguientes diagramas:

Diagrama de actividades: representan el flujo de trabajo.

Diagrama de casos de usos: representan los usuarios de un sistema

Diagrama de estados: representan el comportamiento del sistema en los estados el cual se encuentra los objetos.

Estructurales: son todos los diagramas que muestran el estado estático de un sistema. Entre estos se encuentran:

Diagrama de clases: muestra las clases sus atributos, relaciones y operaciones.

Diagrama de estructura compuesta: muestra la estructura interna de cada clase.

Diagrama de componentes: muestra la relación entre los componentes de un sistema.

Diagrama de casos de usos

El diagrama de caso de uso sigue la notación establecida por UML, incluyendo los elementos del modelo UML los cuales son:

- Actores
- Casos de usos
- Relaciones

Las asociaciones son aquellas relaciones que tiene los actores con los casos usos y las generalizaciones son las relaciones entre los casos de usos, pueden ser uso “uses” o de herencia “Extends”.

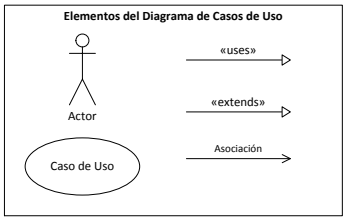


Ilustración 1: Leyenda caso de usos UML

Diagrama de actividades

También llamado diagrama de flujo es una representación gráfica de un proceso o actividad. Este contiene un único punto de entrada y salida.

Ilustración 2 Leyenda de diagrama de actividades

Diagrama de estados

El diagrama de estados representa gráficamente una máquina de estados, que muestra los estados y sus transiciones de los objetos cuando son estimulados externamente.

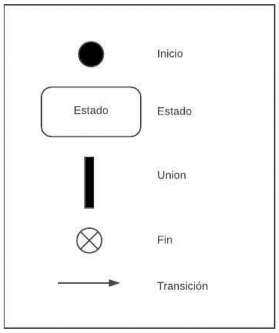


Ilustración 3: Leyenda de diagrama de estados

Diagrama de clases

El diagrama de clases es un modelo estandarizado para mostrar la arquitectura orientado a objetos del sistema que se desea desarrollar. Ayuda a comprender la visión de los esquemas de datos.

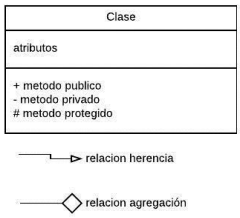


Ilustración 4: Leyenda de diagrama de clases

Diagrama de Secuencia

El diagrama de secuencia es un modelo estandarizado que muestra la interacción de todos los objetos en un sistema. Ayuda a entender como es la interacción entre todos los objetos de un caso de uso a través del tiempo.

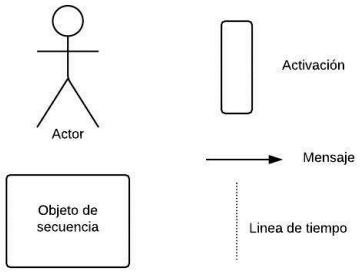


Ilustración 5: Leyenda de diagrama de secuencia

Diagrama de componentes

El Diagrama de componentes es un modelo estandarizado que muestra una abstracción de la división de los componentes de un sistema, que contiene los componentes y las relaciones entre ellos.

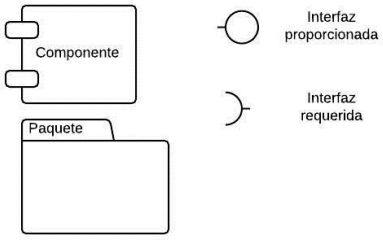


Ilustración 6: Leyenda de diagrama de componente

Metodología de gestión Kanban

Es un sistema de administración altamente eficiente y sus orígenes están en los procesos "Just in time" (Justo a tiempo), forma parte de las metodologías agiles de origen japones. La palabra Kanban significa tarjetas visuales, tiene una serie de ventajas:

- Calidad: Todo debe de ser completado con poco margen de error.
- Reducción de desperdicio: se debe utilizar solo lo necesario para completar la tarea.
- Mejor continua: alcanzar los objetivos con una mejora en el desarrollo del proyecto.

- Flexibilidad: Las tareas se priorizan en el backlog (tareas pendientes) según las necesidades

A diferencia de SCRUM este utiliza un tablero continuo que contiene un listado de tarjetas que poseen las tareas descritas en el EDT que se van desplazando hasta que la tarea se complete. Este tiene como objetivo clarificar la más que se pueda las tareas que se deban de realizar. “Stop Starting , start finish” es el lema principal de Kanban que prioriza las tareas antes de empezar una nueva. Las reglas son:

- El proyecto debe tener un límite.
- No se puede empezar una tarea sin que se haya finalizado otra.
- Las tareas que se abran deben de tener un cierre.

Otra diferencia con SCRUM es que el Kanban se puede mezclar tareas y proyectos con el objetivo de mantener un flujo constante de trabajo.

Metodología de Desarrollo Modelo en cascada

Es una metodología de programación en la cual el desarrollo son pasos vistos hacia abajo como una cascada de agua, y tiene como principios básicos en que el proyecto está divido fases secuenciales, se hace hincapié la planificación y se utiliza un control a través de documentación escrita. El modelo consiste en los siguientes pasos:

- Análisis
- Diseño
- Desarrollo
- Pruebas
- Implementación
- Mantenimiento

Datos persistentes

Son todos las estructuras, propiedades y datos de un sistema de informático que deben sobrevivir de alguna manera todas las versiones o cambios que de éstas sufren a través del ciclo de vida.

2.2.5 Glosario

ACTORES: Un actor en el diagrama de casos de usos de UML se define como una entidad externa al sistema que tiene alguna interacción con el sistema.

ANGULAR: Es una herramienta que permite la creación de Interfaces de Usuario basada en JavaScript. Este permite crear y diseñar vistas simples para cada estado de los sistemas de información. La lógica de todos los componentes que se crean encapsulados (pueden manejar su propio estado) pueden pasarse datos a través de la aplicación sin modificar el DOM.

CODIGO DE BARRAS: Es un código basado en un conjunto de líneas paralelas.

CODIGO QR: Código de barras bidimensional que puede almacenar datos.

COMPONENTE: Es un grupo de elementos que forman la composición de un sistema de información

CONTENEDOR: Es un programa que permite la virtualización para el despliegue de aplicaciones, proporcionando una capa adicional de abstracción que ayuda la virtualización en diferentes sistemas operativos.

ENTERO: Es un número que se representa sin notación decimal.

FRAMEWORK: Es un entorno de trabajo que tiene un conjunto de módulos de software que son utilizado como base para desarrollo de software.

HTTP: Es el protocolo para la transferencia de datos.

IONIC: Es un framework que es utilizado para desarrollar soluciones web a través de distintas plataformas.

JAVASCRIPT: Es un lenguaje de programación orientado a objetos basados en prototipos y débilmente tipado.

JSON: Estándar para el intercambio de información.

MONGODB: Es un motor de base de datos no SQL orientado a colecciones y documentos.

NIP: Número de identificación personal. Es el numero el cual se identifica al personal del Ministerio Publico.

OPEN SOURCE: Es un tipo de licencia que permite tener acceso al código fuente de los sistemas informáticos.

OWASP: Es un proyecto cuyo objetivo es buscar y combatir las causas que hacen que un sistema informático sea inseguro.

REST: Arquitectura de transmisión de datos por el protocolo HTTP.

SICOIN: Sistema de contabilidad integrada cuya función es monitorear las ejecuciones presupuestarias gubernamentales.

SCRUMS: Es una metodología ágil que permite entregas parciales en un proyecto.

SQL: Es un lenguaje de consulta estructurada que se utiliza para administrar y recuperar datos, también tiene otros usos como crear, modificar y eliminar elementos dentro de una base de datos.

UTC: Tiempo Universal Coordinado.

Capítulo 3

Marco Metodológico

3.1 Planificación del proyecto

Para la planificación del proyecto se creó un listado de tareas. Estas tareas están organizadas en hitos, los cuales son los siguientes:

- Planificación proyecto
- Marco Teórico
- Análisis del sistema
- Documento de diseño
- Software (Desarrollo)
- Cierre de proyecto
- Anexos

Las tareas se rigen por un set de reglas, estas son:

- La tarea no puede iniciar si su predecesor no ha finalizado.
- La tarea tiene un inicio y un fin.
- La tarea al finalizar se crea un documento técnico, el cual documenta el trabajo hecho por la tarea.

En el cálculo de la tarea se utilizó el método PERT de tiempo esperado, se considera el tiempo de la tarea como una variable aleatoria en una distribución beta con sesgo a la derecha:

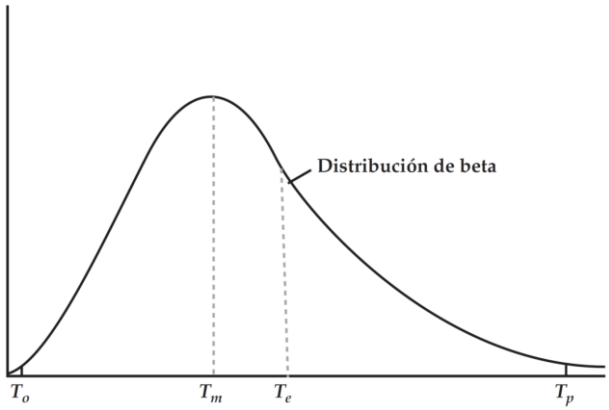


Ilustración 7: Distribución beta

Las tareas se calculan tomando 3 tiempos. El tiempo optimista (To), tiempo pesimista (Tp) y el tiempo más probable (Tm). Esto es debido que en ciertas ocasiones el cálculo en la estimación de los tiempos a veces son demasiados optimistas y en la realidad el tiempo utilizado para finalizar una tarea es mayor que el tiempo más probable. La fórmula es la siguiente:

$$Tt = \frac{(To + 4Tm + Tp)}{6}$$

Dados los tiempos de las tareas, se crea un cronograma con los hitos con las fechas de finalización. Esto crean un punto de control que nos muestra si el proyecta tiene demora o va en tiempo.

Kanban

Se crea el tablero con el listado de tareas y de manera gráfica se representa las tareas pendientes, trabajando y completadas.

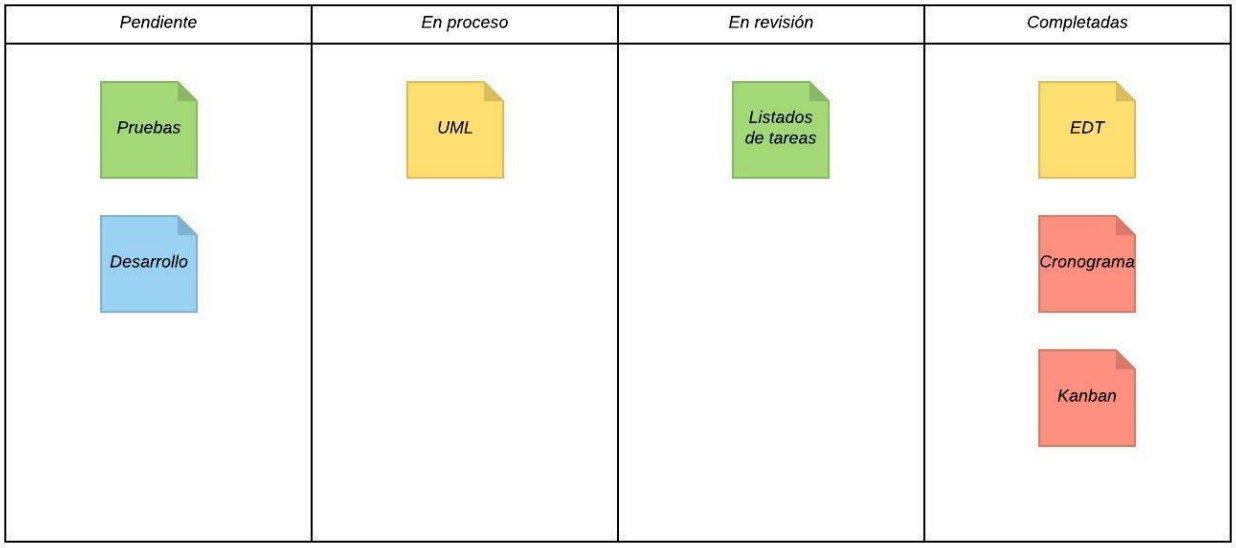


Ilustración 8: Tablero de Kanban para la gestión de tareas de planificación de tareas

3.2 Diseño

3.2.1 UML

Diagrama de Caso de usos

El sistema informático para el control de activos de tecnología y gestión de incidentes para la Dirección de Análisis Criminal interactúa con tres elementos externos:

- Administrador: es el encargado del mantenimiento del sistema. Sus funciones administrativas son las siguientes:
    - Mantenimiento de catálogos: puede ingresar, eliminar y actualizar los distintos catálogos del sistema.
    - Asignación de permisos: puede asignar permisos de cualquier función del sistema a los usuarios.
    - Activación / desactivación del sistema: puede evitar que los usuarios ingresen al sistema.

- Coordinador: es el encargado de revisar lo que registran los técnicos. Entre sus funciones están:
    - Autorizar el ingreso de activos de tecnología.
    - Autorizar el egreso de activos de tecnología.
    - Autorizar la solución del incidente.
    - Generar todos los reportes del sistema.

- Técnico: Es el encargado de registrar todos los movimientos (ingreso, egresos, préstamo y devoluciones) de los activos de tecnología, así como su incidentes y soluciones. Entre sus funciones están:
    - Registrar los movimientos de los activos de tecnología.
    - Registrar los incidentes y sus soluciones.

El Sistema informático para el control de activos de tecnología y gestión de incidentes para la Dirección de Análisis Criminal contará con las siguientes actividades:

- Ingresos y egresos de activos de tecnología
- Préstamos y devoluciones de activos de tecnología
- Registros de los incidentes y sus respectivas soluciones
- Generación de Reportes

El ingreso de activos de tecnología se refiere a ingresar un registro de hardware o software. En esta actividad el técnico registra un nuevo activo de tecnología. Ingresando todos los campos solicitados y revisando si existe algún antecedente en los equipos. Por último, el coordinador revisa los datos y da la autorización para su registro formal del sistema.

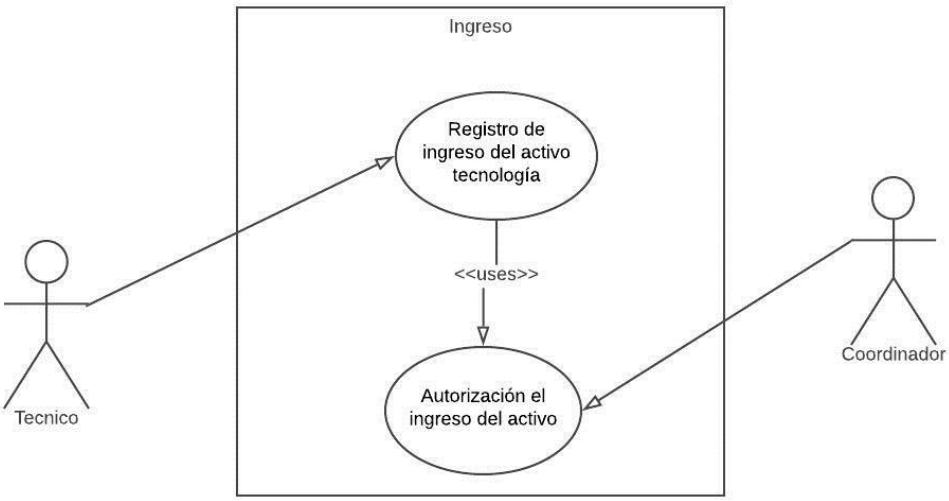


Ilustración 9: Caso de uso de ingreso de un activo de tecnología

El egreso de activos de tecnología se refiere a dar de baja al equipo, el equipo dado de baja no es posible prestarlo, ni devolverlo. Para dar de baja se debe de cumplir con los siguientes requisitos:

- Existir un motivo de baja.
- No debe estar en estado de préstamo.
- No debe de tener ningún incidente en grado de problema sin solución

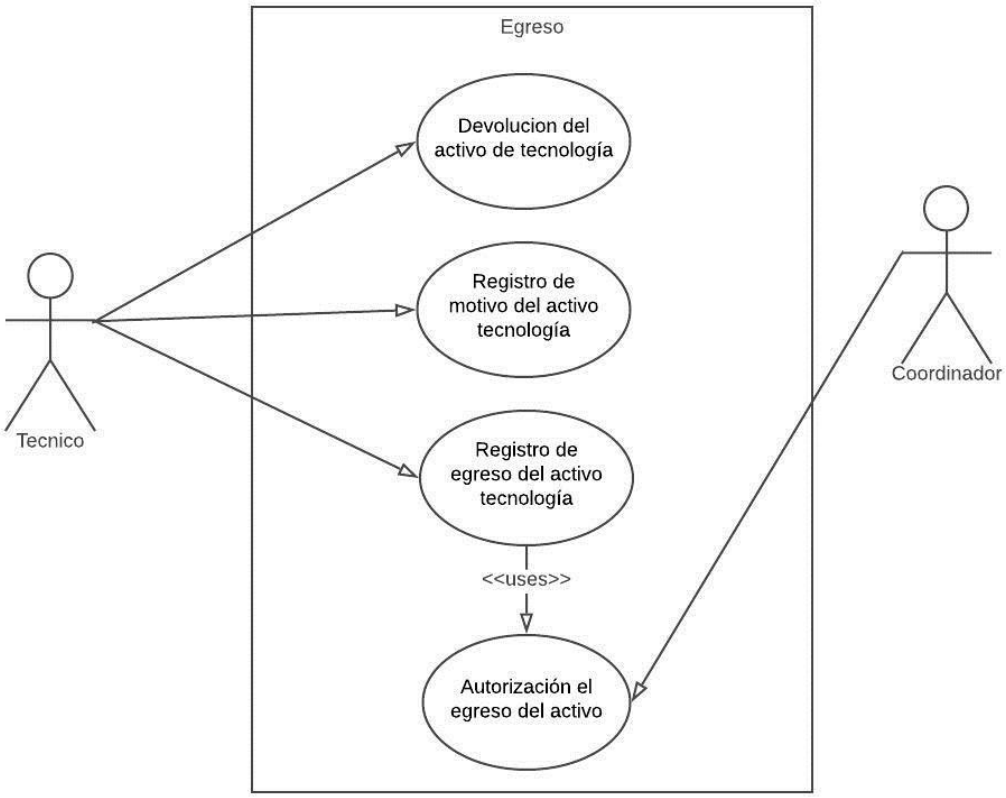


Ilustración 10 Caso de uso del egreso de un activo de tecnología

El préstamo de activos de tecnología es la actividad de registrar el préstamo en el sistema. Este precede de una solicitud. El técnico registra esta solicitud en el sistema. Los requisitos para registrar la solicitud son:

- Usuario que solicita el activo de tecnología.
- Tiempo de préstamo.
- Motivo de préstamo.
- Tipo de información que el activo de tecnología manejara.

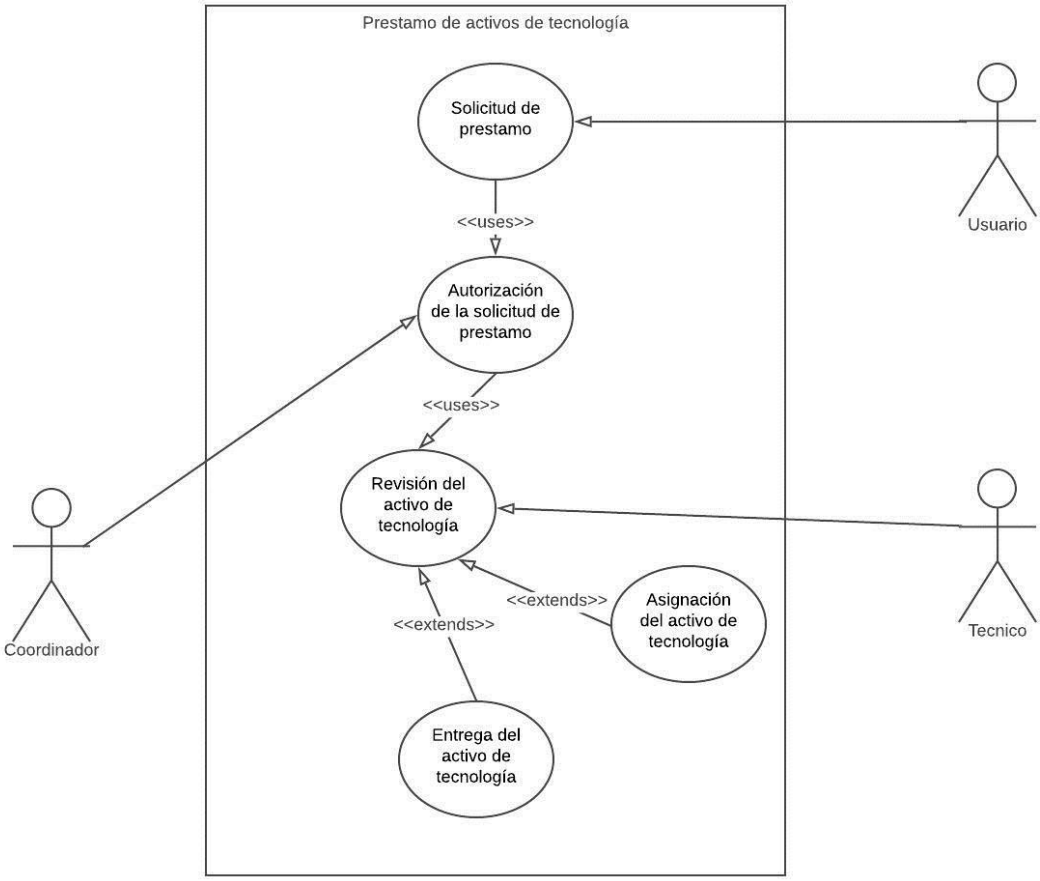


Ilustración 11: Caso de uso de préstamo de activos de tecnología

La devolución de activos de tecnología es la actividad el cual el usuario devuelve el activo de tecnología y el técnico registra la devolución. Esta actividad no necesita autorización de parte del coordinador. Los requisitos para registrar la actividad son los siguientes:

- No debe de tener ningún incidente sin solución
- Revisiones al activo de tecnología completas.

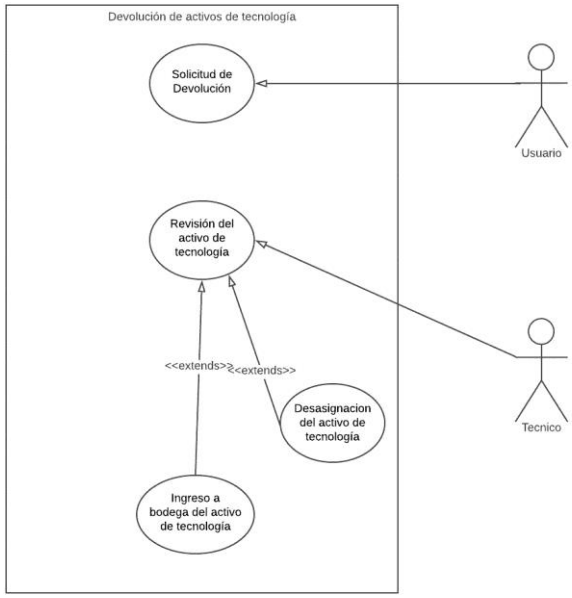


Ilustración 12: Caso de uso de devolución de activos de tecnología

El registro de los incidentes y sus soluciones es la actividad el cual el técnico registra los distintos incidentes con sus respectivas soluciones en un activo de tecnología.

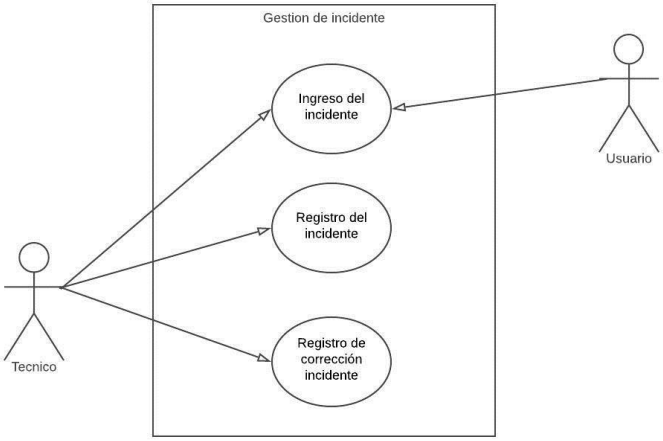


Ilustración 13: Caso de Uso de registro de incidente y sus soluciones.

La generación de reportes el cual el coordinador o el administrador genera reportes sobre los registros que están guardados en el sistema. Los reportes que se pueden generar son los siguientes:

- Bitácoras del sistema: es un reporte el cual contiene todos los movimientos de todos los usuarios del sistema. Este reporte solo puede ser generado por el administrador.
- Incidentes concurrentes: este reporte detalle todos los incidentes registrados en el sistema.
- Listado de activo de tecnología: este reporte contiene el listado completo de todos los activos de tecnología.
- Altas y bajas: este reporte detalla los registros de préstamos y devoluciones de los activos de tecnología.

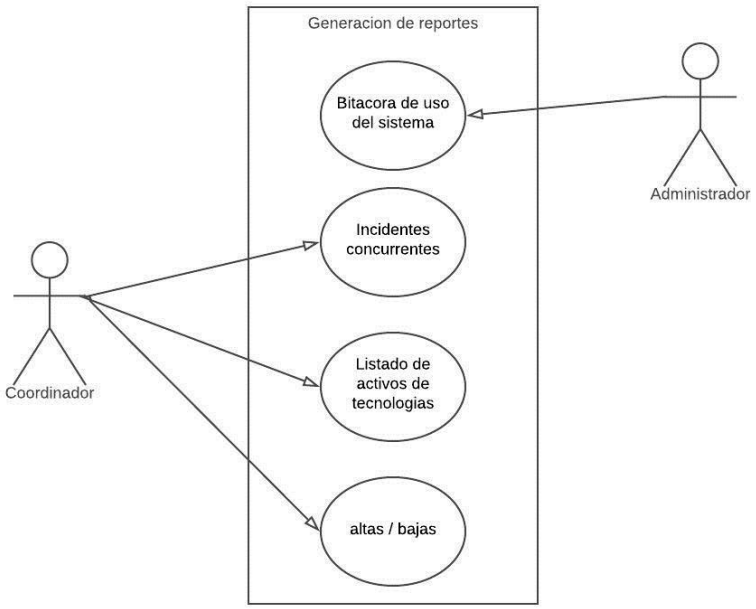


Ilustración 14 Caso de uso de generación de reportes

Diagrama de actividades

Las actividades que se desarrollan en el Sistema informático para el control de activos de tecnología y gestión de incidentes para la Dirección de Análisis Criminal se detallan a continuación:

En la actividad de ingreso de un activo de tecnología consiste en el ingreso de activos de tecnología a la DAC, ya sea por donación o compra directa. El técnico crea un nuevo registro de activo de tecnología e ingresa los datos solicitados. El Coordinador revisa los datos y verifica que estén ingresados correctamente. Cuando el coordinador autoriza el sistema crea un identificador y el técnico procede a generar un QR y un código de barras para etiquetar el activo de tecnología. El activo de tecnología se puede asignar a un usuario de la DAC o se guarda en bodega.

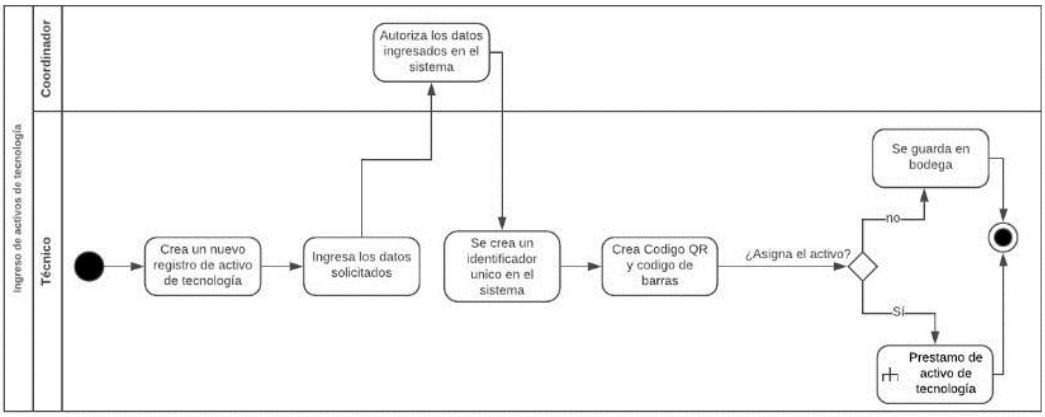


Ilustración 15 Diagrama de actividades del ingreso de activos de tecnología

La actividad de egreso consiste en retirar de la DAC un activo de tecnología ya sea porque está obsoleto o irreparable. El técnico verifica los datos y registra el egreso en el sistema. Este registro debe de contener un motivo, por ejemplo, obsoleto que se refiere a que el activo de tecnología no es útil a la Dirección de Análisis Criminal. Para el listado completos de motivos referirse al anexo 5.1. El coordinador autoriza el egreso, y el sistema da de baja al equipo.

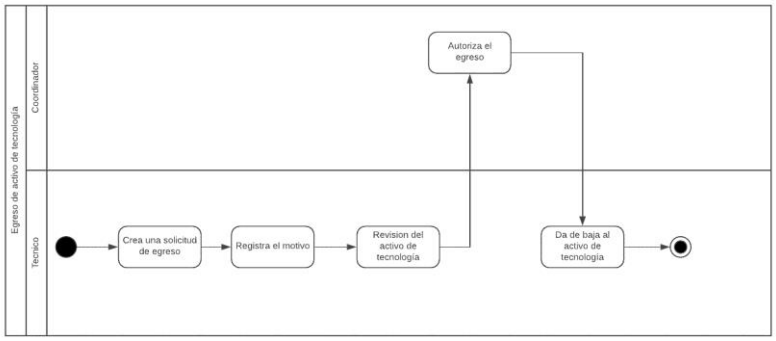


Ilustración 16 Diagrama de actividad del egreso de un activo de tecnología

La actividad de préstamo de un activo de tecnología consiste en asociar a un usuario de la DAC o del Ministerio Público un activo de tecnología disponible. Si no hay disponible se registra la solicitud. Si hay disponible se solicita la autorización del coordinador, después de autorizado se prepara el activo de tecnología y si es necesario que el técnico instale (ya sea colocar el activo en un lugar específico o instalar el software en una maquina) se crea un incidente. Es necesario colocar la temporalidad del préstamo, además del uso que se le va a dar al activo. Se debe de registrar si los datos que va a manejar el activo son sensibles.

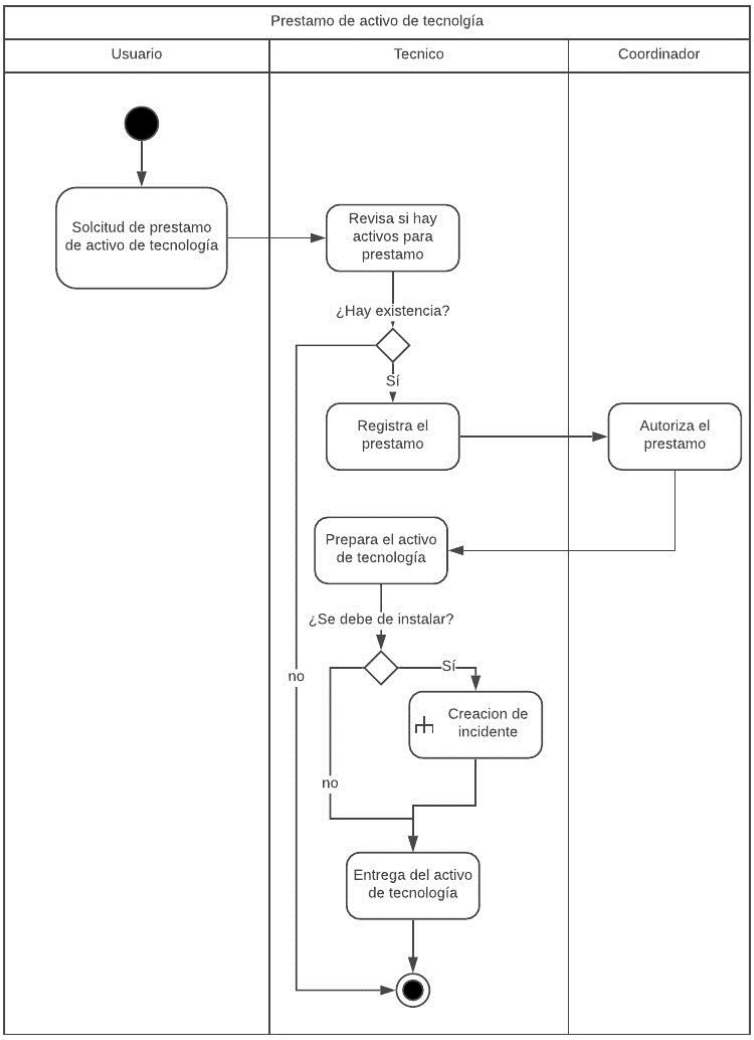


Ilustración 17 Diagrama de actividad de Préstamo de activo

La actividad de devolución cosiste en que se devuelve después de un préstamo un activo de tecnología, el técnico recibe el activo, revisa si existe algún incidente sin solución. Si la hay este procede a solucionarlo, después procede a ingresar el motivo por el cual se está devolviendo el activo de tecnología. Sin un motivo no es posible registrar la devolución.

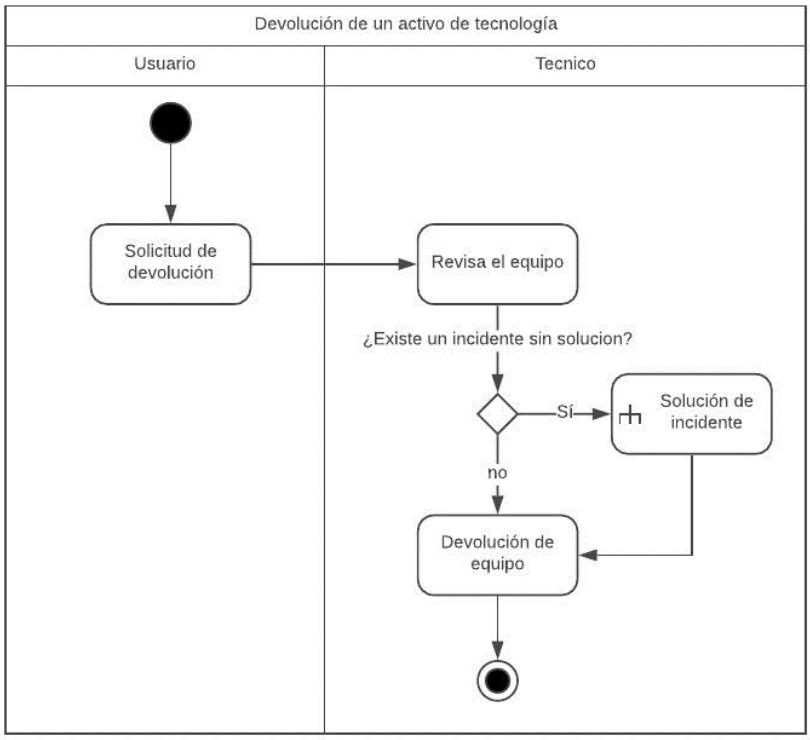


Ilustración 18: Diagrama de actividad de devolución de un activo de tecnología

El ingreso de un incidente consiste en que el técnico registre un problema que se presente en los activos de tecnología. El técnico registra el incidente. El técnico debe de buscar y registrar la solución de este sistema. Si no encuentran una solución para el incidente, este equipo se devuelve y se retira de la DAC por irreparable.

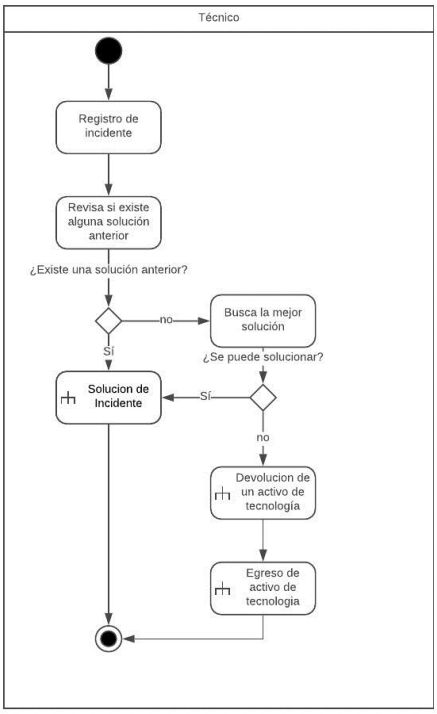


Ilustración 19: Diagrama de actividad de ingreso de un incidente

La solución de incidente es la actividad que se realiza cuando el técnico solucionó el incidente en un activo de tecnología y esta es registrada. Esta solución se somete a una revisión del coordinador para certificar que es la mejor solución, si la solución no es la óptima, se rechaza y se debe de encontrar otra solución.

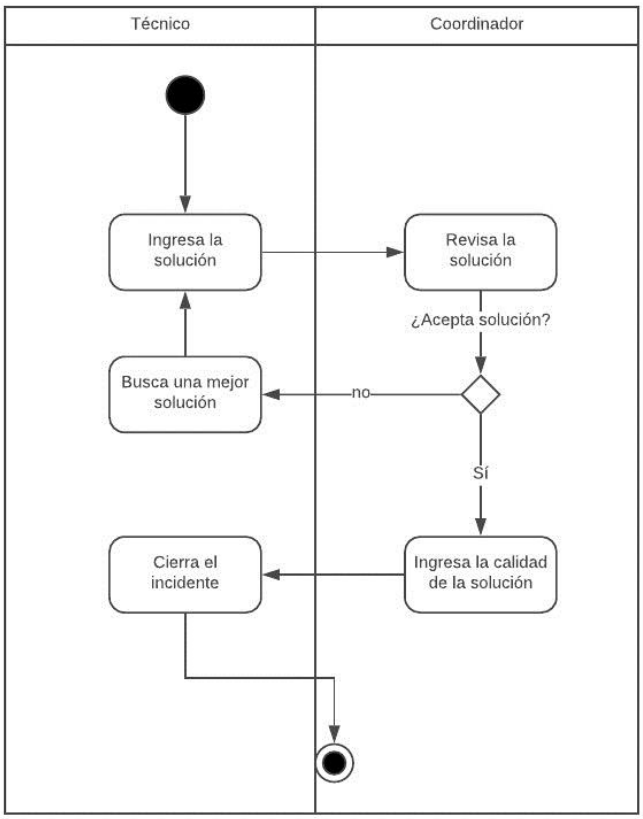


Ilustración 20 Diagrama de actividad de solución de un incidente

Diagrama de Clase

Existen dos diagramas de clases, una muestra la estructura del activo, y la otra muestra la estructura del incidente.

La clase cActivo (c: clase, Activo: activo de tecnología), representa a los activos tecnológicos, tiene un conjunto de atributos y métodos. Los atributos de la clase activo que se declaran con un "_" como prefijo para identificarla como tal son los siguientes:

- _id: es un numero de 12 bytes que se divide en:
    - 4 bytes que representa los segundos desde la media noche UTC del 1 enero de 1970
    - 5 bytes número aleatorio
    - 3 bytes contador que inicia en un numero aleatorio.

  Ej. ObjectId("507f191e810c19729de860ea")
- _fecha_ingreso: es la fecha el cual se ingresó este activo tecnológico. Este es creado en el sistema al momento de registrar el activo.
- _donante: es la institución el cual proviene el activo de tecnología.
- _asignado: es una lista en la cual se encuentran los usuarios que han tenido prestado este activo.
- _fecha_egreso: es la fecha (si tuviera) del egreso del activo.
- _codigo_identificación: es el código que se le da al activo para poder ser leído desde un lector de barras o lector de códigos QR.
- _numero_serie: es el número de serie del fabricante del activo de tecnología.
- _nivel_seguridad: es el nivel de seguridad que se le otorga al activo de tecnología, estos niveles son los siguientes:
    - Baja: Es de libre uso.
    - Media: Es uso exclusivo de la DAC.
    - Alta: Contiene información sensible. Este activo debe de revisarse al entregar y a devolver.
- _codigo_sicoin: es el código que identifica el activo en el sistema sicoin.
- _alias: es un listado de nombres que se le da al activo de tecnología.
- _estado: es el estado del activo de tecnología.

- _ubicacion: es el lugar en el cual está ubicado el activo de tecnología.
- _creado: registra si el activo de tecnología (software) fue creado en la dirección o fue adquirido ya hecho.
- _llave: es la llave del activo de tecnología(software) que se utiliza para la activación.
- _version: es la versión actual del activo de tecnología(software).
- _tipo: es el tipo del activo de tecnología.

Los métodos para la clase cActivo son:

- _actualizarUbicacion(): actualiza la ubicación de un activo, en el atributo
- _asignarActivo(): asigna un activo. Este asigna un id del usuario al cual se le presta el activo de tecnología.
- _crearActivo() : Este método crea el registro en la base de datos, genera un id.
- _devolverActivo(): Este método es utilizado cuando el activo es devuelto.
- _egresarActivo(): Este método se encarga de egresar los activos.
- _eliminarActivo(): Este método elimina el activo. Actualiza el activo
- _generarCodigoQR(): Este método genera o registra el código qr.
- _obtenerActivo(): Obtiene el registro del activo de la base de datos.
- _prestarActivo(): Este método es utilizado cuando se presta un activo.
- _setProblema(): Este método es utilizado cuando se genera un incidente en los activos.
- _solucionarProblema(): Este método es utilizado cuando se soluciona el incidente en los activos.
- _actualizacionVersion(): Actualiza la versión.

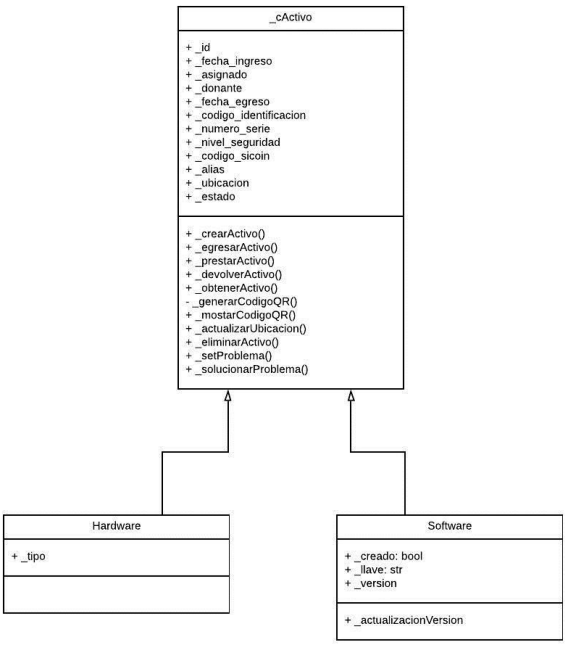


Ilustración 21: Diagrama de clases de activos de tecnología

En los incidentes se tienen dos clases, una representa el incidente cIncidente (c:clase, Incidente). Los atributos de la clase cIncidente que se declaran con un "_" como prefijo para identificarla como tal son los siguientes:

- _id: es el código único que lo identifica en la base de datos.
- _solucion: es el listado de soluciones que tiene el incidente.
- _usuario: es el usuario que reporte el incidente.
- _fecha: es la fecha el cual se registró el incidente.
- _descripcion: es la descripción del incidente.
- _tipo: es el tipo de incidente que se registra.

Sus métodos son:

- _crearIncidente(descr, idActivo): este crea un incidente "descr" en el activo descrito en idActivo
- _cerrarIncidente(idSolucion): este método cierra un incidente colocada en idSolucion.

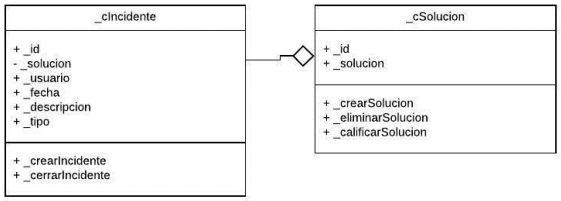


Ilustración 22: Diagrama de clases de incidente

En la clase _cSolucion, este representa las soluciones que se le dan a los incidentes. Los atributos de la clase _cSolucion que se declaran con un "_" como prefijo para identificarla como tal son los siguientes:

- _id: Es el id único que identifica el registro de la solución.
- _solución: Es la solución que se le da al incidente dado.
- _fecha: Fecha en que se creó la solución.

Y sus métodos son:

- _crearSolucion(idIncidente): crea una solución para el incidente identificado con "idIncidente"
- _eliminarSolucion(): elimina la solución.

Diagrama de estados

El objeto activo de tecnología tiene su inicio cuando es creado. Este al ser revisado y autorizado pasa a un estado disponible, el cual el activo está listo para ser prestado o asignado a cualquier usuario.

Cuando este es prestado, el activo pasa a estado Asignado, en este estado ya es posible crear incidente o solucionar los incidentes en los distintos activos. Cuando se registre un incidente sobre el activo, este pasa a un estado de problema, en este estado el activo no se puede devolver.

Cuando se solucione el incidente, el activo pasa a asignado y es posible devolverlo. Para egresar el activo, necesita estar en estado disponible ya que no se puede egresar un activo que este prestado.

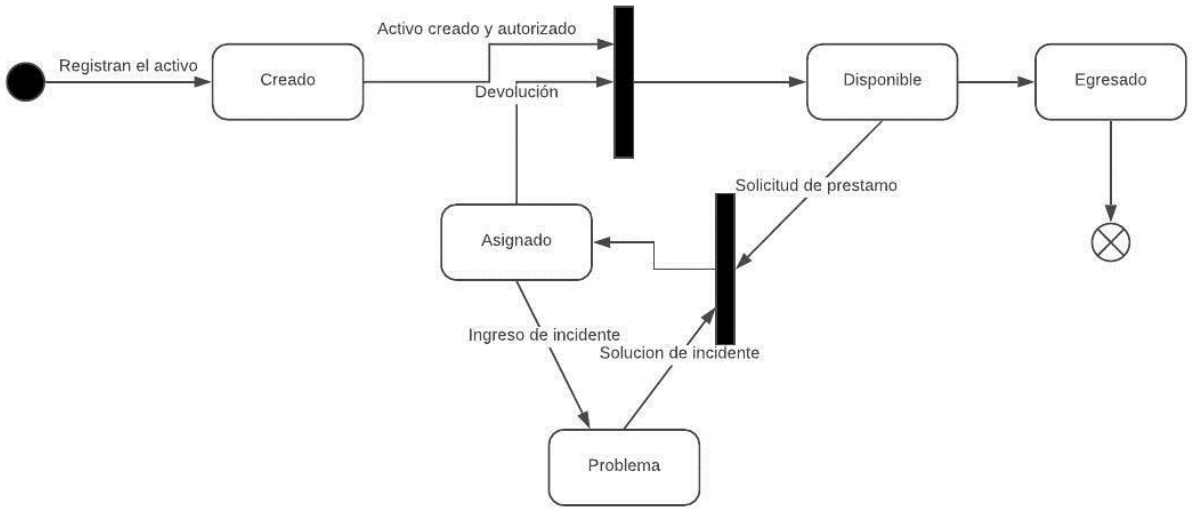


Ilustración 23 Diagrama de estado del objeto activo de tecnología

Diagrama de componentes

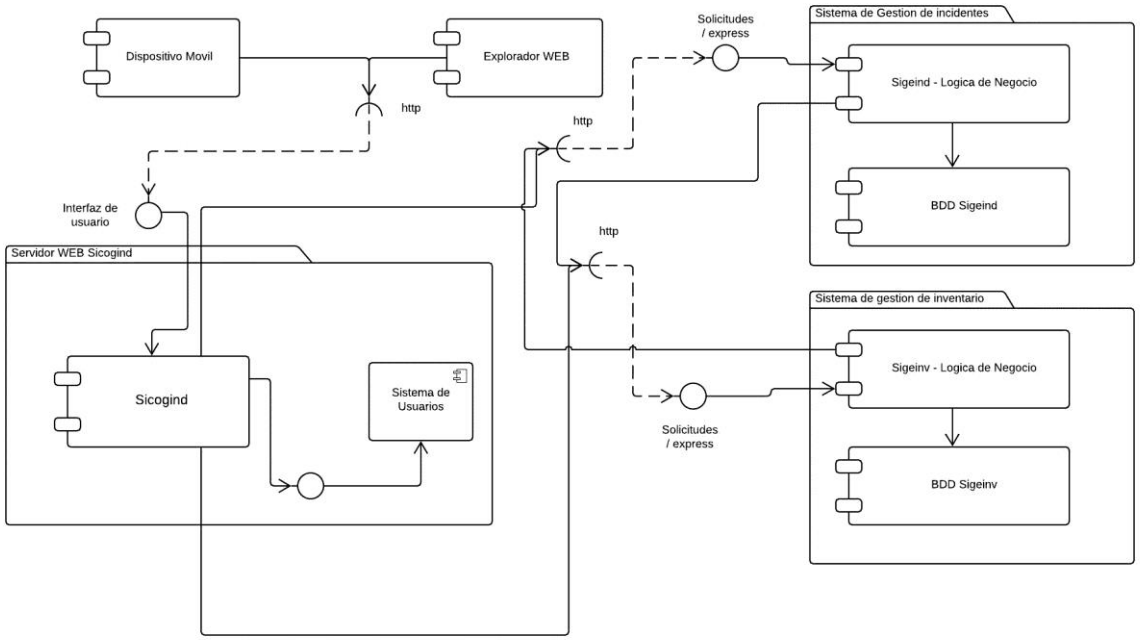


Ilustración 24: Diagrama de componentes

Sistema informático para el control de activos de tecnología y gestión de incidentes para la Dirección de Análisis Criminal tiene 3 componentes:

Sicogind (Sistema informático para el control de activos de tecnología y gestión de incidentes): Es la capa de presentación. Este componente es el encargado de llevar control de los usuarios, sus roles y sus permisos. Este componente está construido utilizando Ionic que es un framework que permite la aplicación web pueda ser interpretado en dispositivo móviles con el sistema operativo de Android o el sistema operativo iOS.

La aplicación web está construida con el framework angular tomando como buenas prácticas la guía de material design. Esta es una guía para crear interfaz de usuario fáciles y agradables para los usuarios.

SigeInv (Sistema de gestión de inventario): Este es el componente que tiene toda la lógica de negocio para el control del inventario de activos de tecnología. Este incluye el control de acceso a la información de la base de datos.

SigeInd (Sistema de gestión de incidentes): este es el componente que tiene toda la lógica de negocio para el control de los incidentes y sus soluciones.

3.2.2 Infraestructura

Estos componentes están creados con nodeJs y la base de datos esta creado con el sistema MongoDB, una base de datos NoSQL. La infraestructura de estos componentes se encapsulará en un contenedor. Este contenedor puede ser utilizado para su implementación en sistemas como MicroK8, Docker o Kubernetes.

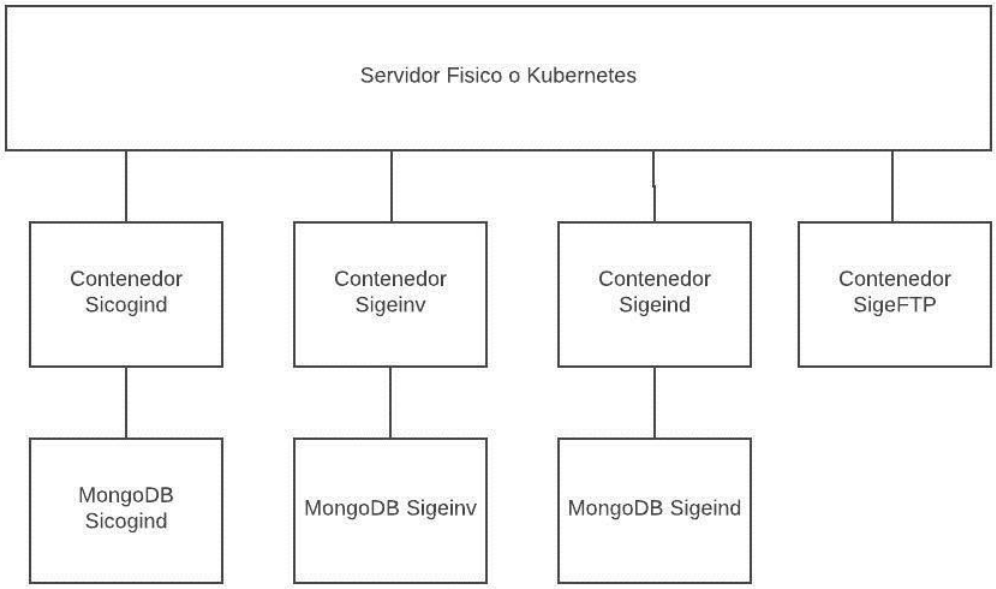


Ilustración 25: Infraestructura de contenedores

Contenedores

Los sistemas se instalarán en los contenedores. Dentro de los contenedores se copiarán los códigos fuentes en el directorio /usr/src/. Los puertos recomendados para exponer en los contenedores son los siguientes:

- **Sicogind:** Puerto 8100
- **Sigeinv:** Puerto: 3000
- **Sigeind:** Puerto: 3002

Los contenedores de los backend se construirán con las imágenes de nodeJS, que son entregados por los creadores de NodeJs.

El contenedor de Ionic/Angular se encapsulará la infraestructura de ionic y se dejará en una carpeta fuera del contendor, en el sistema de archivos para su fácil despliegue.

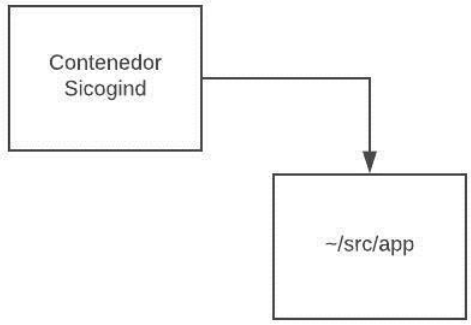


Ilustración 26: Contenedor Sicogind

Contenedores de MongoDB

Los contenedores que contienen encapsulados la infraestructura de las bases de datos de mongoDB son creados con la imagen oficial de mongoDB, el cual se expone el puerto 27017 del contendor. Este puerto no es expuesto en el servidor físico ya que la única manera de interactuar con la base de datos es a través de los distintos sistemas.

La base de datos de sigeind solo puede ser consultada por el contenedor del sigeind. Dando una capa extra de seguridad y así evitar exponer los datos afuera de los servidores.

Los datos persistentes se guardarán en un directorio afuera del contenedor para su fácil manejo y operaciones como el respaldo de la información. Este directorio se llamará Data. Y el contenedor se expondrá ese directorio como el directorio por defecto de mongoDB.

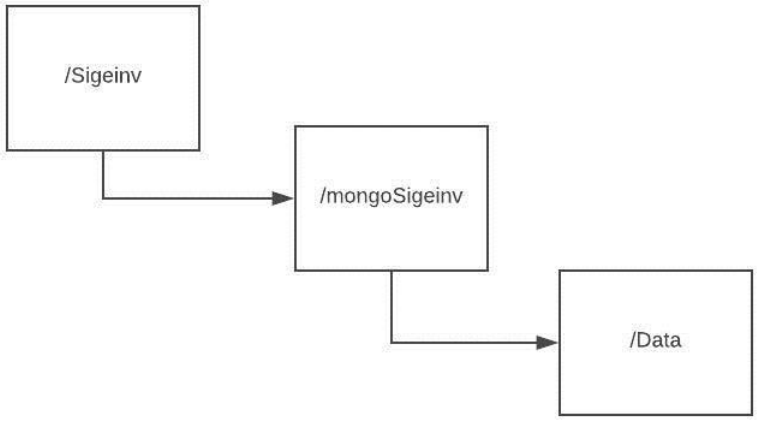


Ilustración 27: Estructura de directorio de los contenedores

3.2.3 Comunicación

La comunicación de estos componentes se hará por el protocolo http que es un protocolo que permite la transferencia de información. La arquitectura de estas comunicaciones se hará a través de REST, es la que más se utiliza en la actualidad y permite la escalabilidad.
El framework utilizado para esta arquitectura es Express. Express permite un conjunto de métodos para el desarrollo del protocolo HTTP.

Estructura de los mensajes

Se creó una estructura de mensajes para que los distintos sistemas puedan entender e interpretar las respuestas de estos. La estructura de los mensajes es:

{

Estatus: <Código de estatus>

, **Mensaje:** Mensaje que se le muestra al usuario

, **Error:** Mensaje (Si existe) de error que devuelven los sistemas.

, **Cuerpo:** Aquí se entregan los resultados solicitados en las peticiones http

}

Estatus

El estatus a diferencia de los códigos de http, nos indica si el usuario tuvo algún éxito o error en la operación en la cual estaban intentando operar. Por ejemplo, si un usuario que no tiene permiso de crear un activo de tecnología quiere crear uno, el código http le devolverá 400, ya que el servidor si operó su petición, pero como su rol no se lo permite el estatus le devolverá error. Los estatus son los siguientes:

- Error: en este estatus la operación que desea hacer no tiene permiso de hacerlo o falta información para hacerlo.
- Éxito: la operación ha sido realizado con éxito.
- Información: la operación se ha realizado con éxito, pero con advertencias.
- Error Aplicación: error fatal de la aplicación que debe ser resuelto de inmediato.

Mensaje

Este es el mensaje que se le muestra al usuario al momento que este haga una operación en los distintos sistemas, por ejemplo “Se ha prestado el activo”. Todos los mensajes para los usuarios deben de ser creados desde los sistemas backend. Los sistemas frontend no genera mensajes al usuario.

Cuerpo

En esta sección de los mensajes se devuelven los datos que solicitan a los distintos mensajes. Por cada operación que pidan, los sistemas solicitantes deben de crear los interfaces que permitan la lectura de la respuesta.

3.2.4 Seguridad

Para la seguridad se contará con autentificación de token. Por cada petición que se haga a los distintos componentes del sistema un token de autentificación deberá de ser proporcionado. La manera de funcionar este token es:

- El usuario envía su usuario/contraseña
- Se valida la autentificación
- Si es exitoso crea un token de autentificación
- Este token se guarda en la sesión del usuario
- En cada petición que haga este usuario envía el token creado
- Los componentes validan los tokens y mandan la respuesta solicitada.

El token debe de ser enviado en las peticiones en la sección header, en el campo de Autentication.

Todos las operaciones y rutas están protegidas con la autentificación del token.

Además de la autentificación de los tokens, las rutas están protegidas por control de roles, para que un usuario no pueda realizar una operación que su rol no lo permita.

Encriptación

La encriptación se hará con el método SHA3-256, es el que se recomienda debido al diseño del algoritmo keccak el cual utiliza una construcción de esponja, esto se refiere a que son absorbidos (transformados con una operación XOR y una función de permutación) y procesados para mostrar la longitud deseada. El SHA3 se convirtió en estándar el 5 de agosto de 2015.

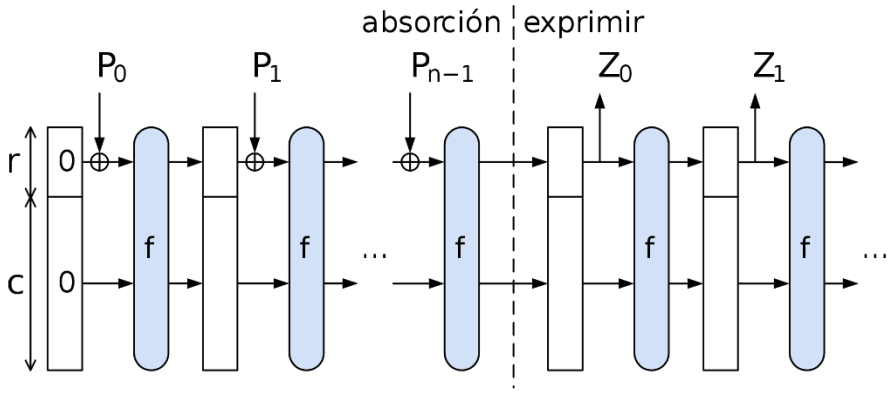


Ilustración 28: Construcción de esponja para funciones HASH (Guido Bertoni J. D., 2019)

El SHA2-256 Y SHA2-512 no se han vulnerado, pero la implementación no es recomendada debido a que estos comparten algoritmos con el SHA1 que fue vulnerado por lo que los ataques a los sha2 ahora son más prácticos.

Ejemplo de una encriptación SHA3, es la palabra “lapicero” se encripta de la siguiente manera: c9157309ee8116207ecacc2a3ddca1de457a66eb6b14f1f6a0febc157d1051121913a76c390e1aec14b5f7b0958cf216086e5d976fcb279470d051a550b7bbc2.

3.2.5 Datos Persistentes

Los datos persistentes del sistema informático para el control de activos de tecnología y gestión de incidentes para la Dirección de Análisis Criminal se guardan en una base de datos NoSQL. El gestor es mongodb y se divide en dos bases de datos.

Sigeind

Esta base de datos tiene todos los datos para gestionar los incidentes, así como los incidentes en sí. La base de datos contiene cuatro colecciones que guardan los distintos datos. Las colecciones son las siguientes:

Tipo_incidente: Este guarda los catálogos de tipo incidentes que se pueden registrar. Su estructura es la siguiente:

Complejidad_incidente: Este guarda el catálogo de la complejidad del incidente

Impacto_incidente: este guarda el catálogo del impacto del negocio que tiene el incidente.

Descripción: String, este atributo da la descripción del incidente

_id: Es la llave que identifica el incidente

activo: int, este atributo tiene un dominio de 0 y 1. Si se encuentra en 0 el incidente no es visible al usuario y si este se encuentra en 1 el incidente es visible al usuario.

Tipo: dice que tipo de incidente es el registrado

Reportado: dice la persona que reporta el incidente.

Impacto: el impacto en el negocio del incidente

Complejidad: dice la complejidad que tiene el incidente

Fecha: fecha del incidente.

Estado: Es el estado del incidente

Resolución: esta colección es la encargada de dar respuesta a los incidentes

Sigeinv

Esta base de datos tiene las colecciones que tiene los datos de los activos de tecnologías en la dirección de análisis criminal.

Donante: es una colección de datos que tiene a todos los donantes de la dirección de análisis criminal.

_id: ObjectId, este el atributo que identifica al donante.

donante: String, este tiene la descripción del donante. Para el listado ver anexo 5.1.

código: es el código que identifica al donante

activo: int, este atributo tiene un dominio de 0 y 1. Si se encuentra en 0 el donante no es visible al usuario y si este se encuentra en 1 el donante no es visible al usuario.

Nivel de seguridad: es el catálogo que tiene los niveles de seguridad de los activos de tecnología.

donante: String, este tiene la descripción el nivel de seguridad. Para el listado ver anexo 5.1.

código: es el código que identifica el nivel de seguridad

activo: int, este atributo tiene un dominio de 0 y 1. Si se encuentra en 0 el nivel de seguridad no es visible al usuario y si este se encuentra en 1 el nivel de seguridad no es visible al usuario.

Tipo_inventario: es una colección que tiene todos los tipos de inventarios que se registran en el sistema

_id: ObjectId, este el atributo que identifica el tipo de inventario.

donante: String, este tiene la descripción el tipo de inventario. Para el listado ver anexo 5.1.

código: es el código que identifica el tipo de inventario

activo: int, este atributo tiene un dominio de 0 y 1. Si se encuentra en 0 el tipo de inventario no es visible al usuario y si este se encuentra en 1 el tipo de inventario no es visible al usuario.

Inventario: es una colección que tiene todos los datos acerca de los activos de tecnología de la dirección de análisis criminal

_id: ObjectId, este el atributo que identifica el inventario.

Donante: es el donante del activo de tecnología.

Código_identificacion: es el código que identifica en la DAC al activo de tecnología.

Numero_serie: es el número de serie del activo de tecnología

Código_sicoin: es el código que provee el sicoin para el activo de tecnología.

Alias: es el sobrenombre el cual se conoce el activo de tecnología.

Observaciones: es las observaciones que se le pone al activo de tecnología.

Tipo_activo: es el tipo de activo de tecnología.

Asignado: es la persona el cual tiene prestado el activo de la tecnología.

Ubicación: es la ubicación física del activo de tecnología

Estado: es el estado del activo de tecnología.

3.2.6 Estructura Código

Backend - NodeJS

Los sistemas que se comunican con los datos persistentes están construidos con la tecnología de NodeJS, el inicio de los sistemas es el archivo **app.js**. Este es archivo que tiene todo el control del negocio. Los directorios que se encuentran son los siguientes:

- Controller: en este directorio se colocan los archivos js, los cuales contienen toda la lógica del sistema.
- Data: en este directorio tiene todos los datos de los catálogos que están en los datos persistentes. Si la base de datos no existe, en este directorio están los datos necesarios para que se inicialicen.
- Model: en este directorio contiene la estructura de los datos persistentes.

Frontend – AngularJs/ionic

En el frontend se tienen dos distintos archivos que son necesarios para una presentación de datos.

Los modelos de datos se nombran como *nombre*.model.ts. Aquí se declaran las clases que contienen los datos que se envían desde el backend.

Los archivos *nombre*.service.ts, contienen el servicio que ayuda a hacer las distintas operaciones en el backend.

Los archivos *nombre*.page, son las páginas de los distintos módulos que están en el sistema. Estos tienen un html, que es la encargada de manejar el DOM y los componentes visuales. Mientras los archivos TS son los encargados de cargar y operar los datos ingresados por parte de los usuarios.

3.2.7 Interfaz de Usuario

La interfaz de usuario está construida de una manera simple. Sin menús desplegados, con botones y pestañas que ayudan la navegación. Se compone tres módulos.

- Login
- Principal
- Reportes

Login

Es el módulo encargado de dar acceso al usuario a los distintos módulos. El usuario provee un usuario y una contraseña. Si es exitoso el sistema le da acceso a la página principal.

Ilustración 29: Pagina de ingreso del sistema

Al ingresar el sistema le entrega un token de autentificación. Este token de autentificación permite autentificarse a todos los demás módulos sin necesidad de ingresar su contraseña de nuevo. El token de autentificación tiene validez de tres horas.

El sistema tiene un control si hay tres intentos fallidos tienen que esperar un minuto para poder volver a intentar.

El token de autentificación se guarda en una variable de sesión el cual se puede consultar con el servicio de aut.service.

Principal

El módulo principal es el controlador de todos los demás módulos. Este protege las direcciones de las distintas páginas para que no puedan ser vistas sin antes ser autentificadas. Si el usuario quiere visitar una página y no se encuentra autentificado. Este la redirige al módulo de login.

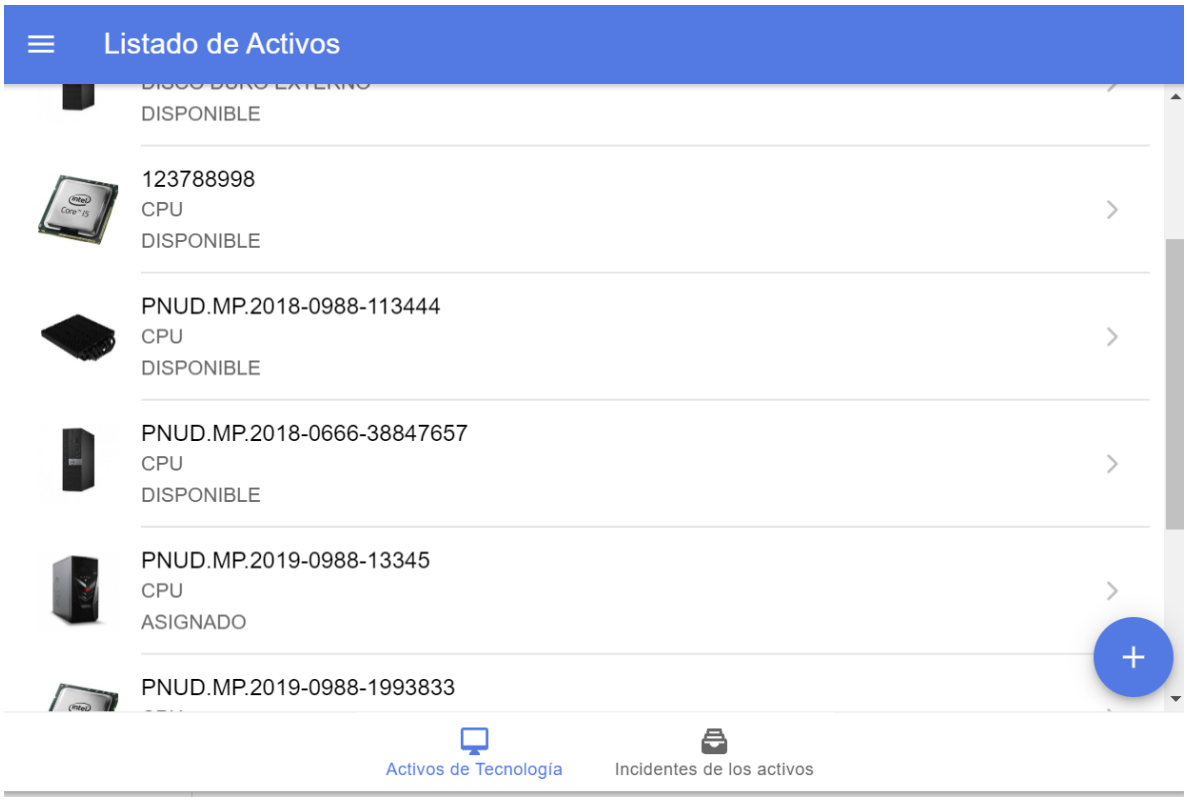


Ilustración 30: Modulo principal

El módulo principal se compone de dos pestañas o submódulos, estos módulos son Activos de Tecnología e Incidentes de los activos.

En la pestaña de activos de tecnología se encuentran todas las operaciones que se pueden hacer en los activos de tecnología. Entre las operaciones que se pueden hacer en esta pestaña son:

- Ver los activos de tecnología
- Crear los activos de tecnología
- Actualizar los activos de tecnología
- Aceptar los activos de tecnología
- Prestar los activos de tecnología
- Devolver los activos de tecnología
- Egresar los activos de tecnología
- Ingresar un incidente en los activos de tecnología
- Resolver los incidentes de los activos de tecnología.

Se puede hacer una búsqueda por cualquiera de los campos de los activos de tecnología. También se puede hacer búsqueda por código QR.

Reportes

En el módulo de reportes se puede generar dos tipos de reportes. El reporte de activos y el reporte de incidentes.

El reporte de activos es el reporte que genera el sistema de los activos de tecnología las cuales están:

- Disponibles: aquellos activos que se pueden prestar.
- Asignado: aquellos activos los cuales están prestados.
- En problemas: aquellos activos los cuales tienen un incidente sin resolver.

El reporte de incidentes genera lo siguiente:

- Listado de incidentes que no tienen solución.
- Listado de incidentes por fechas.

3.2.8 Sistema de archivos

Se utiliza un servidor FTP para guardar las fotos de los activos, para poder obtener estos archivos se utiliza un servicio http, que da la oportunidad de descargar o mostrar los archivos.

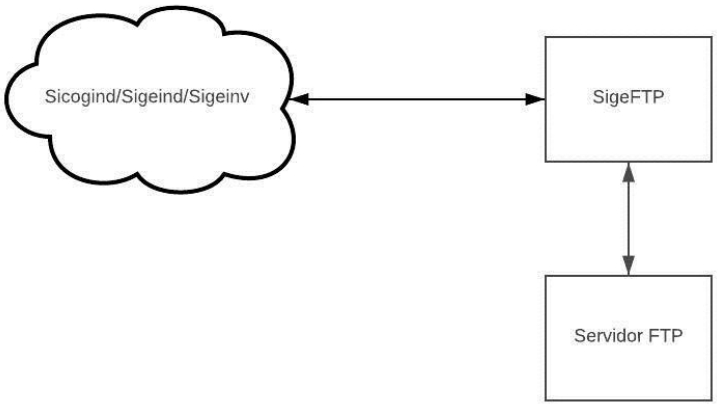


Ilustración 31: modo de acceso a los archivos FTP

3.2.9 Pruebas

FrontEnd

Para las pruebas se utilizará un framework llamado Protactor, este ejecuta una prueba de extremo a extremo utilizando el navegador e interactuando como si un usuario lo haría.

Aquí se realizan pruebas de rol, que revisa la seguridad interna del sistema y verifica que cada rol del sistema tenga acceso a sus operaciones. Y revisa las operaciones que no son permitidas en su rol.

Además, se puede revisar si se tienen excepciones sin ser capturadas o llamadas sin ser registradas.

Backend

Para las pruebas de backend se utiliza el framework Jasmine. Este framework permite hacer pruebas para revisar si el código tiene excepciones sin ser capturadas, errores de seguridad interna. También permite revisar si el flujo de trabajo está trabajando sin ningún problema.

Seguridad

Para las pruebas de seguridad utilizamos OWASP Zed Attack Proxy, esta es una herramienta que permite encontrar vulnerabilidades de seguridad de las aplicaciones. Los pasos que se realiza en las pruebas son las siguientes:

- Evaluación de vulnerabilidad: el sistema es escaneado por problemas de seguridad
- Pruebas de penetración: el sistema es probado con ataques simultáneos.
- Prueba de tiempo de ejecución: el sistema es probado desde el punto de vista de un usuario
- Revisión de código: revisa el código por problemas de seguridad

Los resultados preliminares, en el primer set de pruebas dieron los siguientes resultados:

- El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.
    - **Solución:** Agregar en la cabecera HTTP X-Frame-Options
- El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.

    - **Solución:** X-Content-Type-Options en 'nosniff', en las rutas las cuales los sistemas verifican si el servicio este activo.
- La protección del buscador de web XSS no está disponible, o está deshabilitada por la configuración de la cabecera de respuesta de HTTP 'X-XSS-Protection' en el servidor de web
    - **Solución:** HTTP X-XSS-Protection en '1'

Capítulo 4

Conclusiones y Recomendaciones

4.1 Conclusiones

El Sistema Informático para el Control de Activos de Tecnología y Gestión de Incidentes para la Dirección de Análisis Criminal fue diseñado y desarrollado tomando en cuenta las siguientes características:

- Confidencialidad: el sistema tiene un diseño que permite a los roles tener acceso a determinada información de conformidad con las necesidades y funciones de los mismos, y garantiza que los datos sean accesibles solo a los usuarios que tengan autorización.

- Integridad: el sistema solicita una validación del registro de la información, tanto de los activos como de los incidentes y garantiza que los datos que se ingresan al sistema son correctos.
- Disponibilidad: El sistema está diseñado con una arquitectura portable y escalable, esto permite que si un sistema falla, los otros siguen funcionando, y se reduce el impacto de fallos, proveyendo una alta disponibilidad de los datos cuando estos se necesiten.
- Autenticidad: La arquitectura del sistema provee mecanismo de seguridad y garantiza que los datos guardados son reales y auténticos.

El sistema permite la automatización del ciclo de vida del activo de tecnología en la Dirección de Análisis Criminal, y se registran todos los datos acerca de los estados (creación, asignación, devolución, otros.) con sus debidos controles (usuario registrador y fechas), esto permite generar reportes de una manera rápida y eficiente, además de contar con información actualizada en cualquier momento y abandonar los controles llevados en hojas de papel, así como los que son registradas en hojas de cálculos.

Debido a la integración del sistema de control de incidentes, se tiene mejor control de los activos y se puede indicar qué activos necesitan más atención para corregir sus problemas.

La experiencia del usuario en el sistema fue diseñada de tal manera que ésta sea agradable y sencilla. La curva de aprendizaje para el control del sistema es baja, permitiendo reducir la resistencia al cambio.

4.2 Recomendaciones

- Utilizar un orquestador de contenedores como MicroK8 kubernetes para automatizar la gestión de los mismos, que pueda automatizar la implementación y administración de aplicaciones.
- Utilizar puertos definidos para cada una de las aplicaciones para gestionar el escalado de las aplicaciones de manera ordenada y correcta.
- Incorporar las llaves de seguridad con las de la dirección de análisis criminal para tener seguridad integral.

Base de datos

- Utilizar una política de respaldos para determinar:
    - Inicio del proceso de respaldo
    - Hardware y software que se utilizará
    - Lugar donde se almacenará los datos
    - Recuperación de datos
- Las políticas de respaldo deben de contener toda la información de los aspectos del proceso de respaldo:
    - Tipo de respaldo
    - Frecuencias de respaldo
    - Almacenamiento de los respaldos
    - Seguridad de los respaldos

Manejo de Activos

Se debe utilizar el sistema en todas las operaciones de ingresos de los activos, llevando un registro de todo el hardware y software que ingrese a la Dirección de Análisis Criminal.

Tener un sistema de monitoreo constante de los activos para evitar una desactualización de los datos ingresados en el sistema. La actualización de los datos es responsabilidad directa de los usuarios.

como buena práctica llevar los controles de ISO/IEC 27002:2013 en el apartado de gestión de activos (*ver anexo 5.3*), para optimizar los resultados del sistema y mejorar la gestión de los activos.

Incidentes

Utilizar el sistema de gestión de incidentes para desarrollar diversas formas de registrar los incidentes, que dará facilidad a los usuarios para reportar las fallas y obtener las correcciones de manera rápida.

Capítulo 5

Anexos

5.1 Catálogos

Motivos de egresos

- Obsoleto: cuando el activo de tecnología cumplió su vida útil, debe de ser reemplazado.
- Irreparable: cuando el activo de tecnología no tiene reparación, debe de ser reemplazado.

Motivos de devolución

- Transferencia: cuando un usuario es transferido de un departamento o dirección dentro del Ministerio Publico.
- Finalización: cuando el préstamo tiene un tiempo finito

Tipos de activos de tecnologías

- CPU
- Monitor
- Mouse
- Impresora
- Teclados
- Bocinas
- Audífonos
- Disco duro externo
- Unidad lectora de DVD
- Unidad lectora de Blu-ray
- Switch
- Servidor
- Computadora portátil
- Mochila para computadora portátil
- Memoria Flash

- Proyector
- Software

Tipos de incidente

- Hardware
- Software
- Capacitación
- Inteligencia de negocio
- Felicitación
- Solicitud de instalación.
- Queja

Complejidad del incidente

- Alta
- Media
- Baja

Impacto del negocio

- Alta
- Media
- Baja

Estado del incidente

- Pendiente
- Resuelto
- Reprogramado

Donantes

- Programa de las naciones unidas para el desarrollo
- Agencia de los Estados Unidos para el Desarrollo Internacional
- Agencia canadiense desarrolladora internacional
- Agencia Española de Cooperación Internacional para el Desarrollo

- Ministerio Publico de Guatemala

Nivel de seguridad

- Alta
- Media
- Baja

5.2 Códigos HTTP

- Informativas
    - 100: Puede continuar con las peticiones.
    - 101: Cambio de protocolo ej *http 1.0 a http 1.1*
    - 102: Procesando la petición
    - 103: Reanudación de una petición post o put
- Correctas
    - 200: Petición correcta
    - 201: Petición completada
    - 202: Petición aceptada
    - 203: Petición obtenida de otro servidor
    - 204: Sin contenido
    - 205: Sin contenido, se debe de reiniciar la petición
    - 206: Petición ha sido servido parcialmente
    - 207: Petición en XML
    - 208: Petición notificada anteriormente
- Redirecciones
    - 300: Opciones múltiples de recurso
    - 301: Recuso removidos a otro lugar
    - 302: Encontrado
    - 303: Recurso obtenido desde el método GET
    - 304: Recurso no modificado
    - 305: Recurso con proxy

    - 306: Cambio de proxy
    - 307: Redirección temporal
    - 308: Redirección permanente
- Errores del cliente
    - 400: Mala petición
    - 401: No autorizado
    - 402: Pago requerido
    - 403: Prohibido
    - 404: No encontrado
    - 405: Método no aceptado
    - 406: Respuesta no aceptada
    - 407: Autentificación de proxy requerida
    - 408: Tiempo de petición acabada
    - 409: Petición en conflicto
    - 410: Recurso removido
    - 411: Content-Length falta en el header de la petición
    - 412: Faltan precondiciones de las peticiones
    - 413: Petición muy grande
    - 414: Petición con método GET que debería de ser POST
    - 415: Petición con formato no reconocido
    - 416: Limites petición no reconocidos por el servidor
    - 417: Expect no es encontrado en el header
    - 418: “Soy tetera”
- Errores del servidor
    - 500: Error interno del servidor
    - 501: No implementado
    - 502: Respuesta invalida
    - 503: Servicio no disponible
    - 504: Servidor no obtenido respuesta de otro servidor
    - 505: Http no soportado

- 506: Referencia circular detectada
- 507: Espacio insuficiente
- 508: Bucle infinito detectado
- 509: Limite de ancho de banda excedido

5.3 Objetivos de control y controles de referencia ISO/IEC 27002:2013

Gestión de Activos

- Inventarios de activos: se deben identificar los activos asociados con información e instalaciones de procesamiento de información, debe elaborar y mantener un inventario de estos activos.
- Propiedad de los activos: los activos mantenidos en el inventario deben tener un propietario.
- Uso aceptable de los activos: se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
- Devolución de activos: todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
- Clasificación de la información: la información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
- Etiquetado de la información: se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
- Manejo de activos: se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.

- Gestión de medios removibles: se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
- Disposición de los medios: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.

5.4 Uso del sistema

Inicio de sesión

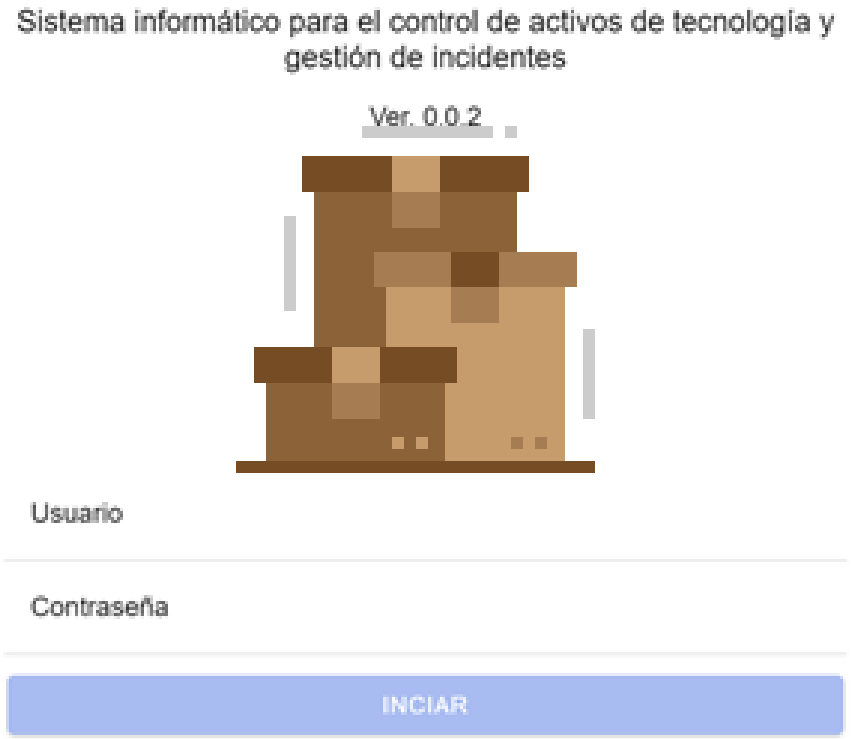


Ilustración 32: Pantalla de inicio de sesión

El inicio de sesión consta del ingreso de un usuario y una contraseña. La administración de estos es llevada por la dirección de análisis criminal. Por parte del sistema lleva las siguientes medidas de seguridad:

- La contraseña no es visible. Esta no es guardada en ningún momento.
- Solo es posible el ingreso de un usuario por sesión de explorador, no es posible que dos usuarios se conecten en un explorador.
- Si existen tres intentos de ingreso con contraseña incorrecta. El sistema bloquea al usuario por un minuto. Durante ese minuto no será posible ingresar o generar tokens en el sistema.

Para la verificación del usuario, el sistema se conecta al sistema de control de usuarios, este es enviado a través de http. Este devuelve tres posibles respuestas con los siguientes estados:

- 400: Es un error general del sistema de autenticación
- 401: El usuario y/o contraseña son invalidas
- 200: Se ha autentificado con éxito

En caso de éxito, el sistema de autentificación devolverá un token de autentificación. Este token es necesario para todas las operaciones del sistema.

Pantalla principal

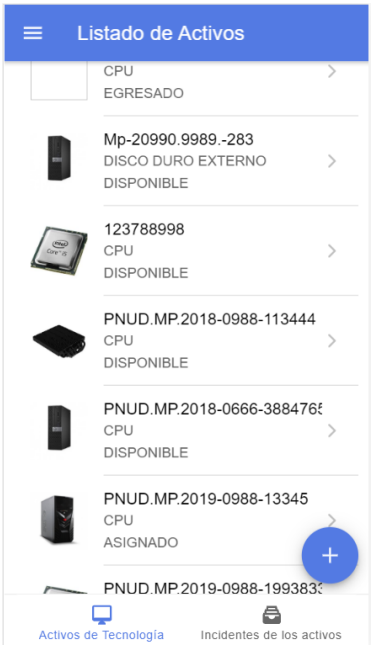


Ilustración 33: Pantalla de inicio

La pantalla de inicio consiste en los siguientes elementos:

- Título: este indica el título de la pestaña el cual esta seleccionado. Estos pueden ser:
  - Listado de activo
  - Listado de incidentes
- Menú en la barra lateral, es aquí donde se encuentran las opciones para el usuario administrador.
- Dos pestañas en la parte inferior, estas pestañas son las siguientes:
  - Activos de tecnología: Son todos los activos tecnología que se encuentran ingresados en el sistema exceptuando aquellos que fueron egresados y rechazados.
  - Incidentes de los activos: Son todos los incidentes que estén asignados al usuario.
- Un botón flotante, donde se puede ingresar un nuevo activo.

Buzón Activos de tecnología

En la pestaña de activos de tecnología, se puede ver un listado completo de todos los activos de tecnología. Desde este listado es factible crear un incidente sobre los activos. Para hacerlo es necesario arrastrar al lado izquierdo el activo y presionar el botón.

Ilustración 34: Creación de un incidente desde el listado de activos de tecnología

Cada activo en el listado tiene los siguientes atributos:

- Código sicoin o Número de serie: si el activo no tiene código sicoin muestra el número de serie.
- Tipo de activo
- Estado del activo
- Foto del activo

Activos de tecnología

Para poder ver el activo de tecnología, es necesario dar click o presionar con el dedo el activo que desea ver, al hacerlo el sistema le mostrara la siguiente pantalla:

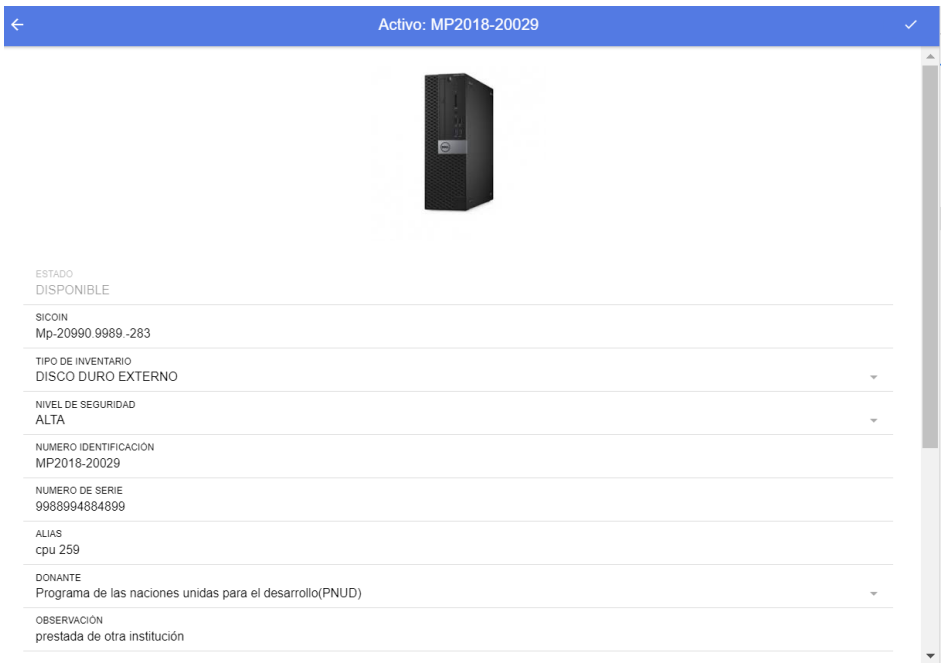


Ilustración 35: Parte superior del detalle de activo

En la parte superior se encuentran tres elementos:

- Botón de atrás: regresa al listado de los activos, **sin guardar ningún cambio**.
- El código de identificación del activo. Este código es generado en la dirección de análisis criminal.
- Botón de aceptar cambios: guarda la información de los distintos campos en parte inferior.

Los campos que se pueden ver y/o modificar son los siguientes:

- Estado: es el estado del activo, este no se puede modificar directamente, sino solo con las operaciones que se describen más adelante.
- SICOIN: Es el código de sicoin otorgado al activo.
- Tipo de inventario: son los tipos de inventarios. Al darle click o presionar este campo saldrá un menú emergente donde se puede escoger el tipo de activo.

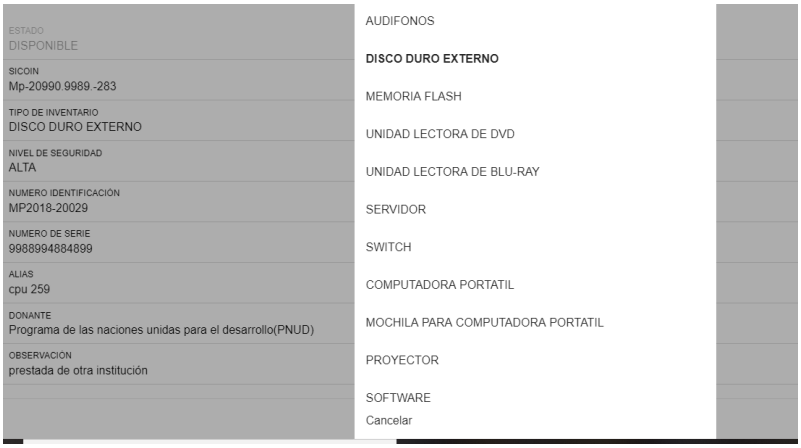


Ilustración 36: Menú de tipo de activo

- Nivel de seguridad: es el nivel de seguridad de la información que maneja el activo.

Ilustración 37: Menú de nivel de seguridad

- Número de identificación: Número de identificación que se le da en la DAC.

- Número de serie: Es el número de serie del activo de tecnología
- Alias: Es un identificador que ayuda en la búsqueda de los activos.
- Donante: es la institución el cual dono el activo de tecnología.

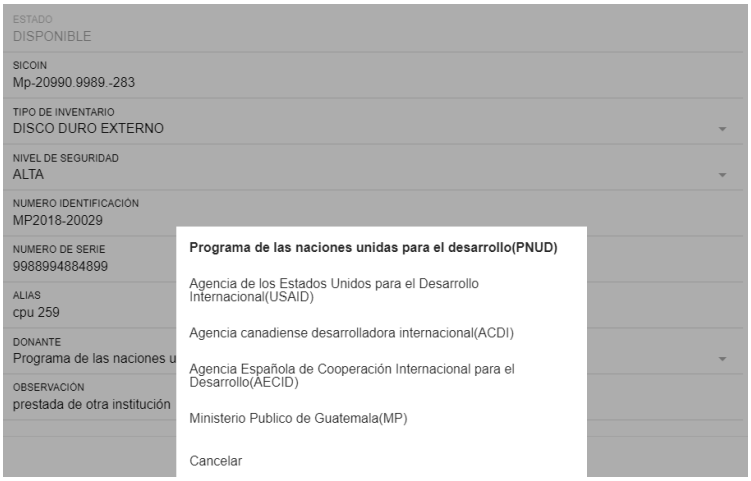


Ilustración 38: Menú de donantes

En la parte inferior de la pantalla se puede modificar la ubicación, agregar los incidentes y hacer todas las operaciones en los activos de tecnología.

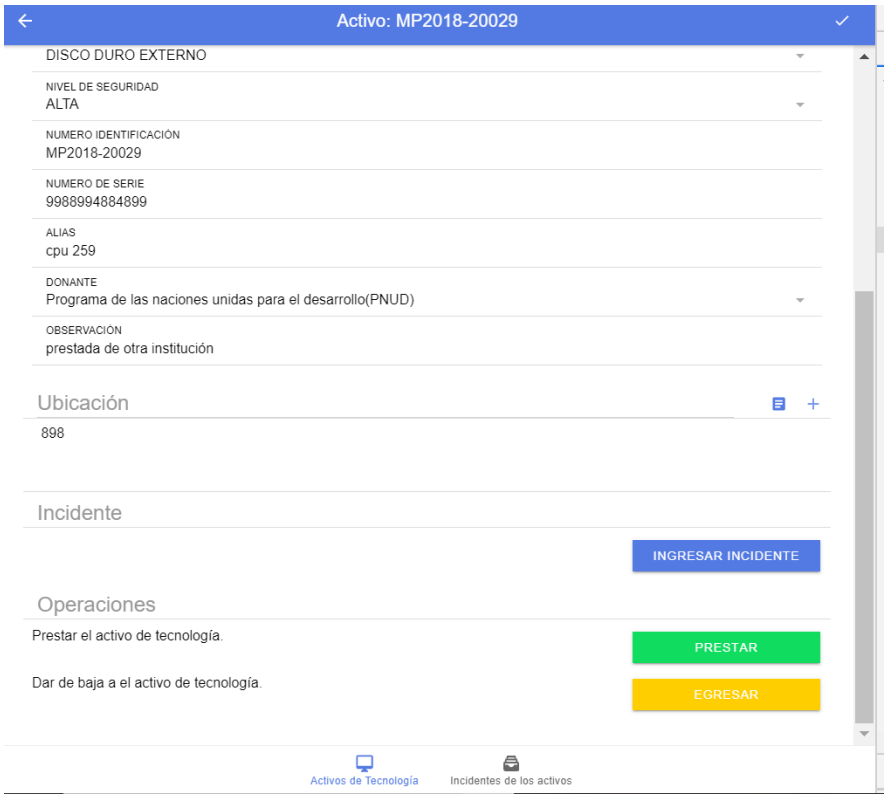
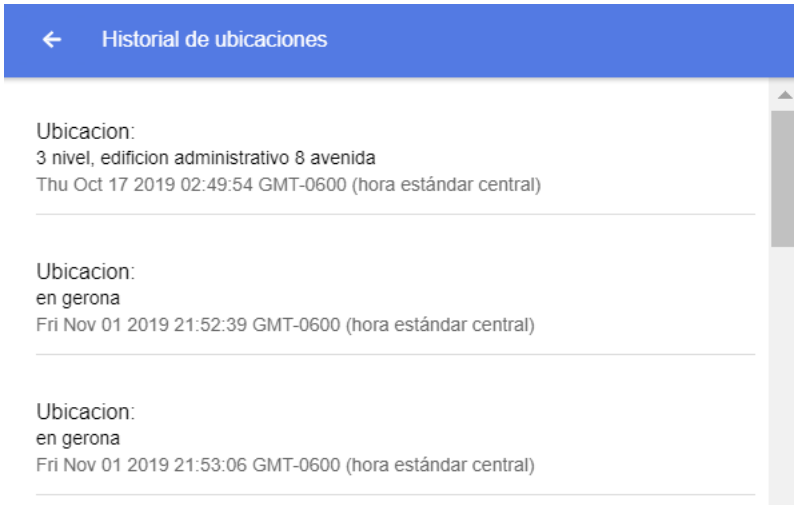


Ilustración 39: Parte inferior del detalle de activo

Para ver el historial de ubicaciones es necesario dar click o presionar el botón .



Cuando el activo de tecnología cambie de ubicación física. Es necesario presionar el botón +, ya que debe tener un listado completo de la ubicación.

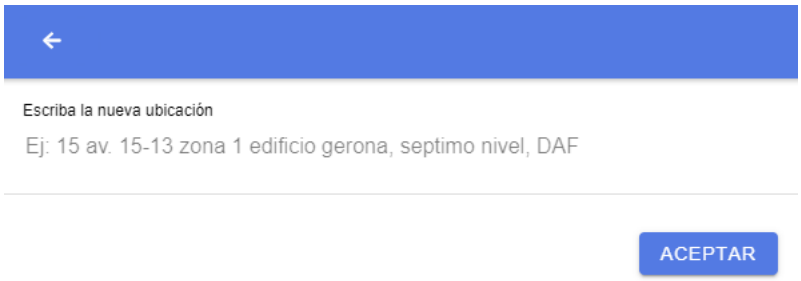


Ilustración 40: Crear una nueva ubicación

Operaciones de los activos de tecnología

Se puede hacer las siguientes operaciones en los activos de tecnología:

- Crear
- Autorizar
- Prestar
- Devolver
- Egresar
- Rechazar

Para crear un activo de tecnología es necesario darle click o presionar el botón flotando que están en la parte inferior derecha de la pantalla:

Ilustración 41: Botón para crear un activo de tecnología

Al presionar este botón aparece la siguiente pantalla:

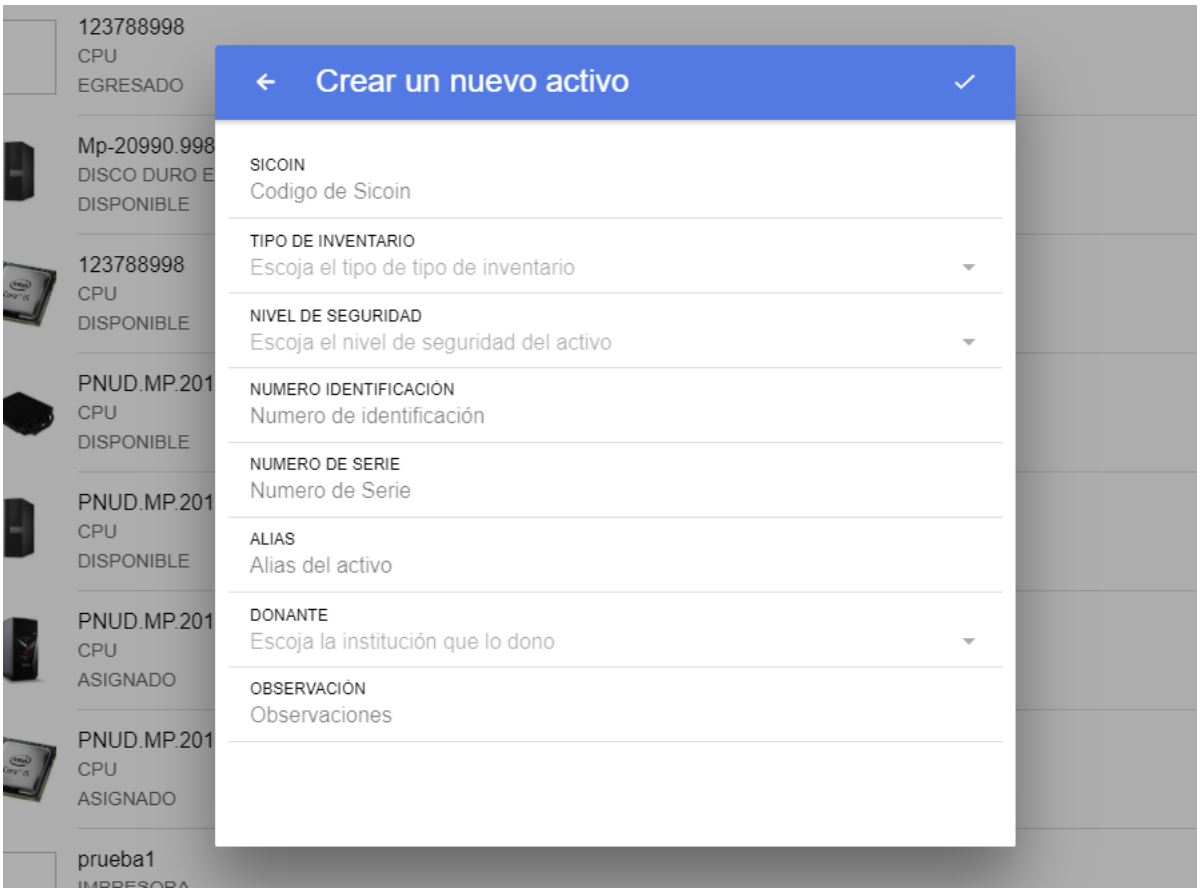


Ilustración 42: Pantalla de creación de activo de tecnología

Donde puede llenar todos los datos que se tengan del activo de tecnología. En la parte superior izquierda está el botón de cancelar, el cual regresa a la pantalla anterior o en la parte superior derecha está el botón que crea el activo de tecnología. Al crear el activo de tecnología tendrá esta pantalla:

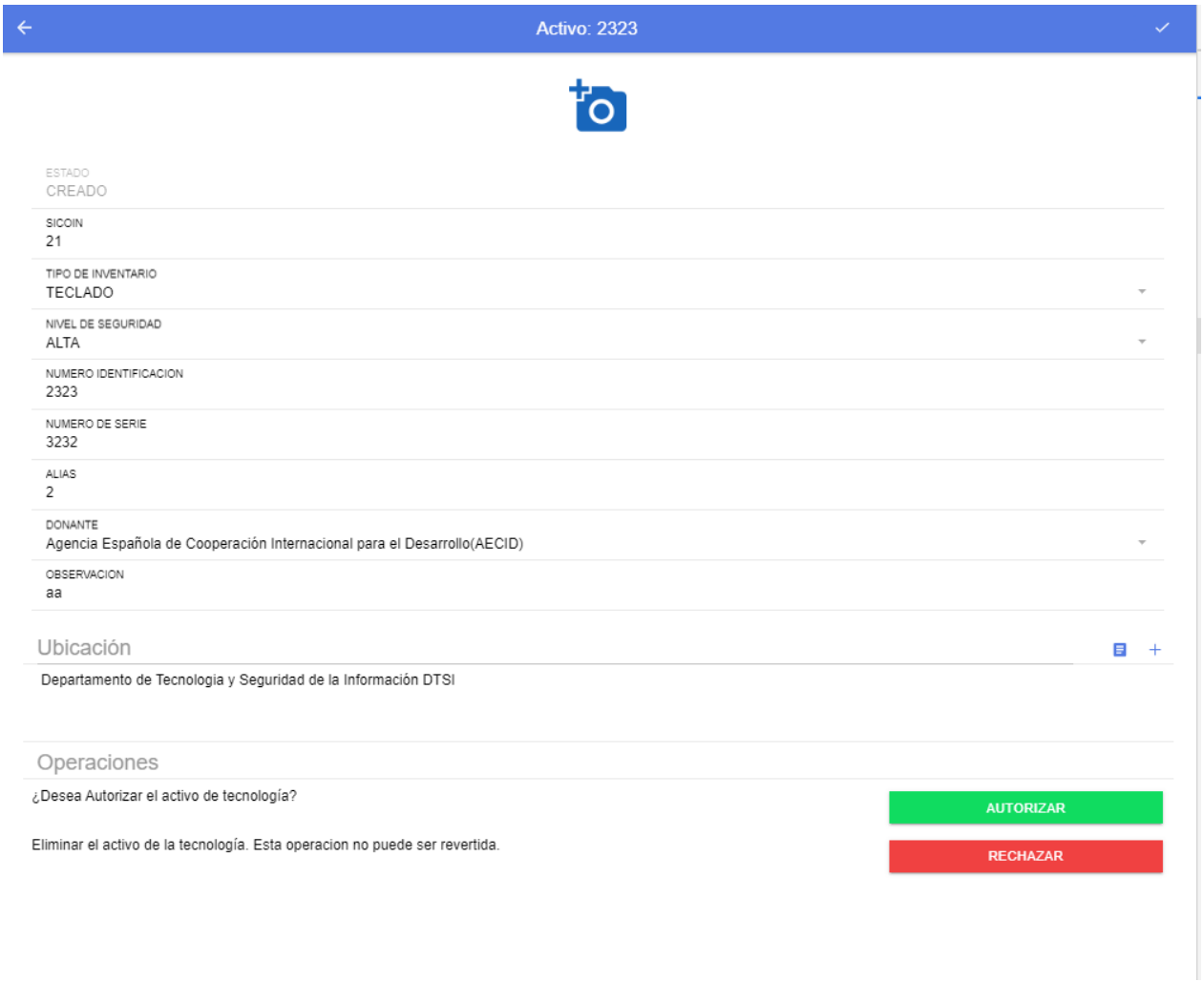


Ilustración 43: Activo recién creado

Cuando el activo este recién creado es necesario autorizarlo. Aquí el coordinador puede autorizar o rechazar el activo de tecnología. Además, al presionar el botón , se puede abrir la cámara (*es necesario dar permiso a la cámara en el dispositivo*) y tomarle una foto al activo de tecnología.

Al rechazar el activo de seguridad, este activo ya no es posible recuperarlo. Al autorizar el activo de tecnología, este pasa a un estado de disponible.

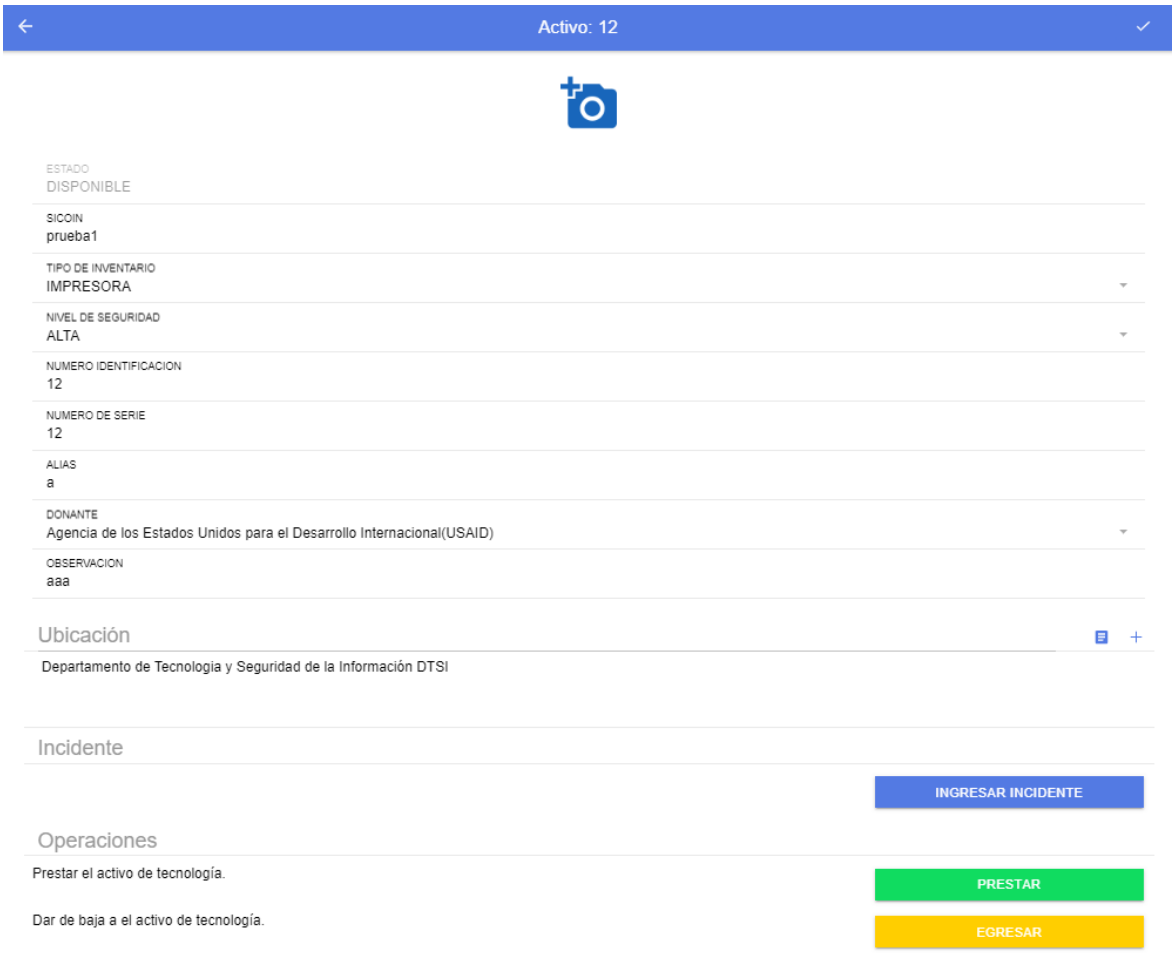


Ilustración 44: Activo en estado de disponible

Al estar en estado disponible, el activo de tecnología ya se le pueden hacer las siguientes operaciones:

- Prestar
- Egresar
- Ingresar un incidente

El egreso de un activo de tecnología consiste en congelar el activo, en ese estado no es posible hacer ninguna operación. Solo un coordinador lo puede regresar a disponible.

Al prestar un activo de tecnología, el sistema le pedirá que escoja a la persona al cual se le prestara este:

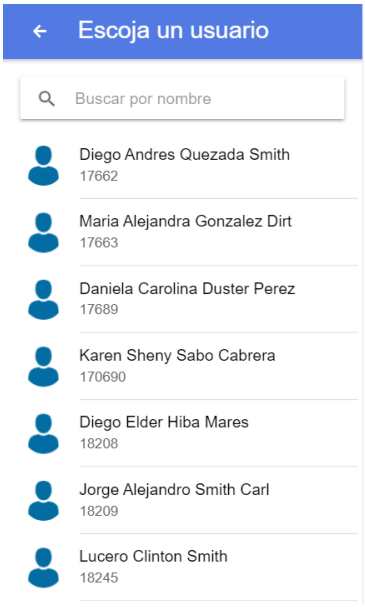


Ilustración 45: Pantalla con listado de usuarios

En esta pantalla se debe hacer una búsqueda por nombres o número de identificación. Es necesario escoger una persona. **No es posible prestar a una persona que no esté ingresado en la base de datos de empleados del ministerio público**.

Al prestar el activo de tecnología, solo se podrá ingresar un incidente o devolver el activo de tecnología:

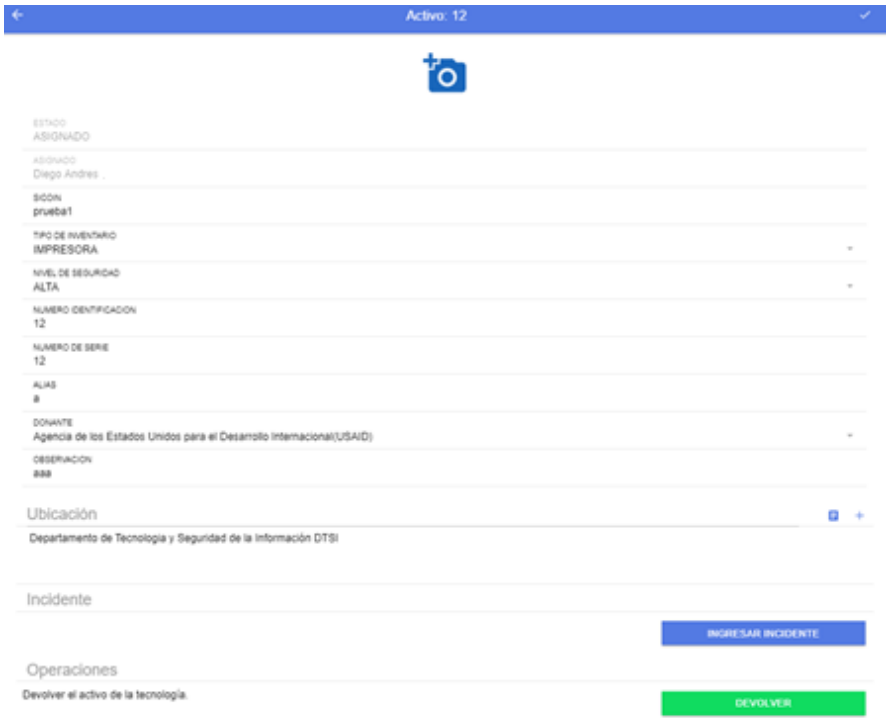


Ilustración 46: Activo Prestado

Al devolver este activo se convierte en disponible, listo para ser prestado de nuevo.

Incidente

Al agregar un incidente al activo de tecnología este pasa a un estado llamado problema, ahí solo es posible resolver el incidente o devolver el activo.

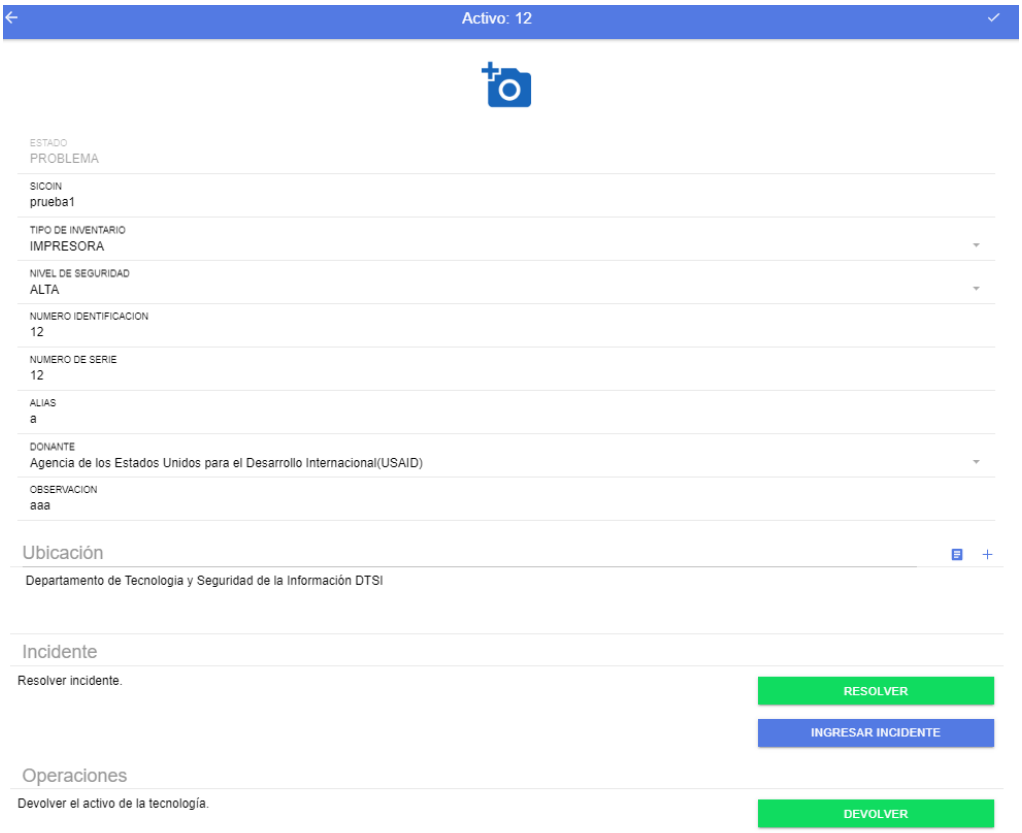


Ilustración 47: Activo en problemas

Al resolver el incidente, el activo vuelve a su estado ya sea asignado o disponible.

Ingreso de incidente

Al darle click o presionar el botón de “INGRESAR INCIDENTE” este abre una ventana donde se puede ingresar un incidente

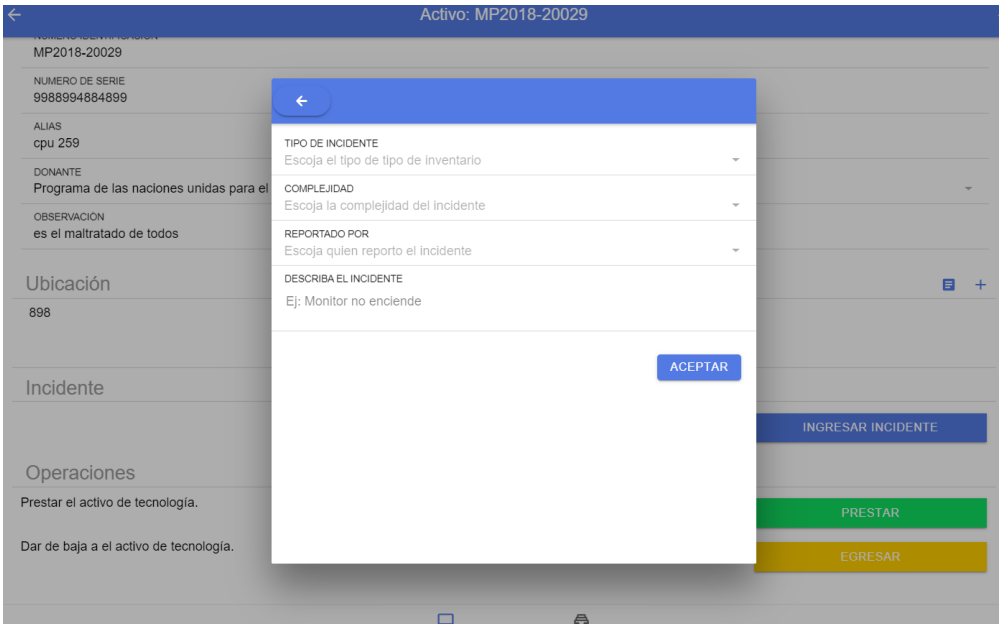


Ilustración 48: Ingreso de un incidente

Aquí puede ingresar los incidentes a los activos de tecnología. Los campos por ingresar son:

- Tipo de incidente
- Adaptabilidad
- Entorno
- Interfaz
- Operativo

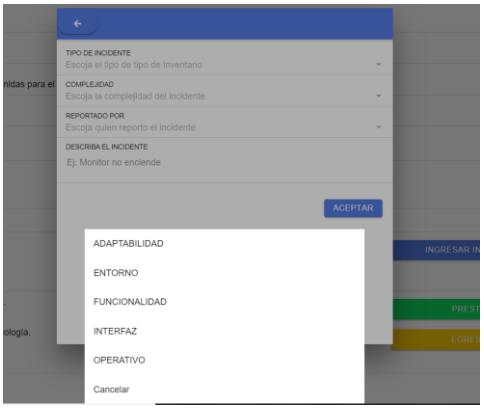


Ilustración 49: Menú tipo de incidentes

- Complejidad: Que tan complejo es la resolución del incidente
  - Alta
  - Baja
  - Media

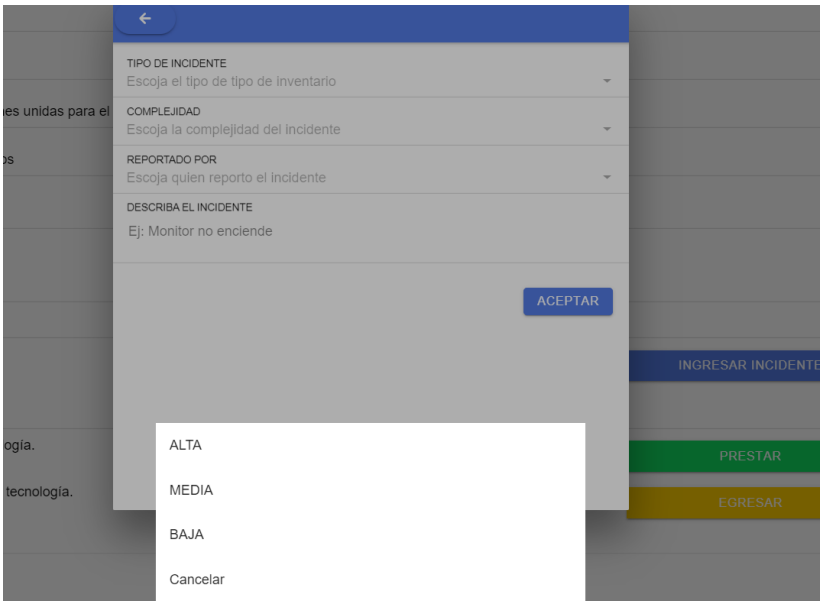


Ilustración 50: Menú de complejidad

- Reportado por: Muestra un menú con todas las personas ingresadas en la base de datos

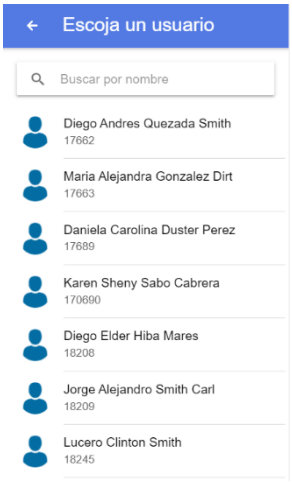


Ilustración 51: Menú de usuarios que reportan el incidente

- Describa el incidente: Es un resumen del incidente

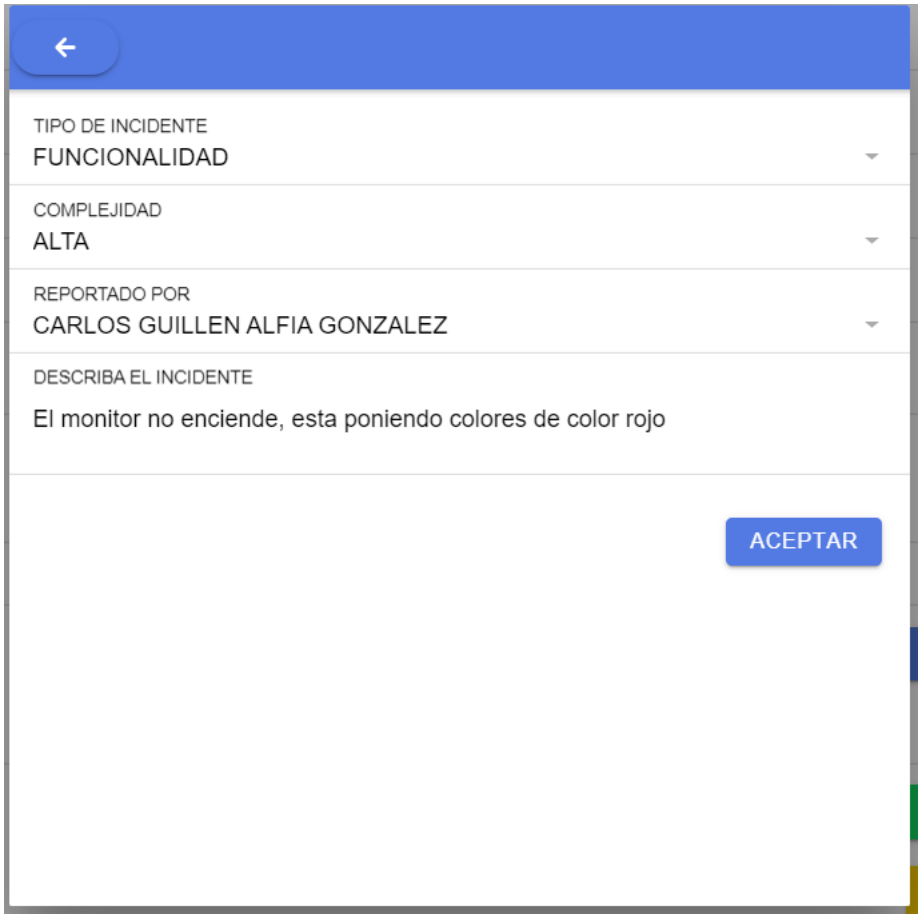


Ilustración 52: Incidente sobre un activo de tecnología

5.5 Seguridad

Comparación entre los algoritmos de encriptación:

Algoritmo	**Salida (bits)**	**Bloque (bits)**	**Operaciones**	**Rendimiento (Skylane)**	**Año**	**Cifrado**
MD5	128	512	And, Xor, Rot, Add ,Or	4.99	1992	32-bit ARX DM

SHA0	160	512	And, Xor, Rot, Add ,Or	3.47	1993	32-bit ARX DM
SHA1	160	512	And, Xor, Rot, Add ,Or	3.47	1995	32-bit ARX DM
SHA2-256	256	512	And, Xor, Rot, Add ,Or, Shr	7.63	2001	32-bit ARX DM
SHA2-512	512	1024	And, Xor, Rot, Add ,Or, Shr	5.06	2001	32-bit ARX DM
SHA3-256	256	1088	And, Xor, Rot, Not	8.59	2015	Keccak sponge

Bibliografía

Diccionario Enciclopédico Vox 1. (2009). Larousse Editorial, S.L.

Express. (s.f.). Obtenido de https://expressjs.com/es/

Foundation, N. (s.f.). *Node JS*. Obtenido de https://nodejs.org/es/.

Google. (2019). *Angular JS*. Obtenido de https://angular.io/.

Guido Bertoni, J. D. (2019). *Keccak specifications*. Obtenido de https://keccak.team/keccak_specs_summary.html

Guido Bertoni, J. D. (2019). *The sponge and duplex constructions*. Obtenido de https://keccak.team/sponge_duplex.html

Ionic. (s.f.). *Ionic Framework*. Obtenido de https://ionicframework.com/.

ISOTools. (s.f.). *Blog especializado en Sistemas de Gestión*. Obtenido de https://www.pmg-ssi.com.

ITIL Incident Management. (s.f.). Obtenido de http://www.itlibrary.org/index.php?page=Incident_Management

Martin Fowler, K. S. (1999). UML Gota a Gota.

MongoDB, I. (s.f.). *MongoDB*. Obtenido de https://www.mongodb.com/es.

OMG. (s.f.). *Unified Modeling Language*. Obtenido de https://www.uml.org/.

Pooley, R. (2002). Utilización de UML en Ingeniería del Software con Objetos y Componentes.

Technology, N. I. (4 de Agosto de 219). *Secure Hash Standard.* Obtenido de https://www.nist.gov/publications/secure-hash-standard