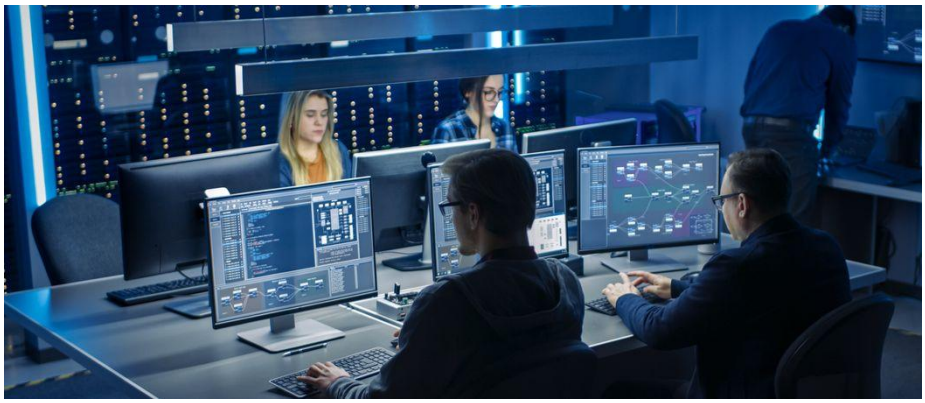
Implementación de herramientas para la gestión de incidentes



Nombre: Andrea Giner Pastor
Profesor: Borja Merino
Fecha de Entrega: 29/01/2025

INDICE

1. Introducción

- Los sistemas de gestión de tickets desempeñan un papel crucial en el soporte empresarial, facilitando una atención al cliente eficiente y organizada. Sin embargo, muchas organizaciones todavía no aprovechan esta herramienta, generalmente debido a una falta de comprensión sobre qué es un sistema de gestión de tickets y cómo puede beneficiar a su negocio. Entre los principales beneficios de implementar un sistema de ticketing destacan los siguientes:

  - Organizar grandes volúmenes de solicitudes a un sistema centralizado.
  - Consolidar Interacciones en un hilo
  - Mantener los estándares de servicio al cliente
  - Mejor comunicación con los clientes
  - Colaboración en equipo fácil y eficiente
  - Procesos automatizados y gestión de cargas de trabajos
  - Mayor eficiencia y productividad de los agentes
  - Seguimiento de valiosas métricas de servicio y KPI[1]
  - Satisfacción del cliente mejorada

- En 2023, el CCN-CERT reportó[2] un notable aumento en los ataques relacionados con el robo de información, tanto en el ámbito del ciberespionaje como del cibercrimen. Este incremento incluyó una proliferación significativa de malware especializado en el robo de datos, conocidos como *infostealers*[3], diseñados para capturar contraseñas y datos de pago, los cuales suelen ser vendidos posteriormente en mercados ilícitos.

- La creciente sofisticación y frecuencia de ciberataques, como los llevados a cabo mediante *infostealers*, resalta la necesidad de que las organizaciones cuenten con herramientas eficaces para gestionar incidentes y proteger la información sensible. En este contexto, los sistemas de gestión de tickets no solo facilitan la atención al cliente, sino que también son fundamentales para organizar y dar seguimiento a los incidentes de seguridad, permitiendo a las empresas responder de manera más ágil y efectiva ante posibles brechas o amenazas.

---

[1] https://rockcontent.com/es/blog/kpis/
[2] https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7188-ccn-cert-ia-35-23-ciberamenazas-y-tendencias-edicion-2023/file.html
[3] https://www.welivesecurity.com/es/seguridad-digital/infostealers-que-hacer-roban-informacion/

2. Resumen Ejecutivo

El objetivo de este trabajo es probar y comprender el funcionamiento de los sistemas de ticketing utilizados por las organizaciones para la gestión de incidentes. En la primera parte, se realiza un análisis del estado del arte de las herramientas de ticketing más comunes en el entorno empresarial, destacando sus características y ventajas en su implementación y uso.

A continuación, se instalará y configurará RTIR (*Request Tracker for Incident Response*)[4], una herramienta *open-source*, con la que se llevará a cabo una prueba de concepto mediante un escenario simulado de incidente. Este ejercicio tiene como finalidad entender cómo se gestionan los incidentes y el flujo de trabajo dentro de las plataformas de ticketing, proporcionando una visión práctica del uso de estas herramientas en situaciones reales.

El trabajo también incluye un análisis sobre las metodologías y competencias de los organismos INCIBE[5], CNPIC[6] y CCN-CERT[7] en la gestión de incidentes de ciberseguridad. Se resalta la importancia de contar con herramientas de ticketing eficientes para facilitar la colaboración, el seguimiento y la resolución de incidentes en tiempo y forma, asegurando así la respuesta adecuada ante posibles amenazas.

[4] https://bestpractical.com/rtir
[5] https://www.incibe.es/
[6] https://cnpic.interior.gob.es/
[7] https://www.ccn-cert.cni.es/es/

3. Sistemas de Ticketing

3.1¿Qué es un ticket?

Un ticket en el contexto de ciberseguridad hace referencia a un registro digital diseñado para documentar y gestionar incidentes de seguridad informática de manera estructurada. Este registro permite centralizar información relevante, facilitando su seguimiento, análisis y resolución. Entre la información que contiene un ticket puede encontrarse:

- Descripción detallada del incidente. Qué sucedió exactamente, cuándo y dónde.
- Nivel de Gravedad. ¿Es una amenaza critica, alta, media o baja?
- Agente Afectado. ¿Qué sistema o usuario fue el objetivo del ataque?
- Acciones tomadas. Que se hizo para resolver el problema y mitigar el riesgo.
- Estado del ticket. Abierto, en progreso, resuelto, etc...

¿Por qué son de gran utilidad a la hora de gestionar ciberataques?

1. ***Rastrear Incidentes:*** para gestionar y resolver problemas de manera eficiente. Al crear un ticket se genera un identificador único que permite rastrear el incidente desde su inicio hasta su resolución. Estos sistemas permiten documentar detalles del incidente, asignar responsabilidades y coordinar acciones de seguimiento.

2. **Asignar Responsabilidades:** para asegurar que cada incidente sea gestionado eficazmente por la persona o equipo adecuado. Este proceso garantiza que las tareas se completen de manera oportuna y eficiente, mejorando la satisfacción del cliente y la productividad del equipo.

3. ***Priorizar acciones:*** para gestionar eficientemente los recursos y asegurar que los problemas más críticos se aborden de inmediato. Al establecer prioridades, se pueden asignar recursos adecuados a incidentes de alta gravedad, mejorando los tiempos de respuesta y la satisfacción del cliente. La priorización también ayuda a organizar el flujo de trabajo, asegurando que los incidentes urgentes no se pierdan y que las expectativas del cliente se gestionen adecuadamente.

4. ***Mejora la respuesta a incidentes:*** Estos sistemas permiten asignar prioridades y responsabilidades, asegurando que los incidentes críticos sean atendidos rápidamente por el personal adecuado. Además, proporcionan un historial detallado de las interacciones y acciones tomadas, lo que ayuda a coordinar esfuerzos y mejorar la eficiencia en la gestión de incidentes.

5. ***Cumplir con regulaciones:*** los tickets ayudan a cumplir con las regulaciones al proporcionar un sistema estructurado para documentar y gestionar incidentes, lo cual es crucial para cumplir con las leyes como el RGPD y la ley de Ciberseguridad. Estas normativas requieren notificar a las autoridades sobre incidentes significativos y mantener registros detallados de las acciones tomadas.

3.2¿Qué es una herramienta de gestión de tickets?

El sistema de seguimiento de tickets es un software utilizado por el equipo de soporte de las empresas para gestionar y responder de manera rápida y eficiente a los problemas de los clientes.

También conocido como "*Issue Tracking System"* en inglés, el sistema crea un ticket de soporte para cada problema, pregunta, queja o pedido reportado al equipo de atención.

En general, un sistema de seguimiento de tickets permite organizar el flujo de trabajo del departamento de atención al cliente, desde la recepción de una solicitud hasta su finalización.

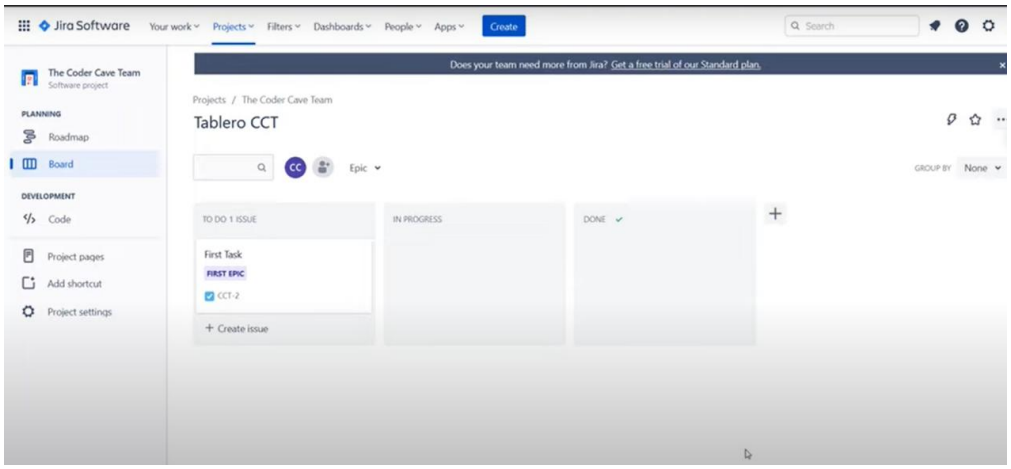
- Ventajas de un Sistema de Tickets:

1. Mejora la eficiencia y productividad en la gestión de incidentes de seguridad, permitiendo una respuesta más rápida y organizada.
2. Proporciona un mayor control y seguimiento de las solicitudes relacionadas con problemas de seguridad, lo que facilita la priorización y resolución de incidentes críticos.
3. Centraliza la gestión de incidentes de seguridad, lo que mejora la organización y reduce la perdida de información importante.
4. Facilita la colaboración y comunicación entre los miembros del equipo de seguridad, permitiendo una resolución más eficaz de los problemas.

5. Ofrece características de seguridad avanzadas, como la generación de códigos únicos, lo que ayuda a prevenir fraudes y garantiza que solo el personal autorizado acceda a la información.
6. Automatiza procesos, lo que reduce los costos operativos y ahorra tiempo, permitiendo que el personal de seguridad se enfoque en tareas más críticas.
7. Mejora la experiencia del usuario final al proporcionar un proceso más ágil para reportar y dar seguimiento a problemas de seguridad.
8. Facilita el cumplimiento de normativas de seguridad al mantener un registro detallado de todos los incidentes y acciones tomadas.
9. Permite una gestión centralizada del inventario de problemas de seguridad, lo que ayuda a optimizar los recursos y priorizar las acciones de mitigación.

4. Estado del Arte

✧ **Jira:** Es una potente herramienta de gestión de proyectos desarrollada por Altassian[8], diseñada principalmente para equipos de desarrollo de software que trabajan con metodologías ágiles como scrum[9] y Kanban[10].

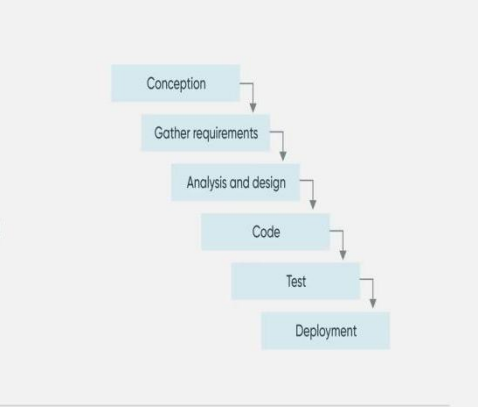


➢ Metodologías Ágiles: Son estructuras de trabajo para la gestión de proyectos en las que los proyectos se dividen en muchas fases dinámicas, normalmente conocidas como "*sprints*". Después de cada *sprint*[11], los equipos reflexionan y observan lo que ha sucedido.

➢ Tipos de metodologías *agile*:

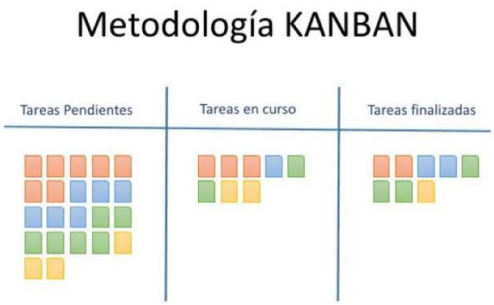
[8] https://www.atlassian.com/es
[9] https://www.atlassian.com/es/agile/scrum
[10] https://asana.com/es/resources/what-is-kanban
[11] https://www.atlassian.com/es/agile/scrum/sprints

- Cascada:[12] Es una metodología lineal y secuencial que divide el ciclo de vida del desarrollo software en fases distintas en las que la siguiente fase solamente puede producirse si se ha completado la fase anterior.



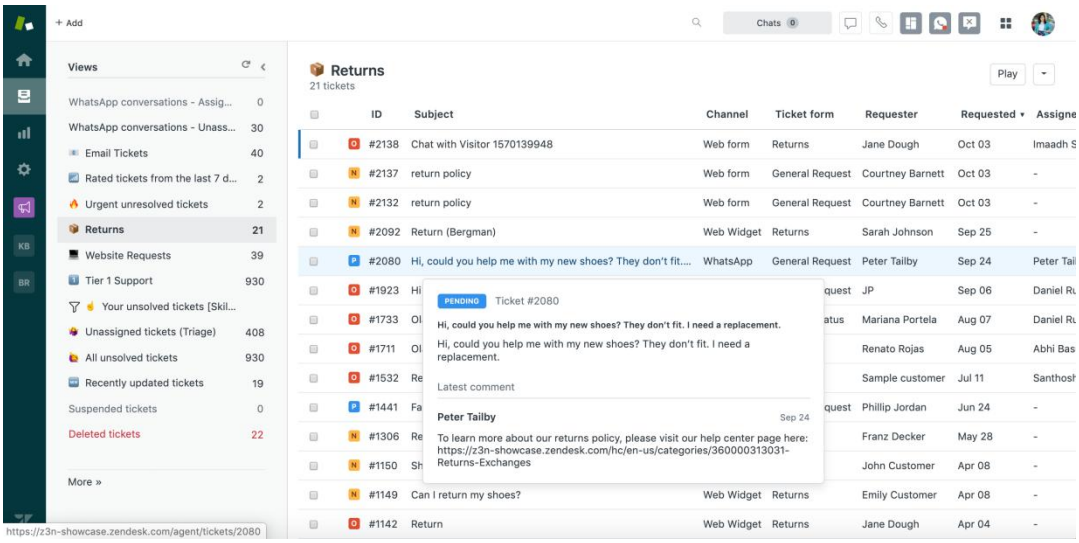
- Scrum:[13] Proceso para llevar a cabo un conjunto de tareas de forma regular con el objetivo principal de trabajar de manera colaborativa.

- Kanban: Se trata de un método visual de gestión de proyectos que permite a los equipos visualizar sus flujos de trabajo y la carga de trabajo.

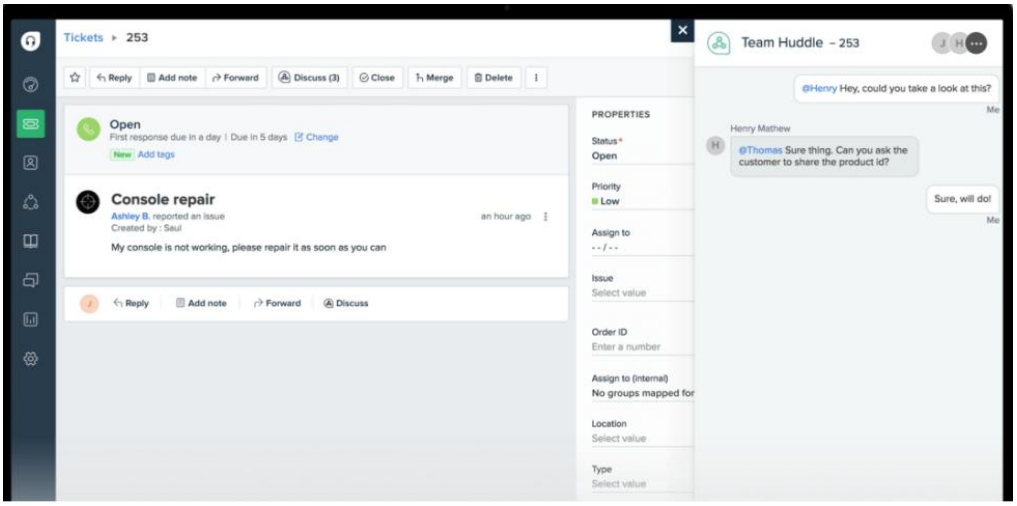


✧ **Zendesk:**[14] Es una plataforma de atención al cliente en la nube que permite a las empresas gestionar sus interacciones con los clientes de manera eficiente. Su objetivo principal es centralizar y optimizar la comunicación a través de múltiples canales, como correo electrónico, chat, redes sociales y teléfono.

[12] https://www.servicenow.com/es/products/strategic-portfolio-management/what-is-agile-vs-waterfall.html
[13] https://donetonic.com/es/agile-y-scrum/
[14] https://www.astroline.com/blog/que-es-zendesk-revision-funcionalidades-y-beneficios

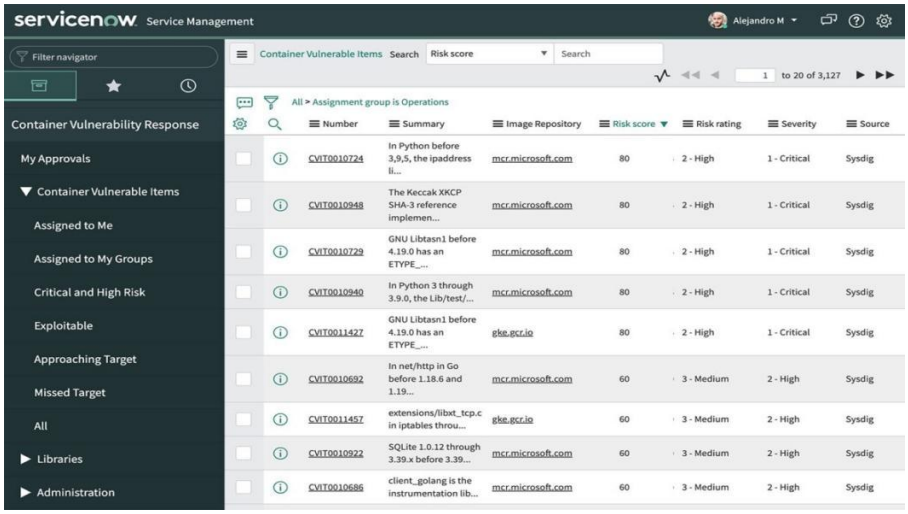


✧ **Freshdesk:**[15] Es un software de atención al cliente basado en la nube diseñado para optimizar la gestión de soporte técnico en organizaciones.

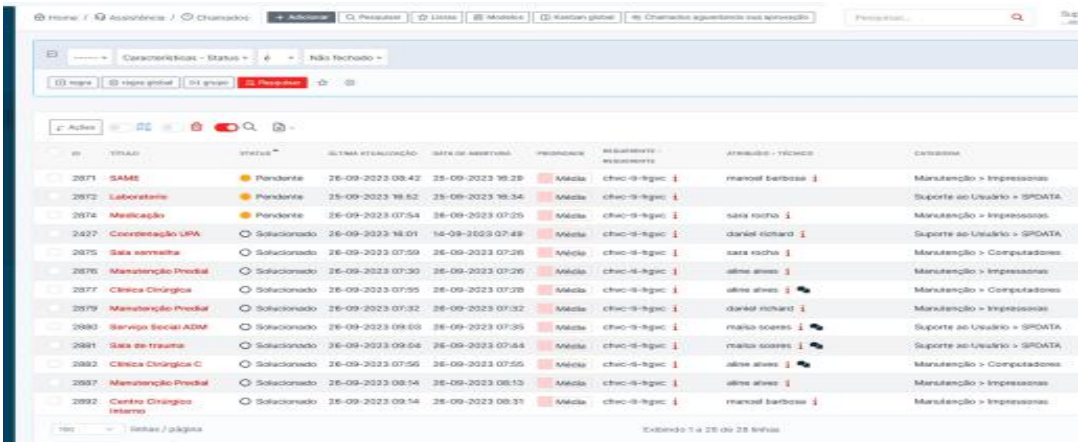


✧ **Servicie-Now**[16]**:** Es una plataforma en la nube diseñada para gestionar y automatizar servicios empresariales. Ofrece herramientas para la gestión de incidentes, problemas, cambios, activos y solicitudes de servicio, entre otros. Su objetivo es mejorar la eficiencia operativa, reducir costos y optimizar la experiencia del usuario mediante la automatización de flujos y el análisis de datos en tiempo real.

[15] https://www.freshworks.com/es/freshdesk/software-de-atencion-al-cliente/
[16] https://blog.invgate.com/es/alternativa-a-servicenow



✧ **GLPI:**[17] Es un software de gestión de servicios de TI de código abierto que permite a las organizaciones gestionar sus activos informáticos y servicios de soporte. GLPI ayuda a centralizar la información, automatizar tareas y mejorar la eficiencia operativa, siendo personalizable y adecuado para diferentes tamaños de empresas.



[17] https://es.fiverr.com/danielrich66/setup-upgrade-or-troubleshooting-your-glpi-ticket-system

5. RTIR

5.1 Que es RTIR y cuáles son sus ventajas

RTIR, o "*Request Tracker for Incident Response*", es una herramienta de gestión de incidentes de **código abierto** diseñada específicamente para equipos de seguridad informática, como CERT (***Computer Emergency Response Team***) y CSIRT (***Computer Security Incident Response Team***). Esta herramienta se utiliza ampliamente en la industria de la Ciberseguridad para ayudar a los expertos a gestionar eficazmente los incidentes de seguridad.

El uso de RTIR en Ciberseguridad ofrece numerosas ventajas para la gestión eficaz de incidentes de seguridad. Algunas de las principales ventajas son:

- ***Gestión estructurada de Incidentes:*** Proporciona un flujo de trabajo predefinido que abarca la detección, análisis, contención y recuperación de Incidentes de Seguridad.

- ***Centralización de la información:*** Permite mantener todos los datos relacionados con un incidente en un solo lugar, facilitando el seguimiento y la colaboración entre los miembros del equipo.

- ***Mejora en la comunicación:*** Ofrece herramientas para gestionar la comunicación con múltiples partes interesadas, incluyendo reporteros, equipos de seguridad, colaboradores y equipo interno.

- ***Automatización de procesos:*** Puede aceptar automáticamente datos de sistemas externos como *splunk*, *ArcSight*, y Nagios, lo que agiliza la recopilación de información.

- ***Personalización Flexible:*** Se puede adaptar a las necesidades específicas de cada organización, permitiendo la adición de campos personalizados y la modificación de flujos de trabajo.

- ***Generación de Informes:*** Facilita la creación de informes de actividad en varios formatos, lo que es crucial para el análisis posterior y la mejora continua.

- ***Correlación de datos:*** Proporciona herramientas para correlacionar información clave de múltiples reportes de incidentes, ayudando a identificar patrones y causas comunes.

- ***Cumplimiento de SLAs:*** Permite el seguimiento de fechas clave para cumplir con los acuerdos de nivel de servicio.

- ***Integración con otras herramientas:*** RTIR se puede integrar con otras herramientas de seguridad, mejorando la eficacia general de la respuesta a incidentes.

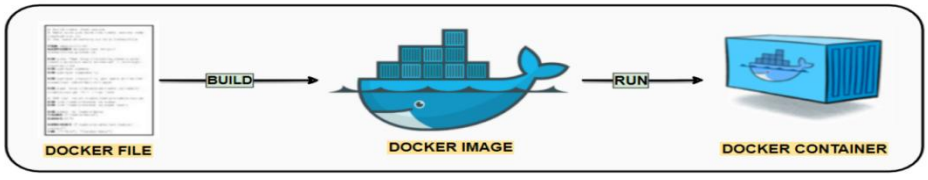
Mejora en la visibilidad: Ofrece un panel de control dedicado a incidentes con listados predefinidos de los tickets más urgentes, proporcionando una visión general rápida de la situación actual.

5.2 Instalación de RTIR (Docker)

- ¿Qué es un Docker[18]?

Es una plataforma de código abierto que permite a los desarrolladores crear, implementar, ejecutar, actualizar y gestionar aplicaciones en contenedores.

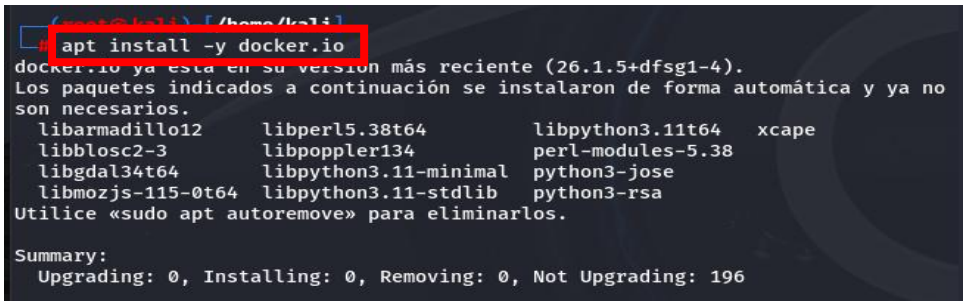
Los contenedores son componentes estandarizados y ejecutables que combinan el código fuente de la aplicación con las bibliotecas del sistema operativo (SO) y las dependencias necesarias para ejecutar ese código en cualquier entorno. Los contenedores simplifican el desarrollo y la entrega de aplicaciones distribuidas, se han hecho cada vez más populares a medida que las organizaciones pasan al desarrollo nativo de la nube y a los entornos híbridos multinube.



[18] https://www.ibm.com/es-es/topics/docker

5.1 Instalación docker

El siguiente comando instala Docker en un sistema Linux (KALI) utilizando el gestor de paquetes APT.



1. El Comando ***apt install*** es el comando para instalar paquetes en sistemas basados en Debian,como Ubuntu.

2. El comando ***-y*** es una opción que responde automáticamente si a todas las preguntas durante la instalación, permitiendo una instalación no interactiva.

3. El comando ***docker.io*** es el nombre del paquete de docker mantenido por Ubuntu.

Al ejecutar este comando, el sistema realizará las siguientes acciones:

1. Descargará el paquete ***docker.io*** y sus dependencias de los repositorios configurados.

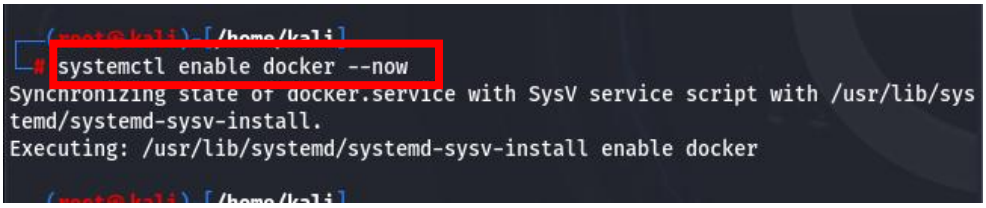
2. Instalará docker y todos los componentes necesarios en el sistema.

3. Configurará docker para que se inicie automáticamente al arrancar el sistema.

Nota: la decisión de haber utilizado Docker se debe a la complejidad inherente de realizar una instalación manual de RTIR, dado el elevado número de paquetes y dependencias[19] que este sistema requiere.

[19] https://rt-wiki.bestpractical.com/wiki/RTIRInstallation

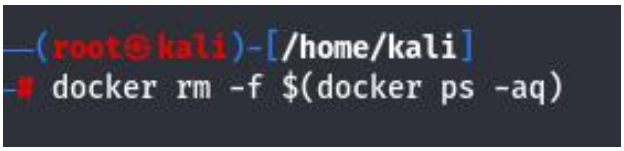
El comando ***systemctl enable --now*** en la terminal de Linux realiza 2 acciones importantes relacionadas con el servicio docker.



1. **Habilita el servicio docker**. Configura Docker para que se inice automáticamente cada vez que el sistema arranque. Esto se logra creando los enlaces simbólicos necesarios en los directorios de inicio de systemd.

2. **Inicia el servicio docker inmediatamente*:*** La opción ***--now*** inicia el servicio Docker en el momento de la ejecución del comando, sin necesidad de ejecutar un comando adicional como sudo systemctl start docker.

Durante las pruebas realizadas en los cuales había problemas con el Docker se ha ejecutado el siguiente comando: ***docker rm -f $(docker ps -aq)*** para eliminar forzosamente todos los contenedores.



1. Docker rm: Este es el comando base para eliminar contenedores docker.
2. -f: Es una opción que fuerza la eliminación de los contenedores, incluso si estan en ejecución.
3. $ (docker ps -aq): Esta parte es una sustitución de comando que genera una lista de todos los IDS de contenedores:

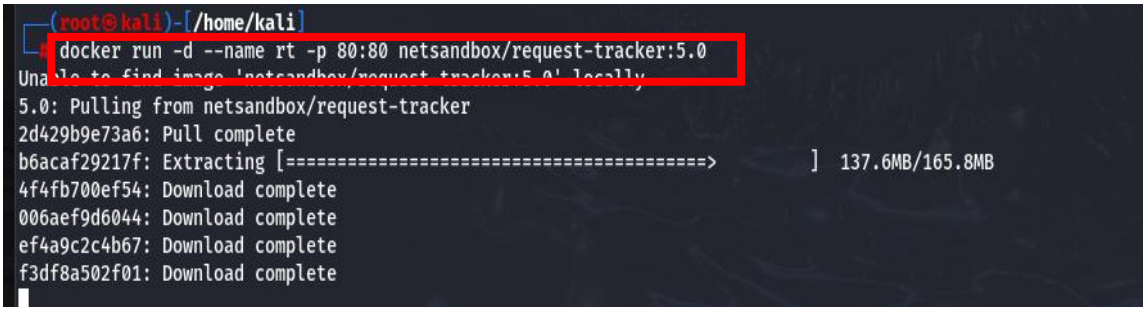
- ***Docker ps:*** Lista los contenedores
- ***-a:*** muestra todos los contenedores, incluyendo los que estan detenidos.
- ***-q:*** Devuelve solo los IDS de los contenedores, sin otra información.

Este comando es útil en las siguientes situaciones:

1. Limpieza del sistema: Cuando se necesita liberar espacio rápidamente eliminando todos los contenedores.
2. Reinicio de entornos: Para restablecer un entorno de desarrollo o prueba a un estado limpio.
3. Mantenimiento: para asegurar que no queden contenedores antiguos o no utilizados.

Ejecuta el Contenedor de Docker

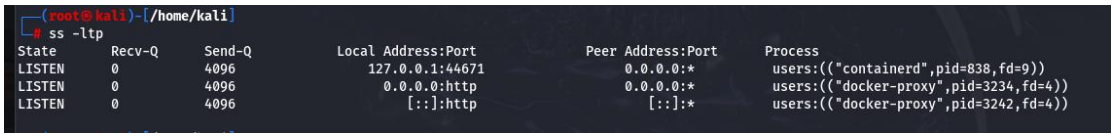
El comando ***docker run -d --name rt -p 80:80 netsandbox/request-tracker:5.0*** en la terminal de Linux realiza las siguientes acciones:



1. ***Docker run*** crea y ejecuta un nuevo contenedor basado en la imagen especificada, en este caso, ***netsandbox-tracker:5.0*** -
2. ***-d detached mode*** ejecuta el contenedor en segundo plano, permitiendo que sigas utilizando la terminal sin que el proceso del contenedor interfiera.
3. ***--name rt*** Asigna el nombre rt al contenedor, facilitando su identificación y gestión más adelante.
4. ***-p 80:80*** Mapea el puerto 80 del host al puerto 80 del contenedor. Esto significa que cualquier solicitud enviada al puerto 80 del sistema anfitrión será redirigida al puerto 80 dentro del contenedor.
5. ***Netsandbox-tracker:5.0*** Específica la imagen de docker que se usará para crear el contenedor.

Información detallada sobre Sockets TCP

El comando ***ss -ltp*** en la terminal de Linux muestra información detallada sobre los Sockets de TCP que están en estado de escucha (*listening*) en el sistema.



1. Muestra solo los Sockets que están en estado de escucha (*listening*).
2. Filtra para mostrar únicamente las conexiones TCP.
3. Muestra el Proceso asociado a cada Sockets, incluyendo el PID y el nombre del programa

***Sockets**:[20] Es una interfaz de comunicación que permite el intercambio de datos entre 2 dispositivos o aplicaciones a través de una red. Se caracteriza por:*

1. *Facilita la transferencia de información entre programas en diferentes equipos.*
2. *Utilizar una combinación única de dirección IP y número de puerto para identificarse.*
3. *Seguir un modelo cliente-servidor para establecer la comunicación.*

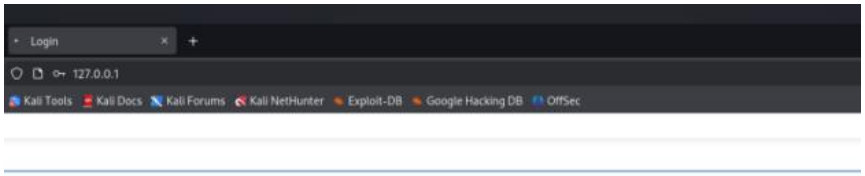
Existen 2 tipos principales de Sockets:

1. *Sockets de flujo (TCP): Proporcionan una conexión bidireccional confiable y ordenada, ideal para transmisiones continuas de datos.*
2. *Sockets de datagrama (UDP): Ofrecen un servicio no orientado a la conexión, enviando datos en paquetes independientes.*

Los Sockets son fundamentales en la programación de redes y permiten que las aplicaciones se comuniquen entre sí, ya sea en la misma máquina o través de Internet.

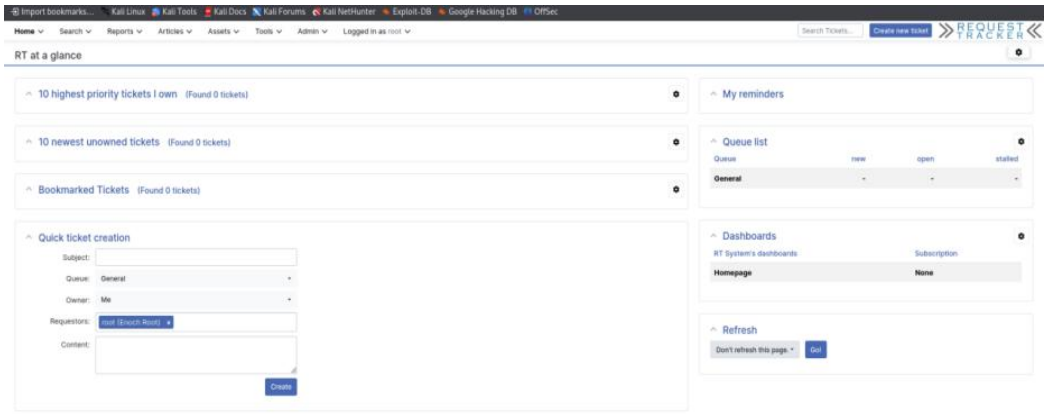
[20] https://www.perplexity.ai/search/que-es-un-socket-tcp-3R22hRF8RiC27HX_7CKj9w

Abrimos el navegador y accedemos a localhost



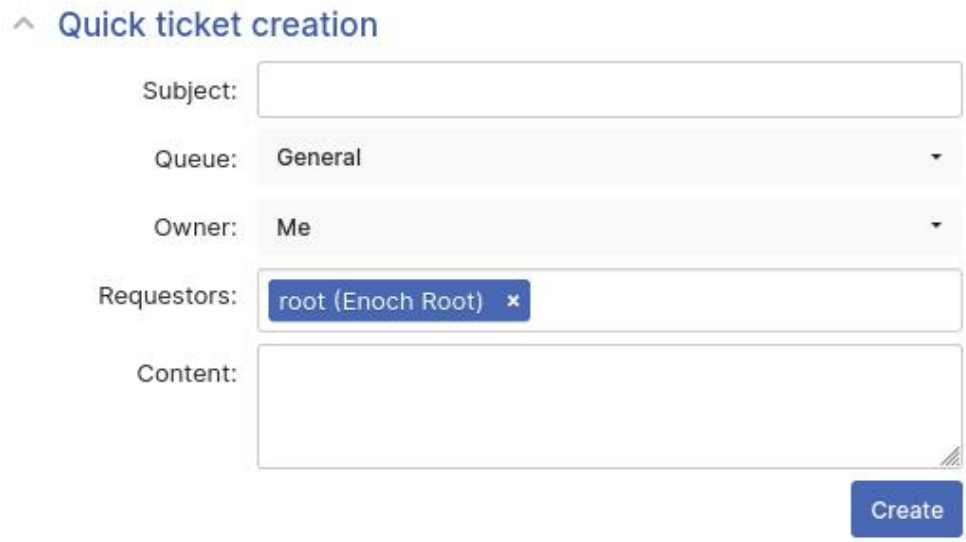
Usuario: ***root***
Contraseña: ***password***

Nos encontramos dentro de la Aplicación RTIR

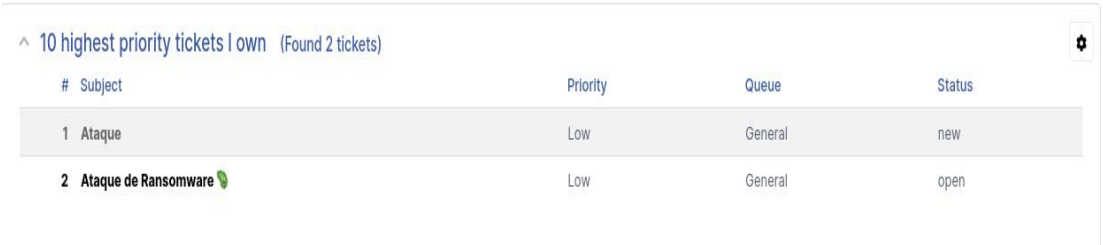


5.3 Creación de un Ticket

Al crear un nuevo ticket en RTIR nos aparece la ventana mostrada en la imagen siguiente, con el cuál primero tenemos que identificar el tipo de incidente para posteriormente priorizar y asignarle una criticidad al mismo.

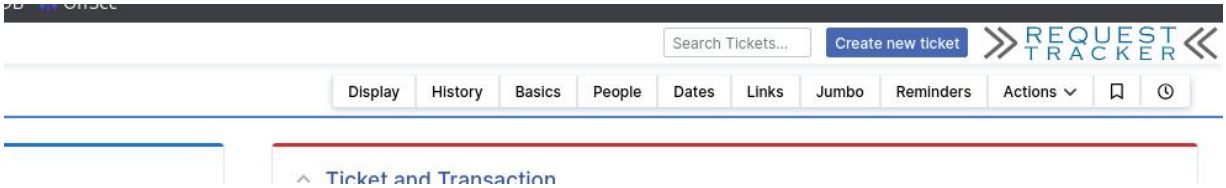


Una vez que hemos creado el ticket, nos aparece la siguiente ventana donde nos aparece la identificación del tipo de incidente, la prioridad, la cola del incidente y el estado.

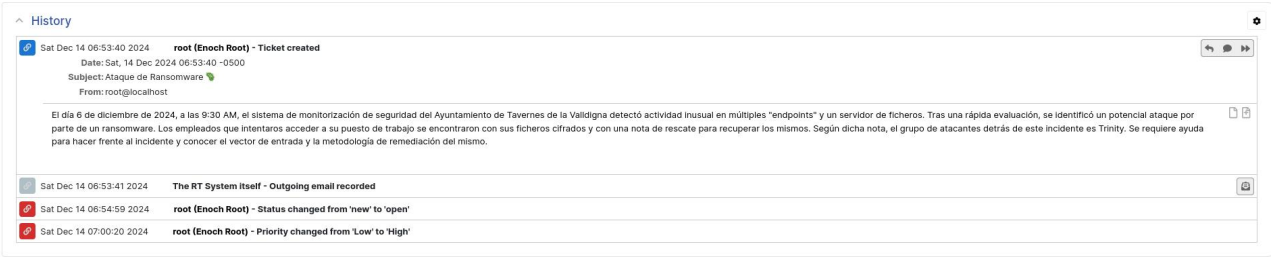


Desde la misma interfaz, podemos modificar la prioridad, la cola del incidente y el estado del ticket. En este caso, procederemos a ajustar la prioridad y el estado del ticket, ya que hemos generado una alerta de *ransomware*. Dado que la alerta tiene alta prioridad, el estado del ticket pasará de "Nuevo" a "Abierto".

En la barra de arriba nos aparecen las siguientes opciones donde podemos ver el historial del incidente para tener esa información adecuada y poder trabajar correctamente.

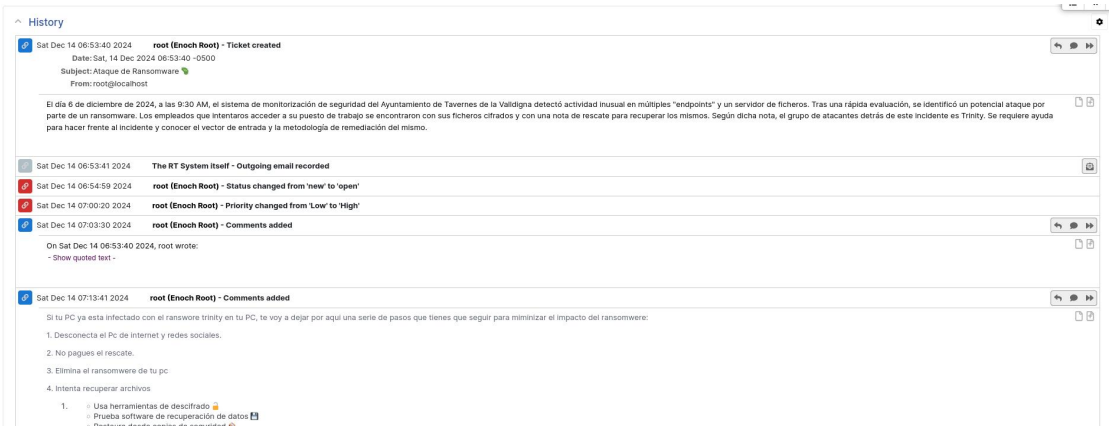


Una vez dentro del historial se nos abre la siguiente ventana con la siguiente información del incidente:



En este caso, estoy respondiendo a mí misma, simulando que el cliente X me envía un ticket y debo indicarle una serie de pasos a seguir para continuar con el proceso.

En el siguiente histórico se puede observar todo el *timeline* del ciclo de vida del ticket previamente descrito:



6. *Gestión de Incidentes INCIBE, CCN-CERT y CNPIC*

INCIBE (Instituto Nacional de Ciberseguridad): Es una entidad de referencia en España especializada en Ciberseguridad, cuya laboral es fundamental para el desarrollo de una sociedad digital segura y confiable. Como organismo público dependiente del Ministerio de Asuntos Económicos y Transformación Digital, desempeña un papel crucial en la protección contra los crecientes desafíos cibernéticos que enfrentan individuos, empresas e instituciones Su enfoque principal es mejorar la Ciberseguridad de los ciudadanos y empresas privadas, contribuyendo así a fortalecer la seguridad digital en el país y a proteger a la sociedad contra las amenazas cibernéticas emergentes.

Los procedimientos de notificación y gestión de incidentes de INCIBE se basan en la ***Guía Nacional de Notificación y Gestión de Ciberincidentes***[21] . El proceso comienza cuando el afectado notifica el incidente por correo electrónico a INCIBE-CERT. Luego, INCIBE-CERT evalúa el incidente y lo comunica al organismo receptor correspondiente, que se pone en contacto con el afectado para obtener más información.

INCIBE-CERT realiza un análisis inicial, clasifica el incidente y determina las medidas de respuesta, proporcionando recomendaciones al afectado.

---

21 https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

CCN-CERT: El CCN-CERT es un organismo público y tiene la capacidad de respuesta a incidentes de seguridad de la información del Centro Criptólogico nacional (CCN) de España. Fue creado en 2006 como el CERT Gubernamental Nacional español.

Los procedimientos de notificación y gestión de incidentes del CCN-CERT son los siguientes:

El canal preferente para notificar incidentes es a través de la aplicación Lucia. Como canal secundario, se puede utilizar el correo electrónico ***mailto:Incidentes@ccn-cert.cni.es*** **.**

Una vez recibida la notificación, el CCN-CERT sigue estos pasos:

1. Evalúa el incidente y lo comunica al organismo receptor correspondiente según el tipo de Incidente.
2. Colabora con organismos públicos y empresas de interés estratégico en la detección, evaluación, respuesta y tratamiento del Incidente.
3. Brinda, apoyo técnico y operativo en las etapas de detección, reacción, contención y eliminación.
4. Clasifica el Incidente según peligrosidad y prioridad.
5. Implementa medidas de respuesta y proporciona recomendaciones al afectado.
6. En casos de Incidentes de nivel alto o superior, notifica al Comité de Crisis y coordina la respuesta técnica a nivel nacional.
7. Actúa como nodo de Intercambio de Información de Ciberincidentes en las Administraciones Publicas.

CNPIC: El centro nacional de protección de Infraestructuras criticas es un organismo público adscrito a la Secretaria de estado de seguridad del ministerio del Interior de España. Su función principal es impulsar, coordinar y supervisar todas las actividades relacionadas con la protección de las infraestructuras críticas nacionales.

Los procedimientos de notificación y gestión de Incidentes del CNPIC son los siguientes:

1. Cuando ocurre un incidente que afecta a una Infraestructura crítica, el operador afectado notifica al CSIRT de referencia (INCIBE o CCN-CERT).

2. El CSIRT de referencia evalúa el incidente y lo comunica al CNPIC si está relacionado con una infraestructura critica.

3. El CNPIC, a través de la oficina de Coordinación Cibernética (OCC), coordina la comunicación con los CSIRT nacionales de referencia: CERTSI para operadores privados y CCN-CERT para operadores públicos.
4. En caso de una situación de crisis, el operador designado informa al CNPIC, que a su vez lo comunica a las unidades de inteligencia competentes.
5. Si es necesario, el CNPIC puede activar el equipo de respuesta ante emergencias (CERT) correspondiente.
6. El CNPIC actúa como punto de contacto nacional con la Comisión Europea y otros Estados en materia de protección de Infraestructuras críticas.
7. Para incidentes que afecten a operadores críticos del sector privado, la gestión se realiza conjuntamente entre INCIBE y la OCC del CNPIC.
8. El CNPIC mantiene y actualiza el catálogo nacional de infraestructuras críticas, utilizando esta información para coordinar las respuestas a incidentes.

Este procedimiento asegura una respuesta coordinada y eficaz ante incidentes que afecten a las infraestructuras críticas nacionales, manteniendo la seguridad y el funcionamiento de los servicios esenciales.

6.1 Lucia

Lucia (Listado Unificado de Coordinación de Incidentes y Amenazas) es una herramienta de gestión de incidentes de ciberseguridad desarrollada por el CCN-CERT (centro criptológico Nacional - *Computer Emergency Response Team*) de España.

Esta herramienta sirve para:

- Mejorar la coordinación en la gestión de incidentes de ciberseguridad entre organizaciones y el CCN-CERT.

- Facilita el cumplimiento de 2 requisitos del esquema nacional de seguridad (ENS):
  - La notificación obligatoria de incidentes
  - La carga de datos en el informe nacional del estado de seguridad (INES)
- Sincronizar información e incidentes de cada organización con la instancia central de lucia en el CCN-CERT.

- Proporcionar una plataforma única y distribuida para la gestión de Incidentes.
- Automatizar tareas como notificaciones, recordatorios y cierres automáticos.
- mantener la trazabilidad y seguimiento de los incidentes.
- Ofrecer un lenguaje común de peligrosidad y clasificación de incidentes.

Lucia está disponible para organismos públicos y empresas, y se puede descargar desde el portal del CCN-CERT. Su uso ayuda a mejorar la ciberseguridad española al facilitar la coordinación y el intercambio de información sobre incidentes de seguridad entre las organizaciones y el CERT Gubernamental Nacional.

6.2 Sistema de Alerta Temprana

Un sistema de alerta temprana (SAT) es una red de herramientas y procedimientos diseñados para identificar y comunicar rápidamente información sobre posibles peligros, riesgos o situaciones adversas en diversos escenarios. Su principal objetivo es ayudar a los responsables de la toma de decisiones a implementar medidas preventivas para reducir el impacto de posibles riesgos o catástrofes, salvaguardando vidas y recursos.

El SAT sirve para:

- Detectar y analizar amenazas potenciales, como desastres naturales o emergencias sanitarias.
- Evaluar la gravedad de los riesgos identificados.
- Emitir alertas oportunas a las autoridades y la población afectada.
- Facilitar la implementación de medidas preventivas y de respuesta.

Un SAT eficaz consta de 4 elementos claves:

- Monitoreo y detección: recolección de datos a través de sensores, satélites, y otras fuentes.
- Análisis y evaluación de riesgos: determinación del impacto potencial y la urgencia de las acciones necesarias.
- Comunicación de la alerta: transmisión rápida de información a través de múltiples canales.

- respuesta y acción: implementación de medidas de emergencia y protocolos de seguridad.

La importancia de los SAT radica en su capacidad para reducir riesgos de

desastres, proteger vidas e infraestructuras y contribuir a una mayor resiliencia frente a futuras amenazas. En un mundo donde el cambio climático aumenta la frecuencia e intensidad de los desastres, los SAT se han vuelto indispensables para garantizar la seguridad de las comunidades y mitigar los impactos de fenómenos destructivos.

7. Conclusiones

Las herramientas de *ticketing* juegan un papel fundamental en la gestión de incidentes, un área que cada vez cobra mayor relevancia debido a la creciente frecuencia y complejidad de los incidentes de ciberseguridad. Estas herramientas permiten centralizar, organizar y gestionar de manera eficiente los incidentes, garantizando una respuesta rápida y coordinada. En un entorno donde las amenazas son cada vez más sofisticadas, disponer de un sistema de *ticketing* adecuado es crucial para minimizar el impacto de los incidentes y reducir los tiempos de resolución, lo que permite a las organizaciones mantener la continuidad operativa.

En este contexto, RTIR (*Request Tracker for Incident Response*) se presenta como una herramienta poderosa y flexible, que facilita la gestión de incidentes de ciberseguridad mediante un sistema de tickets completamente configurable. RTIR no solo ayuda a gestionar el flujo de trabajo de manera ordenada, sino que también permite a los equipos de respuesta documentar de forma precisa cada acción tomada, optimizando así la trazabilidad y el análisis posterior del incidente