

SOC (Security Operations Center)

Módulo 5 – Herramientas



IT SERVICE MANAGEMENT - EJERCICIOS

Sheila Fernández Cisneros – 25/07/2024

Tarea 1:

Las plataformas ITSM (IT Service Management) son herramientas de ticketing que pueden ayudar a los analistas a operar con las alertas y establecer comunicación con los clientes de una manera más eficiente y organizada. Para probar una de estas herramientas usaremos una plataforma que ofrece una demo gratuita (Jira). En el foro encontraréis un tutorial para crear una instancia personalizada en esta plataforma.

Como primer ejercicio se pide crear un proyecto ITSM en Jira con un nombre personalizado. Tras haberlo creado, se pide ir a Project Settings > Portal Settings. Dentro de Service Project Information nos aparecen dos campos: Portal Name e Introduction Text. Se pide modificar ambos campos de manera personalizada y darle a Save. Una vez hecho mandar una captura. Comparte también el link del portal donde se aloja tu proyecto.

Ejemplo: <https://pruebaitsm.atlassian.net/servicedesk/customer/portal/2>

The screenshot shows the 'Portal settings' page under 'Project settings'. The 'Portal configuration' tab is selected. In the 'Portal details' section, the 'Portal URL' is set to <https://pruebaitsm.atlassian.net/servicedesk/cust>. In the 'Service project information' section, the 'Portal name' is set to 'pruebasitsm2' and the 'Introduction text' is set to '¡Bienvenido al proyecto!'. A 'Save' button is visible at the bottom left. A 'Logo' placeholder is at the bottom right.

Creación de Proyecto ITSM en Jira

Objetivo: Crear un proyecto de ITSM en Jira, personalizar el nombre del portal y el texto de introducción, y proporcionar el enlace del proyecto.

Pasos Seguidos:

1. Creación del Proyecto:

- Acceder a la plataforma Jira y navegar hasta la opción de crear un nuevo proyecto.
- En el formulario de creación de proyectos, ingresar los siguientes datos:
 - **Nombre del Proyecto:** HackTheWorld
 - **Clave del Proyecto:** TEST
 - **Tipo de Equipo:** Risk & Compliance
 - **Acceso al Canal:** Restricted
- A continuación, selecciona la opción “Create” para finalizar la creación del proyecto.

2. Configuración del Portal:

- Ir a la configuración del proyecto seleccionando “Project Settings” y luego “Portal Settings”.
- En la sección “Service Project Information”, modificamos los siguientes campos:
 - **Portal Name:** HackTheWorld
 - **Introduction Text:** Hello world! Let's hack the world!
- Guarda los cambios haciendo clic en “Save”.

Aquí está el enlace del portal donde se aloja el proyecto:
<https://hackershei.atlassian.net/servicedesk/customer/portal/2>

[← Back to project templates](#)

Create project

Add your project's details and confirm your template to create your new project in seconds. Edit project details anytime in project settings.

Required fields are marked with an asterisk *

Name *

HackTheWorld

Key ⓘ *

TEST

Team type *

Risk & Compliance

This will help us customize your project setup experience.

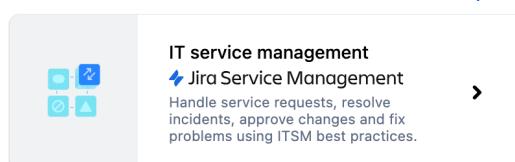
Channel access ⓘ *

Restricted

Control who can submit requests to your team.

Template

[More templates](#)



[←](#) [→](#) [G](#) hackershei.atlassian.net/jira/servicedesk/projects/TEST/settings/portal-settings

[Jira](#) Your work [Projects](#) [Filters](#) [Dashboards](#) [Teams](#) [Plans](#) [Assets](#) [Apps](#) [Create](#) [Help](#) [Feedback](#) [Settings](#) [Logout](#)

HackTheWorld Service project
You're on the Free plan [UPGRADE](#)

[Back to project](#)

[External resources](#)

[Change management](#)

[Incident management](#)

[Customer permissions](#)

[Language support](#)

Portal settings [Portal configuration](#) [Portal groups](#)

Portal details

Portal URL: <https://hackershei.atlassian.net/servicedesk/ci>

Service project information
Required fields are marked with an asterisk *

Portal name *: HackTheWorld

Introduction text: Hello world! Let's hack the world!

[Save](#)

Logo: [Add logo](#)

Channel access
RESTRICTED Only people directly invited to this project can submit requests.

Your Coach

Welcome

Let's get you started in a few easy steps.

Quick setup

Quickly make your project ready for use by completing set-up tasks

- > Create your ITSM project
- > Update your portal name
- > Set up email requests
- > Set up chat requests
- > Set up a service
- > Add a team member

> Get started with a tour

Manage Incidents

Reduce incident response time in a few steps

[Explore sample space](#)

Tarea 2:

Es necesario establecer un medio para establecer conexión con los clientes y que estos hagan sus solicitudes (requests) y obtengan respuesta desde un medio común. Para ello haremos que estos se contacten con nosotros a través de una dirección de correo. Para configurarlo, navegaremos hacia Project Settings > Email requests y le daremos a Add external email (en este caso al ser un entorno de prueba, la dirección de contacto será nuestro email personal). Añádelo y ponlo por defecto en el Reply-to address. Una vez lo hayas configurado dale a Update y haz una captura.

Luego de esto, tendrás todas las herramientas para crear una nueva incidencia. Dirígete al botón de Create en la pestaña superior para crear una nueva Issue.

Your work ▾ Projects ▾ Filters ▾ Dashboards ▾ Teams ▾ Assets Apps ▾ Create

Subject*

URL de phishing detectada en el correo de un cliente

Body

Normal text ▾ | B I ... | A ▾ | ≡ ≡ | ⌂ ⌂ @ ⌂ ⌂ ⌂ ⌂ ⌂ ⌂ + ▾

El usuario Pepito@gmail.com ha reportado que ha recibido la siguiente URL de phishing:
djdfhgdjfgdj-comprasonline.com

Investiga si es maliciosa y reportanos el resultado.

Configuración de Correo y Creación de Incidencia en Jira

Objetivo: Configurar una dirección de correo externa para recibir solicitudes y crear una nueva incidencia basada en un correo recibido.

Pasos Seguidos:

1. **Configuración de la Dirección de Correo: Se intentó de varias maneras.**
 - Ir a “Project Settings” y luego selecciona “Email requests”.
 - Hice clic en “Add external email” e ingresa un correo como dirección de contacto.

The screenshot shows the 'Email' settings page in Jira. At the top, it says 'Projects / HackTheWorld / Project settings'. Below that is a section titled 'Email' with a '...' button. A note says: 'Use the email channel to turn customer emails into requests in your service project. Each service project can have up to 10 connected email accounts. [Find more information on connecting multiple email addresses.](#)' Another note says: 'Manage permissions for sending email requests and adding other participants by email in [Customer permissions](#)'.

Reply-to address

The selected email address is used when customers reply to email notifications for requests raised via channels other than email. Your project needs to have at least two connected email accounts to update the reply-to address.
[Read more about reply-to email addresses.](#)

A dropdown menu shows 'support@hackershei.atlassian.net' with a 'Update' button next to it.

Connected email accounts

Email Address	Request Type	Incoming email logs	Last email received	Actions
support@hackershei.atlassian.net <small>REPLY-TO ADDRESS</small>	Emailed request	View logs	No emails received	...

Primer intento fallido:

- Se completaron los detalles de la dirección de correo externo usando las siguientes configuraciones:
- Se eligió la tercera opción de “**continue with other**”
 - **Email address:** fitlink42@gmail.com
 - **Password:** (contraseña a elegir)
 - **Mail Server:** gmail
 - **Protocol:** IMAPS
 - **Port:** 993
 - **Request type:** Emailed request

Add external email address

Select an email provider to get started.

 Continue with Google

 Continue with Microsoft

 Continue with Other

Jira Service Management's use and transfer to any other app of information received from Google APIs will adhere to the [Google API Services User Data Policy](#), including the Limited Use requirements.

[Cancel](#)

Add details of your external email address

Customers can use this email address to raise requests only in **HackTheWorld**.

Required fields are marked with an asterisk *

Email address *

ftlink42@gmail.com

My username is different from email address.

Password *

.....

Mail Server *

gmail

Protocol *

IMAPS

Port *

993

POP

POP3S

IMAP

IMAPS

d description as required fields.
d from this email address.

[Cancel](#)

[Add](#)

Add details of your external email address

Customers can use this email address to raise requests only in **HackTheWorld**.

Required fields are marked with an asterisk *

Email address *

ftlink42@gmail.com

My username is different from email address.

Password *

.....

Mail Server *

gmail

Protocol *

IMAPS

Port *

993

Request type *

Select a request type

You can select request types with only summary and description as required fields.
The request type will be assigned to requests raised from this email address.
[Read more about request types in email channel](#).

[Cancel](#)

[Add](#)

Add details of your external email address

Customers can use this email address to raise requests only in **HackTheWorld**. Required fields are marked with an asterisk *

Email address *
ftlink42@gmail.com

My username is different from email address.

Password *
.....

Report a system problem
 Report broken hardware
 Request a change
 Request admin access
 Request new hardware
 Request new software
 Set up VPN to the office
 Emailed request
 Investigate a problem

only summary and description as required fields.
No requests raised from this email address.
[email channel](#).

Cancel **Add**

Add details of your external email address

Customers can use this email address to raise requests only in **HackTheWorld**. Required fields are marked with an asterisk *

Email address *
ftlink42@gmail.com

My username is different from email address.

Password *
.....

Mail Server *
gmail

Protocol * IMAPS **Port *** 993

Request type * Emailed request

You can select request types with only summary and description as required fields. The request type will be assigned to requests raised from this email address.
[Read more about request types in email channel](#).

Cancel **Add**

Segundo intento fallido:

- Se intentó con el protocolo POP3S y el puerto 995, pero de nuevo se generó un error de conexión, el mismo que recibía con la configuración anterior.

Add details of your external email address

Customers can use this email address to raise requests only in **HackTheWorld**. Required fields are marked with an asterisk *

Email address *
ftlink42@gmail.com

My username is different from email address.

Password *
.....

Mail Server *
gmail

Protocol * POP3S **Port *** 995

Request type * Emailed request

You can select request types with only summary and description as required fields. The request type will be assigned to requests raised from this email address.
[Read more about request types in email channel](#).

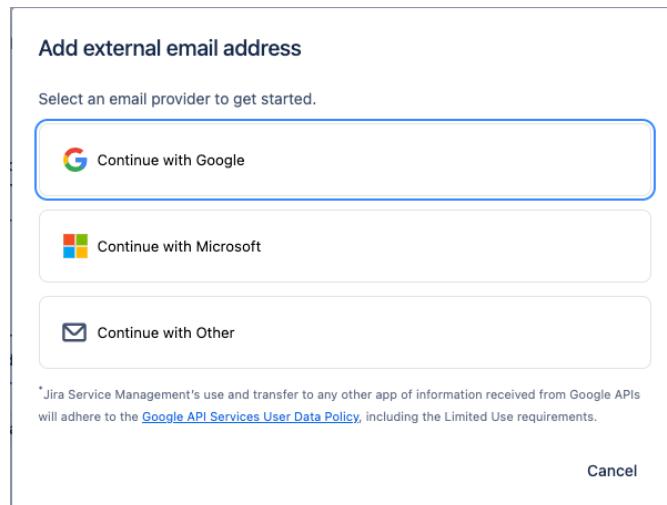
Cancel **Add**

✖ Couldn't add email address ✖

Unfortunately JIRA couldn't connect to the mail server. Here is what the mail server said: "SOCKS: Host unreachable"

Tercer intento:

- Finalmente, se utilizó la opción de “Continue with Google” la cual hace ajustes automáticos en los que se le debe dar obligatoriamente permisos a Jira para consultar información personal de tu email y entonces se pudo añadir el correo correctamente.
- Se procede a guardar la configuración y el correo se añade exitosamente como dirección de respuesta.



Sign in with Google

Jira Service Management wants access to your Google Account

ftlink42@gmail.com

Select what **Jira Service Management** can access

Read, compose, and send emails from your Gmail account. [Learn more](#)

Because you're using Sign in with Google, Jira Service Management will be able to

Associate you with your personal info on Google

See your personal info, including any personal info you've made publicly available

See your primary Google Account email address

Make sure you trust Jira Service Management

You may be sharing sensitive info with this site or app. Learn about how Jira Service Management will handle your data by reviewing its [terms of service](#) and [privacy policies](#). You can always see or remove access in your [Google Account](#).

[Learn about the risks](#)

Cancel Continue

Update request type

Change the request type for requests created from ftlink42@gmail.com.

Request type

Emailed request ▾

You can select request types with only summary and description as required fields. The request type will be assigned to requests raised from this email address. [Read more about request types in email channel.](#)

Skip Update

2. Creación de Incidencia:

- Navega al botón “Create” en la pestaña superior para crear una nueva incidencia.
- Selecciona el proyecto actual, tipo de incidencia como “[System] Incident” y tipo de solicitud como “Emailed Request”.
- Personalizamos el asunto y el cuerpo del mensaje de la incidencia:
 - **Asunto:** Descarga de archivo malicioso a través de dominio sospechoso
 - **Cuerpo:** El usuario Juan Perez con IP 192.168.1.100 ha descargado un archivo malicioso desde el dominio sospechoso:
 - **URL del dominio malicioso:** www.dominio-malicioso.com
 - **Nombre del archivo:** malicioso.exe
 - **Hash del archivo:** f5d3f4ab-c0a2-4e94-a5fe-2b9d7af23456

Por favor, investiguen si es malicioso y reporten el resultado.

- Después de llenar todos los campos, hacemos clic en “Create” para finalizar la creación de la incidencia.
- Finalmente, verificamos que la incidencia fue creada y está lista para ser gestionada.

El correo fue configurado correctamente para recibir solicitudes y una nueva incidencia fue creada con los detalles proporcionados.

Projects / HackTheWorld / Project settings

Email

Use the email channel to turn customer emails into requests in your service project. Each service project can have up to 10 connected email accounts. [Find more information on connecting multiple email addresses.](#)

Manage permissions for sending email requests and adding other participants by email in [Customer permissions](#).

Reply-to address

The selected email address is used when customers reply to email notifications for requests raised via channels other than email. Your project needs to have at least two connected email accounts to update the reply-to address. [Read more about reply-to email addresses.](#)

Connected email accounts

Email Address	Request Type	Incoming email logs	Last email received	Actions
 support@hackershei.atlassian.net	Emailed request	View logs	No emails received	...
 ftlink42@gmail.com REPLY-TO ADDRESS	Emailed request	View logs	No emails received	...

[Create Atlassian email](#) [Add external email](#)

Jira Your work ▾ Projects ▾ Filters ▾ Dashboards ▾ Teams ▾ Plans ▾ Assets Apps ▾ Create

Projects / HackTheWorld / Project settings

Email

Use the email channel to turn customer emails into requests in your service project. Each service project can have up to 10 connected email accounts. [Find more information on connecting multiple email addresses.](#)

Manage permissions for sending email requests and adding other participants by email in [Customer permissions](#).

Reply-to address

The selected email address is used when customers reply to email notifications for requests raised via channels other than email. Your project needs to have at least two connected email accounts to update the reply-to address. [Read more about reply-to email addresses.](#)

Connected email accounts

Email Address	Request Type	Incoming email logs	Last email received	Actions
 support@hackershei.atlassian.net	Emailed request	View logs	No emails received	...
 ftlink42@gmail.com REPLY-TO ADDRESS	Emailed request	View logs	No emails received	...

[Create Atlassian email](#) [Add external email](#)

Create issue

Required fields are marked with an asterisk *

Project*

Issue type* Task

[Learn about issue types](#)

Request type* No request type Issues can't be shared with customers, and may not work as expected.

Use request type fields

Summary*

Components

Attachment

Due date

Description

We support markdown! Try `**bold**`, `'inline code'`, or ````` for code blocks.

Create another issue

Create issue

Required fields are marked with an asterisk *

1

Project *

HackTheWorld (TEST)

Issue type *

Task

- Task
- [System] Service request
- [System] Incident
- [System] Problem
- [System] Change
- [System] Post-incident review
- [System] Service request with approvals

What's this?

ay not work as expected.

Create issue

Required fields are marked with an asterisk *

1

Project *

HackTheWorld (TEST)

Issue type *

[System] Incident

[Learn about issue types](#)

Request type *

What's this?

Report a system problem
Let us know if something isn't working properly and we'll aim to get it back up and running quickly.

No request type

Issues can't be shared with customers, and may not work as expected.

Service requests

Emailed request

Request received from your email support channel.

Fix an account problem

Having trouble accessing certain websites or systems? We'll help you out.

Get a guest wifi account

Bring a request to ask for temporary wifi access for guests.

Create issue

Project *

HackTheWorld (TEST)

Issue type *

[System] Service request

[Learn about issue types](#)

Request type *

Emailed request

Request received from your email support channel.

Use request type fields (?)

Raise this request on behalf of *

Shei

Subject *

Descarga de archivo malicioso a través de dominio sospechoso

Body

Normal text Normal text | **B** *I* ... | A A | list list | link image email comment mention more

El usuario Juan Perez con IP 192.168.1.100 ha descargado un archivo malicioso desde el dominio sospechoso:

- **URL del dominio malicioso:** www.dominio-malicioso.com
- **Nombre del archivo:** [malicioso.exe](#)
- **Hash del archivo:** f5d3ffab-c0a2-4e9d-a15e-2b9d7a123456

Por favor, investiguen si es malicioso y reporten el resultado.

Organizations

Select organization

Create another issue

[Cancel](#) [Create](#)

 You've created "TEST-1" issue

[View issue](#) · [Copy link](#)

The screenshot shows a Jira issue page for a project named 'TEST-1'. The main content is a ticket titled 'Descarga de archivo malicioso a través de dominio sospechoso' (Suspicious domain download of malicious file). The ticket was raised by 'Shei' via Jira. The description states that a user named Juan Perez (IP 192.168.1.100) downloaded a malicious file from the domain 'www.dominio-malicioso.com'. The file is named 'malicioso.exe' and has a hash of 'f5d3ffab-c0a2-4e9d-a15e-2b9d7a123456'. A note at the bottom asks for investigation and reporting of results.

Activity:

- Show: All, Comments (selected), History, Work log, Approvals
- Sort: Newest first ↴

Details:

- Assignee: Unassigned (Assign to me)
- Reporter: Shei
- Request Type: Emailed request
- Priority: Medium
- Urgency: None
- Impact: None
- Affected services: + Add service
- Pending reason: None

Automation: Rule executions

Created 43 seconds ago | Updated 42 seconds ago | Configure

Tarea 3:

Es hora de tratar con la incidencia que hemos creado tal y como se haría en un equipo normal. Navega hacia la pestaña de Queues y asegúrate de que la incidencia se ha creado correctamente. Luego de esto haz click en la incidencia y haz una captura de la página que sale.

Normalmente en un equipo de seguridad es común que estéis varios compañeros al mismo tiempo para hacer frente a las incidencias. Para ello, estas herramientas de ticketing ofrecen una serie de opciones al momento de asignarse y empezar a trabajar con una incidencia. Al abrir la incidencia

recientemente creada, aparecerá a la derecha un botón azul que dice: ‘Waiting for Support’. Si clicamos en él, podemos cambiar el estado de la incidencia. Como la vamos a tratar ahora mismo, cambiaremos el estado a ‘In Progress’. Se nos abrirá la siguiente ventana:

The screenshot shows a modal window titled 'In progress' for creating a comment. At the top, there's a dropdown labeled 'Assignee' with 'Unassigned' selected. Below it is a button 'Assign to me'. The main area is a 'Comment' input field with two tabs: 'Respond to customer' (which is selected) and 'Internal comment'. A note below says, 'Your comment will be visible to customers. Embed attachments to make them visible to customers.' There's a rich text editor toolbar above the input field. At the bottom left are 'preview' and 'syntax help' links. On the right side, there are 'In progress' and 'Cancel' buttons.

Asígnate la incidencia y abajo dale a insertar un ‘Internal comment’.

Puedes poner algo como: “Incidencia en progreso”, o un comentario personalizado. Ejecuta la acción y comprueba que el comentario se ha generado correctamente. ¿De qué color aparece este comentario interno?

Gestión de Incidencia en Jira

Objetivo: Gestionar la incidencia creada, cambiar su estado a “In Progress” y añadir un comentario interno.

Pasos Seguidos:

1. Verificación de la Incidencia:

- Navega a la pestaña “Queues” para asegurarse de que la incidencia se ha creado correctamente.
- Hacer clic en la incidencia para acceder a sus detalles.

2. Cambio de Estado de la Incidencia:

- A la derecha de la pantalla de detalles de la incidencia, hacer clic en la opción “Waiting for Support”.
- Cambia el estado de la incidencia a “In Progress”.

- Se abre una ventana donde me asigno la incidencia y añado un comentario interno.

3. Añadir Comentario Interno:

- En la ventana de “In Progress”, selecciona la opción “Internal comment”.
- Escribe el comentario: “Incidencia en progreso”.
- Ejecuta la acción y comproba que el comentario se ha generado correctamente.

El comentario interno aparece en color **amarillo**.

Con estos pasos, la incidencia ha sido correctamente gestionada y se ha añadido un comentario interno para reflejar que está en progreso.

The screenshots illustrate the Jira Service Desk interface for managing service requests. The top screenshot shows the 'All open' queue for the 'HackTheWorld' project, displaying a single request with the key 'TEST-1'. The bottom screenshot provides a detailed view of this specific request, showing its description, pinned fields, and activity log, including the internal comment added during the 'In Progress' phase.

Jira Your work Projects Filters Dashboards Teams Plans Assets Apps Create

hackershei.atlassian.net/jira/servicedesk/projects/TEST/queues/custom/4

HackTheWorld Service project You're on the Free plan + UPGRADE Back to project

Queues

STARRED Select the star icon next to your queues to add them here.

TEAM PRIORITY

All open	1
Assigned to me	0
Open tasks	0

Manage queues Give feedback

Projects / HackTheWorld / Queues All open

Search for issues

1 Issue

Request Type	Key	Summary	Reporter	Assignee	Status	Created	Time to resolution
Emailed request	TEST-1	Descarga de archivo malicioso a través de dominio sospechoso	Shel	Unassigned	WAITING FOR SUPPORT	26/Jul/24	05 Aug 12:42

Respond to customer → WAITING FOR CUSTOMER

- In progress → IN PROGRESS
- Escalate → ESCALATED
- Pending → PENDING
- Cancel request → CANCELLED
- Resolve this issue → RESOLVED

View workflow

In progress

Assignee
Unassigned

Assign to me

Comment

Respond to customer Internal comment

Your comment will be visible to customers. Embed attachments to make them visible to customers.

Style B I U A ¹A ²A ³A ⁴A ⁵A ⁶A ⁷A ⁸A ⁹A ¹⁰A ¹¹A ¹²A ¹³A ¹⁴A ¹⁵A ¹⁶A ¹⁷A ¹⁸A ¹⁹A ²⁰A ²¹A ²²A ²³A ²⁴A ²⁵A ²⁶A ²⁷A ²⁸A ²⁹A ³⁰A ³¹A ³²A ³³A ³⁴A ³⁵A ³⁶A ³⁷A ³⁸A ³⁹A ⁴⁰A ⁴¹A ⁴²A ⁴³A ⁴⁴A ⁴⁵A ⁴⁶A ⁴⁷A ⁴⁸A ⁴⁹A ⁵⁰A ⁵¹A ⁵²A ⁵³A ⁵⁴A ⁵⁵A ⁵⁶A ⁵⁷A ⁵⁸A ⁵⁹A ⁶⁰A ⁶¹A ⁶²A ⁶³A ⁶⁴A ⁶⁵A ⁶⁶A ⁶⁷A ⁶⁸A ⁶⁹A ⁷⁰A ⁷¹A ⁷²A ⁷³A ⁷⁴A ⁷⁵A ⁷⁶A ⁷⁷A ⁷⁸A ⁷⁹A ⁸⁰A ⁸¹A ⁸²A ⁸³A ⁸⁴A ⁸⁵A ⁸⁶A ⁸⁷A ⁸⁸A ⁸⁹A ⁹⁰A ⁹¹A ⁹²A ⁹³A ⁹⁴A ⁹⁵A ⁹⁶A ⁹⁷A ⁹⁸A ⁹⁹A ¹⁰⁰A ¹⁰¹A ¹⁰²A ¹⁰³A ¹⁰⁴A ¹⁰⁵A ¹⁰⁶A ¹⁰⁷A ¹⁰⁸A ¹⁰⁹A ¹¹⁰A ¹¹¹A ¹¹²A ¹¹³A ¹¹⁴A ¹¹⁵A ¹¹⁶A ¹¹⁷A ¹¹⁸A ¹¹⁹A ¹²⁰A ¹²¹A ¹²²A ¹²³A ¹²⁴A ¹²⁵A ¹²⁶A ¹²⁷A ¹²⁸A ¹²⁹A ¹³⁰A ¹³¹A ¹³²A ¹³³A ¹³⁴A ¹³⁵A ¹³⁶A ¹³⁷A ¹³⁸A ¹³⁹A ¹⁴⁰A ¹⁴¹A ¹⁴²A ¹⁴³A ¹⁴⁴A ¹⁴⁵A ¹⁴⁶A ¹⁴⁷A ¹⁴⁸A ¹⁴⁹A ¹⁵⁰A ¹⁵¹A ¹⁵²A ¹⁵³A ¹⁵⁴A ¹⁵⁵A ¹⁵⁶A ¹⁵⁷A ¹⁵⁸A ¹⁵⁹A ¹⁶⁰A ¹⁶¹A ¹⁶²A ¹⁶³A ¹⁶⁴A ¹⁶⁵A ¹⁶⁶A ¹⁶⁷A ¹⁶⁸A ¹⁶⁹A ¹⁷⁰A ¹⁷¹A ¹⁷²A ¹⁷³A ¹⁷⁴A ¹⁷⁵A ¹⁷⁶A ¹⁷⁷A ¹⁷⁸A ¹⁷⁹A ¹⁸⁰A ¹⁸¹A ¹⁸²A ¹⁸³A ¹⁸⁴A ¹⁸⁵A ¹⁸⁶A ¹⁸⁷A ¹⁸⁸A ¹⁸⁹A ¹⁹⁰A ¹⁹¹A ¹⁹²A ¹⁹³A ¹⁹⁴A ¹⁹⁵A ¹⁹⁶A ¹⁹⁷A ¹⁹⁸A ¹⁹⁹A ²⁰⁰A ²⁰¹A ²⁰²A ²⁰³A ²⁰⁴A ²⁰⁵A ²⁰⁶A ²⁰⁷A ²⁰⁸A ²⁰⁹A ²¹⁰A ²¹¹A ²¹²A ²¹³A ²¹⁴A ²¹⁵A ²¹⁶A ²¹⁷A ²¹⁸A ²¹⁹A ²²⁰A ²²¹A ²²²A ²²³A ²²⁴A ²²⁵A ²²⁶A ²²⁷A ²²⁸A ²²⁹A ²³⁰A ²³¹A ²³²A ²³³A ²³⁴A ²³⁵A ²³⁶A ²³⁷A ²³⁸A ²³⁹A ²⁴⁰A ²⁴¹A ²⁴²A ²⁴³A ²⁴⁴A ²⁴⁵A ²⁴⁶A ²⁴⁷A ²⁴⁸A ²⁴⁹A ²⁵⁰A ²⁵¹A ²⁵²A ²⁵³A ²⁵⁴A ²⁵⁵A ²⁵⁶A ²⁵⁷A ²⁵⁸A ²⁵⁹A ²⁶⁰A ²⁶¹A ²⁶²A ²⁶³A ²⁶⁴A ²⁶⁵A ²⁶⁶A ²⁶⁷A ²⁶⁸A ²⁶⁹A ²⁷⁰A ²⁷¹A ²⁷²A ²⁷³A ²⁷⁴A ²⁷⁵A ²⁷⁶A ²⁷⁷A ²⁷⁸A ²⁷⁹A ²⁸⁰A ²⁸¹A ²⁸²A ²⁸³A ²⁸⁴A ²⁸⁵A ²⁸⁶A ²⁸⁷A ²⁸⁸A ²⁸⁹A ²⁹⁰A ²⁹¹A ²⁹²A ²⁹³A ²⁹⁴A ²⁹⁵A ²⁹⁶A ²⁹⁷A ²⁹⁸A ²⁹⁹A ³⁰⁰A ³⁰¹A ³⁰²A ³⁰³A ³⁰⁴A ³⁰⁵A ³⁰⁶A ³⁰⁷A ³⁰⁸A ³⁰⁹A ³¹⁰A ³¹¹A ³¹²A ³¹³A ³¹⁴A ³¹⁵A ³¹⁶A ³¹⁷A ³¹⁸A ³¹⁹A ³²⁰A ³²¹A ³²²A ³²³A ³²⁴A ³²⁵A ³²⁶A ³²⁷A ³²⁸A ³²⁹A ³³⁰A ³³¹A ³³²A ³³³A ³³⁴A ³³⁵A ³³⁶A ³³⁷A ³³⁸A ³³⁹A ³⁴⁰A ³⁴¹A ³⁴²A ³⁴³A ³⁴⁴A ³⁴⁵A ³⁴⁶A ³⁴⁷A ³⁴⁸A ³⁴⁹A ³⁵⁰A ³⁵¹A ³⁵²A ³⁵³A ³⁵⁴A ³⁵⁵A ³⁵⁶A ³⁵⁷A ³⁵⁸A ³⁵⁹A ³⁶⁰A ³⁶¹A ³⁶²A ³⁶³A ³⁶⁴A ³⁶⁵A ³⁶⁶A ³⁶⁷A ³⁶⁸A ³⁶⁹A ³⁷⁰A ³⁷¹A ³⁷²A ³⁷³A ³⁷⁴A ³⁷⁵A ³⁷⁶A ³⁷⁷A ³⁷⁸A ³⁷⁹A ³⁸⁰A ³⁸¹A ³⁸²A ³⁸³A ³⁸⁴A ³⁸⁵A ³⁸⁶A ³⁸⁷A ³⁸⁸A ³⁸⁹A ³⁹⁰A ³⁹¹A ³⁹²A ³⁹³A ³⁹⁴A ³⁹⁵A ³⁹⁶A ³⁹⁷A ³⁹⁸A ³⁹⁹A ⁴⁰⁰A ⁴⁰¹A ⁴⁰²A ⁴⁰³A ⁴⁰⁴A ⁴⁰⁵A ⁴⁰⁶A ⁴⁰⁷A ⁴⁰⁸A ⁴⁰⁹A ⁴¹⁰A ⁴¹¹A ⁴¹²A ⁴¹³A ⁴¹⁴A ⁴¹⁵A ⁴¹⁶A ⁴¹⁷A ⁴¹⁸A ⁴¹⁹A ⁴²⁰A ⁴²¹A ⁴²²A ⁴²³A ⁴²⁴A ⁴²⁵A ⁴²⁶A ⁴²⁷A ⁴²⁸A ⁴²⁹A ⁴³⁰A ⁴³¹A ⁴³²A ⁴³³A ⁴³⁴A ⁴³⁵A ⁴³⁶A ⁴³⁷A ⁴³⁸A ⁴³⁹A ⁴⁴⁰A ⁴⁴¹A ⁴⁴²A ⁴⁴³A ⁴⁴⁴A ⁴⁴⁵A ⁴⁴⁶A ⁴⁴⁷A ⁴⁴⁸A ⁴⁴⁹A ⁴⁵⁰A ⁴⁵¹A ⁴⁵²A ⁴⁵³A ⁴⁵⁴A ⁴⁵⁵A ⁴⁵⁶A ⁴⁵⁷A ⁴⁵⁸A ⁴⁵⁹A ⁴⁶⁰A ⁴⁶¹A ⁴⁶²A ⁴⁶³A ⁴⁶⁴A ⁴⁶⁵A ⁴⁶⁶A ⁴⁶⁷A ⁴⁶⁸A ⁴⁶⁹A ⁴⁷⁰A ⁴⁷¹A ⁴⁷²A ⁴⁷³A ⁴⁷⁴A ⁴⁷⁵A ⁴⁷⁶A ⁴⁷⁷A ⁴⁷⁸A ⁴⁷⁹A ⁴⁸⁰A ⁴⁸¹A ⁴⁸²A ⁴⁸³A ⁴⁸⁴A ⁴⁸⁵A ⁴⁸⁶A ⁴⁸⁷A ⁴⁸⁸A ⁴⁸⁹A ⁴⁹⁰A ⁴⁹¹A ⁴⁹²A ⁴⁹³A ⁴⁹⁴A ⁴⁹⁵A ⁴⁹⁶A ⁴⁹⁷A ⁴⁹⁸A ⁴⁹⁹A ⁵⁰⁰A ⁵⁰¹A ⁵⁰²A ⁵⁰³A ⁵⁰⁴A ⁵⁰⁵A ⁵⁰⁶A ⁵⁰⁷A ⁵⁰⁸A ⁵⁰⁹A ⁵¹⁰A ⁵¹¹A ⁵¹²A ⁵¹³A ⁵¹⁴A ⁵¹⁵A ⁵¹⁶A ⁵¹⁷A ⁵¹⁸A ⁵¹⁹A ⁵²⁰A ⁵²¹A ⁵²²A ⁵²³A ⁵²⁴A ⁵²⁵A ⁵²⁶A ⁵²⁷A ⁵²⁸A ⁵²⁹A ⁵³⁰A ⁵³¹A ⁵³²A ⁵³³A ⁵³⁴A ⁵³⁵A ⁵³⁶A ⁵³⁷A ⁵³⁸A ⁵³⁹A ⁵⁴⁰A ⁵⁴¹A ⁵⁴²A ⁵⁴³A ⁵⁴⁴A ⁵⁴⁵A ⁵⁴⁶A ⁵⁴⁷A ⁵⁴⁸A ⁵⁴⁹A ⁵⁵⁰A ⁵⁵¹A ⁵⁵²A ⁵⁵³A ⁵⁵⁴A ⁵⁵⁵A ⁵⁵⁶A ⁵⁵⁷A ⁵⁵⁸A ⁵⁵⁹A ⁵⁶⁰A ⁵⁶¹A ⁵⁶²A ⁵⁶³A ⁵⁶⁴A ⁵⁶⁵A ⁵⁶⁶A ⁵⁶⁷A ⁵⁶⁸A ⁵⁶⁹A ⁵⁷⁰A ⁵⁷¹A ⁵⁷²A ⁵⁷³A ⁵⁷⁴A ⁵⁷⁵A ⁵⁷⁶A ⁵⁷⁷A ⁵⁷⁸A ⁵⁷⁹A ⁵⁸⁰A ⁵⁸¹A ⁵⁸²A ⁵⁸³A ⁵⁸⁴A ⁵⁸⁵A ⁵⁸⁶A ⁵⁸⁷A ⁵⁸⁸A ⁵⁸⁹A ⁵⁹⁰A ⁵⁹¹A ⁵⁹²A ⁵⁹³A ⁵⁹⁴A ⁵⁹⁵A ⁵⁹⁶A ⁵⁹⁷A ⁵⁹⁸A ⁵⁹⁹A ⁶⁰⁰A ⁶⁰¹A ⁶⁰²A ⁶⁰³A ⁶⁰⁴A ⁶⁰⁵A ⁶⁰⁶A ⁶⁰⁷A ⁶⁰⁸A ⁶⁰⁹A ⁶¹⁰A ⁶¹¹A ⁶¹²A ⁶¹³A ⁶¹⁴A ⁶¹⁵A ⁶¹⁶A ⁶¹⁷A ⁶¹⁸A ⁶¹⁹A ⁶²⁰A ⁶²¹A ⁶²²A ⁶²³A ⁶²⁴A ⁶²⁵A ⁶²⁶A ⁶²⁷A ⁶²⁸A ⁶²⁹A ⁶³⁰A ⁶³¹A ⁶³²A ⁶³³A ⁶³⁴A ⁶³⁵A ⁶³⁶A ⁶³⁷A ⁶³⁸A ⁶³⁹A ⁶⁴⁰A ⁶⁴¹A ⁶⁴²A ⁶⁴³A ⁶⁴⁴A ⁶⁴⁵A ⁶⁴⁶A ⁶⁴⁷A ⁶⁴⁸A ⁶⁴⁹A ⁶⁵⁰A ⁶⁵¹A ⁶⁵²A ⁶⁵³A ⁶⁵⁴A ⁶⁵⁵A ⁶⁵⁶A ⁶⁵⁷A ⁶⁵⁸A ⁶⁵⁹A ⁶⁶⁰A ⁶⁶¹A ⁶⁶²A ⁶⁶³A ⁶⁶⁴A ⁶⁶⁵A ⁶⁶⁶A ⁶⁶⁷A ⁶⁶⁸A ⁶⁶⁹A ⁶⁷⁰A ⁶⁷¹A ⁶⁷²A ⁶⁷³A ⁶⁷⁴A ⁶⁷⁵A ⁶⁷⁶A ⁶⁷⁷A ⁶⁷⁸A ⁶⁷⁹A ⁶⁸⁰A ⁶⁸¹A ⁶⁸²A ⁶⁸³A ⁶⁸⁴A ⁶⁸⁵A ⁶⁸⁶A ⁶⁸⁷A ⁶⁸⁸A ⁶⁸⁹A ⁶⁹⁰A ⁶⁹¹A ⁶⁹²A ⁶⁹³A ⁶⁹⁴A ⁶⁹⁵A ⁶⁹⁶A ⁶⁹⁷A ⁶⁹⁸A ⁶⁹⁹A ⁷⁰⁰A ⁷⁰¹A ⁷⁰²A ⁷⁰³A ⁷⁰⁴A ⁷⁰⁵A ⁷⁰⁶A ⁷⁰⁷A ⁷⁰⁸A ⁷⁰⁹A ⁷¹⁰A ⁷¹¹A ⁷¹²A ⁷¹³A ⁷¹⁴A ⁷¹⁵A ⁷¹⁶A ⁷¹⁷A ⁷¹⁸A ⁷¹⁹A ⁷²⁰A ⁷²¹A ⁷²²A ⁷²³A ⁷²⁴A ⁷²⁵A ⁷²⁶A ⁷²⁷A ⁷²⁸A ⁷²⁹A ⁷³⁰A ⁷³¹A ⁷³²A ⁷³³A ⁷³⁴A ⁷³⁵A ⁷³⁶A ⁷³⁷A ⁷³⁸A ⁷³⁹A ⁷⁴⁰A ⁷⁴¹A ⁷⁴²A ⁷⁴³A ⁷⁴⁴A ⁷⁴⁵A ⁷⁴⁶A ⁷⁴⁷A ⁷⁴⁸A ⁷⁴⁹A ⁷⁵⁰A ⁷⁵¹A ⁷⁵²A ⁷⁵³A ⁷⁵⁴A ⁷⁵⁵A ⁷⁵⁶A ⁷⁵⁷A ⁷⁵⁸A ⁷⁵⁹A ⁷⁶⁰A ⁷⁶¹A ⁷⁶²A ⁷⁶³A ⁷⁶⁴A ⁷⁶⁵A ⁷⁶⁶A ⁷⁶⁷A ⁷⁶⁸A ⁷⁶⁹A ⁷⁷⁰A ⁷⁷¹A ⁷⁷²A ⁷⁷³A ⁷⁷⁴A ⁷⁷⁵A ⁷⁷⁶A ⁷⁷⁷A ⁷⁷⁸A ⁷⁷⁹A ⁷⁸⁰A ⁷⁸¹A ⁷⁸²A ⁷⁸³A ⁷⁸⁴A ⁷⁸⁵A ⁷⁸⁶A ⁷⁸⁷A ⁷⁸⁸A ⁷⁸⁹A ⁷⁹⁰A ⁷⁹¹A ⁷⁹²A ⁷⁹³A ⁷⁹⁴A ⁷⁹⁵A ⁷⁹⁶A ⁷⁹⁷A ⁷⁹⁸A ⁷⁹⁹A ⁸⁰⁰A ⁸⁰¹A ⁸⁰²A ⁸⁰³A ⁸⁰⁴A ⁸⁰⁵A ⁸⁰⁶A ⁸⁰⁷A ⁸⁰⁸A ⁸⁰⁹A ⁸¹⁰A ⁸¹¹A ⁸¹²A ⁸¹³A ⁸¹⁴A ⁸¹⁵A ⁸¹⁶A ⁸¹⁷A ⁸¹⁸A ⁸¹⁹A ⁸²⁰A ⁸²¹A ⁸²²A ⁸²³A ⁸²⁴A ⁸²⁵A ⁸²⁶A ⁸²⁷A ⁸²⁸A ⁸²⁹A ⁸³⁰A ⁸³¹A ⁸³²A ⁸³³A ⁸³⁴A ⁸³⁵A ⁸³⁶A ⁸³⁷A ⁸³⁸A ⁸³⁹A ⁸⁴⁰A ⁸⁴¹A ⁸⁴²A ⁸⁴³A ⁸⁴⁴A ⁸⁴⁵A ⁸⁴⁶A ⁸⁴⁷A ⁸⁴⁸A ⁸⁴⁹A ⁸⁵⁰A ⁸⁵¹A ⁸⁵²A ⁸⁵³A ⁸⁵⁴A ⁸⁵⁵A ⁸⁵⁶A ⁸⁵⁷A ⁸⁵⁸A ⁸⁵⁹A ⁸⁶⁰A ⁸⁶¹A ⁸⁶²A ⁸⁶³A ⁸⁶⁴A ⁸⁶⁵A ⁸⁶⁶A ⁸⁶⁷A ⁸⁶⁸A ⁸⁶⁹A ⁸⁷⁰A ⁸⁷¹A ⁸⁷²A ⁸⁷³A ⁸⁷⁴A ⁸⁷⁵A ⁸⁷⁶A ⁸⁷⁷A ⁸⁷⁸A ⁸⁷⁹A ⁸⁸⁰A ⁸⁸¹A ⁸⁸²A ⁸⁸³A ⁸⁸⁴A ⁸⁸⁵A ⁸⁸⁶A ⁸⁸⁷A ⁸⁸⁸A ⁸⁸⁹A ⁸⁹⁰A ⁸⁹¹A ⁸⁹²A ⁸⁹³A ⁸⁹⁴A ⁸⁹⁵A ⁸⁹⁶A ⁸⁹⁷A ⁸⁹⁸A ⁸⁹⁹A ⁹⁰⁰A ⁹⁰¹A ⁹⁰²A ⁹⁰³A ⁹⁰⁴A ⁹⁰⁵A ⁹⁰⁶A ⁹⁰⁷A ⁹⁰⁸A ⁹⁰⁹A ⁹¹⁰A ⁹¹¹A ⁹¹²A ⁹¹³A ⁹¹⁴A ⁹¹⁵A ⁹¹⁶A ⁹¹⁷A ⁹¹⁸A ⁹¹⁹A ⁹²⁰A ⁹²¹A ⁹²²A ⁹²³A ⁹²⁴A ⁹²⁵A ⁹²⁶A ⁹²⁷A ⁹²⁸A ⁹²⁹A ⁹³⁰A ⁹³¹A ⁹³²A ⁹³³A ⁹³⁴A ⁹³⁵A ⁹³⁶A ⁹³⁷A ⁹³⁸A ⁹³⁹A ⁹⁴⁰A ⁹⁴¹A ⁹⁴²A ⁹⁴³A ⁹⁴⁴A ⁹⁴⁵A ⁹⁴⁶A ⁹⁴⁷A ⁹⁴⁸A ⁹⁴⁹A ⁹⁵⁰A ⁹⁵¹A ⁹⁵²A ⁹⁵³A ⁹⁵⁴A ⁹⁵⁵A ⁹⁵⁶A ⁹⁵⁷A ⁹⁵⁸A ⁹⁵⁹A ⁹⁶⁰A ⁹⁶¹A ⁹⁶²A ⁹⁶³A ⁹⁶⁴A ⁹⁶⁵A ⁹⁶⁶A ⁹⁶⁷A ⁹⁶⁸A ⁹⁶⁹A ⁹⁷⁰A ⁹⁷¹A ⁹⁷²A ⁹⁷³A ⁹⁷⁴A ⁹⁷⁵A ⁹⁷⁶A ⁹⁷⁷A ⁹⁷⁸A ⁹⁷⁹A ⁹⁸⁰A ⁹⁸¹A ⁹⁸²A ⁹⁸³A ⁹⁸⁴A ⁹⁸⁵A ⁹⁸⁶A ⁹⁸⁷A ⁹⁸⁸A ⁹⁸⁹A ⁹⁹⁰A ⁹⁹¹A ⁹⁹²A ⁹⁹³A ⁹⁹⁴A ⁹⁹⁵A ⁹⁹⁶A ⁹⁹⁷A ⁹⁹⁸A ⁹⁹⁹A ¹⁰⁰⁰A ¹⁰⁰¹A ¹⁰⁰²A ¹⁰⁰³A ¹⁰⁰⁴A ¹⁰⁰⁵A ¹⁰⁰⁶A ¹⁰⁰⁷A ¹⁰⁰⁸A ¹⁰⁰⁹A ¹⁰¹⁰A ¹⁰¹¹A ¹⁰¹²A ¹⁰¹³A ¹⁰¹⁴A ¹⁰¹⁵A ¹⁰¹⁶A ¹⁰¹⁷A ¹⁰¹⁸A ¹⁰¹⁹A ¹⁰²⁰A ¹⁰²¹A ¹⁰²²A ¹⁰²³A ¹⁰²⁴A ¹⁰²⁵A ¹⁰²⁶A ¹⁰²⁷A ¹⁰²⁸A ¹⁰²⁹A ¹⁰³⁰A ¹⁰³¹A ¹⁰³²A ¹⁰³³A ¹⁰³⁴A ¹⁰³⁵A ¹⁰³⁶A ¹⁰³⁷A ¹⁰³⁸A ¹⁰³⁹A ¹⁰⁴⁰A ¹⁰⁴¹A ¹⁰⁴²A ¹⁰⁴³A ¹⁰⁴⁴A ¹⁰⁴⁵A ¹⁰⁴⁶A ¹⁰⁴⁷A ¹⁰⁴⁸A ¹⁰⁴⁹A ¹⁰⁵⁰A ¹⁰⁵¹A ¹⁰⁵²A ¹⁰⁵³A ¹⁰⁵⁴A ¹⁰⁵⁵A ¹⁰⁵⁶A ¹⁰⁵⁷A ¹⁰⁵⁸A ¹⁰⁵⁹A ¹⁰⁶⁰A ¹⁰⁶¹A ¹⁰⁶²A ¹⁰⁶³A ¹⁰⁶⁴A ¹⁰⁶⁵A ¹⁰⁶⁶A ¹⁰⁶⁷A ¹⁰⁶⁸A ¹⁰⁶⁹A ¹⁰⁷⁰A ¹⁰⁷¹A ¹⁰⁷²A ¹⁰⁷³A ¹⁰⁷⁴A ¹⁰⁷⁵A ¹⁰⁷⁶A ¹⁰⁷⁷A ¹⁰⁷⁸A ¹⁰⁷⁹A ¹⁰⁸⁰A ¹⁰⁸¹A ¹⁰⁸²A ¹⁰⁸³A ¹⁰⁸⁴A ¹⁰⁸⁵A ¹⁰⁸⁶A ¹⁰⁸⁷A ¹⁰⁸⁸A ¹⁰⁸⁹A ¹⁰⁹⁰A ¹⁰⁹¹A ¹⁰⁹²A ¹⁰⁹³A ¹⁰⁹⁴A ¹⁰⁹⁵A ¹⁰⁹⁶A ¹⁰⁹⁷A ¹⁰⁹⁸A ¹⁰⁹⁹A ¹¹⁰⁰A ¹¹⁰¹A ¹¹⁰²A ¹¹⁰³A ¹¹⁰⁴A ¹¹⁰⁵A ¹¹⁰⁶A ¹¹⁰⁷A ¹¹⁰⁸A ¹¹⁰⁹A ¹¹¹⁰A ¹¹¹¹A ¹¹¹²A ¹¹¹³A ¹¹¹⁴A ¹¹¹⁵A ¹¹¹⁶A ¹¹¹⁷A ¹¹¹⁸A ¹¹¹⁹A ¹¹²⁰A ¹¹²¹A ¹¹²²A ¹¹²³A ¹¹²⁴A ¹¹²⁵A ¹¹²⁶A ¹¹²⁷A ¹¹²⁸A ¹¹²⁹A ¹¹³⁰A ¹¹³¹A ¹¹³²A ¹¹³³A ¹¹³⁴A ¹¹³⁵A ¹¹³⁶A ¹¹³⁷A ¹¹³⁸A ¹¹³⁹A ¹¹⁴⁰A ¹¹⁴¹A ¹¹⁴²A ¹¹⁴³A ¹¹⁴⁴A ¹¹⁴⁵A ¹¹⁴⁶A ¹¹⁴⁷A ¹¹⁴⁸A ¹¹⁴⁹A ¹¹⁵⁰A ¹¹⁵¹A ¹¹⁵²A ¹¹⁵³A ^{1154</sup}

In progress

Assignee
Shei

Assign to me

Comment

Respond to customer Internal comment

Your comments will not be visible to customers on the portal.

Style B I U A ~~A~~ ^A _A Ø \equiv \equiv \oplus \ominus

Incidencia en progreso

preview · syntax help

In progress Cancel

< Back TEST-1

Descarga de archivo malicioso a través de dominio sospechoso

Create subtask Link issue Add form ...

Shei raised this request via Jira

[View request in portal](#)

[Hide details](#)

Description

El usuario Juan Perez con IP 192.168.1.100 ha descargado un archivo malicioso desde el dominio sospechoso:

- URL del dominio malicioso: www.dominio-malicioso.com
- Nombre del archivo: malicioso.exe
- Hash del archivo: f5d3ffab-c0a2-4e9d-a15e-2b9d7a123456

Por favor, investiguen si es malicioso y reporten el resultado.

Similar requests

Activity

Show: All Comments History Work log Approvals

Newest first ↴



Add internal note / Reply to customer



Pro tip: press M to comment



Shei 9 seconds ago + Internal note

Incidencia en progreso

Edit · Delete ·

Tarea 4:

Tenemos el incidente actualmente en progreso. En la ventana de la derecha podemos consultar varias propiedades de la incidencia: Prioridad, Urgencia, Impacto, etc. Por defecto nos sale una prioridad Medium, pero imagina que conocemos la severidad del incidente. Los analistas de seguridad muchas veces tienen que hacer estas acciones con alertas que llegan conociendo su alcance. Prueba a cambiar los campos de prioridad, urgencia e impacto a High, High y Minor/Localized respectivamente y manda una captura de ello.

Request Type	Emailed request
Priority	Medium
Urgency	None
Impact	None
Affected services <small> ⓘ</small>	Add service
Pending reason	None

Fíjate dentro de esta misma ventana en el apartado llamado SLAs. ¿Qué SLAs tienes puestos por defecto? ¿Qué crees que significan? Al cambiar la prioridad y actualizar la página, ¿cambian también los SLAs?

Por último, cambia el estado de la incidencia de In Progress a Resolved. Para ello, tendremos que dar un código de resolución. Estos códigos varían entre diferentes herramientas de ITSM. En este caso lo podemos poner como Done. En Linked Issues no hace falta poner nada ya que no hay más incidentes relacionados. Por último, añadimos una nota en Respond to Customer para confirmar que la incidencia ha sido resuelta.

Ejemplo: “Hola, le informamos de que el incidente ha sido resuelto y la URL ha sido blacklisteada”. Asegúrate de que se genera correctamente.

¿De qué color aparece el comentario al cliente? ¿Se han cumplido los SLA establecidos?

Actualización de Incidencia en Jira

Objetivo: Cambiar las propiedades de la incidencia, verificar los SLAs, y resolver la incidencia.

Pasos Seguidos:

1. Cambio de Prioridad, Urgencia e Impacto:

- Con la incidencia en progreso, navega a la sección de propiedades a la derecha.
- Cambia los siguientes campos:
 - **Prioridad:** High
 - **Urgencia:** High
 - **Impacto:** Minor/Localized

2. Verificación de SLAs:

- Revisa los SLAs establecidos por defecto. En este caso, los SLAs por defecto son:
 - **Time to first response:** Tiempo para la primera respuesta.
 - **Time to resolution:** Tiempo para resolver la incidencia.
- Los SLAs indican los tiempos máximos permitidos para la primera respuesta y la resolución de la incidencia. Estos parámetros ayudan a garantizar que las incidencias se gestionen de manera oportuna.
- Después de cambiar la prioridad y actualizar la página, verificamos si los SLAs cambiaron en función de la nueva prioridad. Observamos que los SLAs se ajustaron para reflejar tiempos de respuesta más rápidos debido a la mayor prioridad asignada.

3. Resolución de la Incidencia:

- Cambia el estado de la incidencia de “In Progress” a “Resolved”.
- Selecciona el código de resolución como “Done”.
- Añade una nota en “Respond to Customer” para confirmar que la incidencia ha sido resuelta:
 - **Mensaje:** “Hola, le informamos de que el incidente ha sido resuelto y la URL ha sido blacklisted.”

Respuesta:

- **Color del Comentario al Cliente:** El comentario al cliente aparece sin color.
- **Cumplimiento de SLAs:** Los SLAs se han cumplido, ya que el tiempo de resolución del incidente ha sido por debajo de los límites de seguridad de respuesta establecidos.

Con estos pasos, la incidencia ha sido actualizada correctamente en términos de prioridad, urgencia e impacto, y ha sido resuelta siguiendo los procedimientos adecuados.

SLAs

- 29 Jul 12:42 ⏱ Time to first response within 8h
- 01 Aug 16:42 ⏱ Time to resolution within 36h

Pinned fields

Click on the ⌂ next to a field label to start pinning.

Details

Assignee	Shei
Reporter	Shei
Request Type	Emailed request
Priority	High
Urgency	High
Impact	Minor / Localized
Affected services ⓘ	+ Add service
Pending reason	None

In Progress ⚡ Actions

- Pending → PENDING
- Cancel request → CANCELLED
- Resolve this issue → RESOLVED

View workflow

Resolve this issue

⚠ Request resolved

Resolution

✓ Please select... ⓘ

- Done
- Won't Do
- Duplicate
- Declined

Resolve this issue

⚠ Request resolved

Resolution

Done ?

Linked Issues

blocks ?

Issue

+

Begin typing to search for issues to link. If you leave it blank, no link will be made.

Comment

Respond to customer Internal comment

Your comment will be visible to customers. Embed attachments to make them visible to customers.

Style B I U A ^A A ^A A A A A A

Estimado cliente, le informamos que el incidente ha sido resuelto, no ha habido consecuencias y la URL ha sido blackisteada.

[preview](#) · [syntax help](#)

Resolve this issue Cancel



You're on the Free plan

UPGRADE

← Back to project

Queues

STARRED

Select the star icon next to your queues to add them here.

TEAM PRIORITY

All open 0

Assigned to me 0

Open tasks 0

⚙ Manage queues

↳ Give feedback

◀ Back TEST-1 ▶ ▼ ▲

Descarga de archivo malicioso a través de dominio sospechoso

✉ Create subtask 🔗 Link issue 📝 Add form ...

👤 Shei raised this request via Jira

[View request in portal](#)

Hide details

Description

El usuario Juan Perez con IP 192.168.1.100 ha descargado un archivo malicioso desde el dominio sospechoso:

- **URL del dominio malicioso:** www.dominio-malicioso.com
- **Nombre del archivo:** malicioso.exe
- **Hash del archivo:** f5d3ffab-c0a2-4e9d-a15e-2b9d7a123456

Por favor, investiguen si es malicioso y reporten el resultado.

Similar requests

Activity

Show: All Comments History Work log Approvals

Newest first ▼

👤 Add internal note / Reply to customer 📎

Pro tip: press M to comment

👤 Shei 3 seconds ago

Estimado cliente, le informamos que el incidente ha sido resuelto, no ha habido consecuencias y la URL ha sido blackisteada.

Edit · Delete · 💬

👤 Shei 14 minutes ago • ✍ Internal note

Incidencia en progreso

Edit · Delete · 💬

Resolved Done Actions

SLAs	
29 Jul 12:42	Time to first response within 8h
01 Aug 16:42	Time to resolution within 36h

Pinned fields

Click on the ↗ next to a field label to start pinning.

Details	
Assignee	👤 Shei
Reporter	👤 Shei
Request Type	✉ Emailed request
Priority	⚠ High
Urgency	High
Impact	Minor / Localized
Affected services	○ + Add service
Pending reason	None

More fields Labels, Request participants, Time trac... ▼

Automation ⚡ Rule executions ▼

Created 28 minutes ago Configure
Updated 6 seconds ago
Resolved 6 seconds ago

Tarea 5:

(Opcional): Invita a un compañero del curso a tu proyecto. Para ello, navega hacia Project Settings > People y selecciona Add People. Puedes preguntar a un compañero/a por su dirección de correo electrónico y añadirlo al proyecto. Lo puedes añadir como Service Desk Team o Administrator. Asegúrate de que no sea Service Desk Customer.

Le llegará una invitación para unirse al correo. Nota: en la versión gratuita de Jira que estamos usando podrás invitar un máximo de 2 personas. Una vez se haya unido, crea un Incidente personalizado como el que creaste anteriormente y asignaselo a tu compañero/a. Comprueba que la persona a la que le asignaste el incidente ha cumplido o no con los SLA.

Si quieres, puedes navegar a Project Settings > SLAs y modificarlos para que sea más fácil / más difícil para esa persona resolverlo. En caso de modificarlos, haz una captura y envíala en el ejercicio.

Pasa también una captura con el incidente asignado a tu compañero/a y su resolución (en caso de que lo haya resuelto).

Si al resolverlo te ha desaparecido el Incidente, dirígete al Board para verlo.

Invitación y Asignación de Incidencia en Jira

Objetivo: Invitar a un compañero al proyecto, asignarle una incidencia y comprobar el cumplimiento de los SLA.

Pasos Seguidos:

1. Invitación de un Compañero:

- Navega a Project Settings y selecciona “People”.
- Hacer clic en “Add People” e ingresar la dirección de correo electrónico del compañero.
- Asigna al compañero el rol de “Service Desk Team” o “Administrator”.

2. Creación y Asignación de Incidencia:

- Crea una nueva incidencia personalizada similar a la creada anteriormente.
- Asigna la incidencia al compañero recién invitado.

3. Verificación de Cumplimiento de SLA:

- Navega a “Project Settings > SLAs” para revisar y, si es necesario, modificar los SLAs para facilitar o dificultar la resolución.
- Verifica el cumplimiento de los SLAs asignados a la incidencia.

4. Capturar de Incidencia Asignada:

- Tomamos una captura de la incidencia asignada al compañero.
- Verificamos si la incidencia ha sido resuelta por el compañero y si se cumplieron los SLAs establecidos.

Respuesta:

Con estos pasos, se ha invitado a un compañero al proyecto, se le ha asignado una incidencia y he verificado el cumplimiento de los SLAs. También he sido invitada al proyecto de una compañera y he resuelto una incidencia que se me ha asignado. La captura muestra el proceso y la resolución exitosa de la incidencia, confirmando la gestión eficiente del proyecto en Jira.

The screenshots show the Jira Project Settings - People page. The top screenshot displays the current list of users, showing one user named 'Shei' with the email 'ftlink42@gmail.com' and a role of 'Administrators'. The bottom screenshot shows a modal dialog for adding a new user, with the search bar containing 'e.g. Maria, maria@company.com' and the role dropdown set to 'Choose role'.

Añadimos la compañera como administradora.

The screenshot shows the 'People' section of a Jira project named 'HackTheWorld'. A modal window titled 'Add people' is open, prompting for a name or email ('kuetara81') and a role ('Choose role'). Below the modal, two project roles are listed: 'Administrators' (selected) and 'Service Desk Customers'. The 'Administrators' role is described as a project role for managing customers.

The screenshot shows the 'People' section of the same Jira project. The 'Add people' modal is now closed, and the role dropdown has been populated with 'Administrators'. The 'Add' button is visible at the bottom of the modal.

The screenshot shows the 'People' section of the Jira project. The list of users includes Ana (role: Administrators) and Shei (role: Administrators). The 'Roles' filter dropdown is visible above the user list.

Name	Email	Role	Action
Ana	-	Administrators	Remove
Shei	ftlink42@gmail.com	Administrators	Remove

Creamos una incidencia que asignamos a la compañera para que resuelva.

Create issue

Required fields are marked with an asterisk *

Project * 1 ...

Issue type * [System] Service request

Learn about issue types

Request type * What's this?

Emailed request
Request received from your email support channel.

Use request type fields ⓘ

Raise this request on behalf of * S Shei

Subject * Incidente de Phising detectado a través de correo electrónico

Body

Normal text | **B** *I* ... | A | ≡ ≡ | 🔗 ✉ @ ⌚ ✉ ↳ ⓘ +

El usuario Maria Pérez (maria.perez@email.com) ha recibido un email con URL sospechosa (www.malicioso.com).
Por favor, investigue el incidente y reporte al cliente.|

Organizations

Select organization

Create another issue Cancel Create

Asignamos la incidencia a la compañera.

The screenshot shows a Jira issue page for a project named 'TEST-2'. The issue title is 'Incidente de Phising detectado a través de correo electrónico'. The status is 'In Progress'. A dropdown menu is open under the 'Assignee' field, which currently displays 'Unassigned'. The dropdown also lists suggestions like 'Shei - ftlink42@gmail.com', 'Automatic', and 'Start Typing for Users'. Other users listed include 'All Users' and 'Ana'. At the bottom of the dropdown, there are links for 'preview' and 'syntax help', along with 'In progress' and 'Cancel' buttons.

Agregamos un comentario interno en la incidencia para la compañera.

The screenshot shows a Jira issue page for 'TEST-2'. The title is 'Incidente de Phising detectado a través de correo electrónico'. The status is 'In Progress'. A modal window is open, titled 'In progress', showing the comment input area. The comment text is 'Por favor, investiga este incidente y informa al cliente.' The 'Internal comment' tab is selected. The 'Respond to customer' tab is also present. The Jira interface includes standard buttons like 'Create subtask', 'Link issue', 'Add form', and '...'. On the right, there's a sidebar with SLAs and a 'Similar requests' section. The bottom right of the modal has 'In progress' and 'Cancel' buttons.

Projects / HackTheWorld / TEST-2

Incidente de Phising detectado a través de correo electrónico

[Create subtask](#) [Link issue](#) [Add form](#) ...

Shei raised this request via Jira [View request in portal](#)

Description
El usuario María Pérez (maria.perez@email.com) ha recibido un email con URL sospechosa (www.malicioso.com).
Por favor, investigue el incidente y reporte al cliente.

Similar requests

Activity
Show: All [Comments](#) History Work log Approvals Newest first ↴

[Add internal note](#) / [Reply to customer](#)

Pro tip: press [M](#) to comment

Shei 25 seconds ago • [Internal note](#)
Por favor, investiga este incidente y informa al cliente.
[Edit](#) · [Delete](#) · [...](#)

In Progress Actions

SLAs

29 Jul 13:24 [Time to first response within 8h](#)

02 Aug 09:24 [Time to resolution within 36h](#)

Pinned fields

Click on the [x](#) next to a field label to start pinning.

Details

Assignee [Ana](#) [Assign to me](#)

Reporter [Shei](#)

Request Type [Emailed request](#)

Priority [High](#)

Urgency [High](#)

Impact [Minor / Localized](#)

Affected services [+ Add service](#)

Pending reason None

La compañera sigue los mismos pasos y me invita a su proyecto, donde crea una incidencia para que resuelva. Recibo la notificación.

Projects Filters Dashboards Teams Assets Apps Create

Search

Projects / PruebasITSM / Project settings

People

Search roles Roles

Name	Email
A Ana	-
S Shei	ftlink42@gmail.com

Notifications Only show unread

Direct Watching

TODAY

[Ana assigned an issue to you 3 minutes ago](#)
[Incidente de Phishing](#)
 PRUEB-2 • In Progress
[+2 updates from Ana](#)

That's all your notifications from the last 30 days.

Pro tip: press [↓ ↑](#) to move through notifications. See all shortcuts

The screenshot shows the Jira Service Management interface. On the left, there's a sidebar with various project management and service delivery options. The main area displays an incident ticket titled "Incidente de Phishing". The ticket details a user report about a phishing attempt where a link was used to impersonate another user. The ticket is currently in "In Progress" status. The right side of the screen shows detailed information about SLAs (Service Level Agreements), pinned fields, and ticket details like assignee, reporter, and priority.

Procedemos a resolverlo mandando una notificación al cliente, siguiendo los mismos pasos anteriores.

This screenshot shows the same incident ticket after some actions have been taken. In the "Actions" section of the right panel, a "Resolve this issue → RESOLVED" option has been selected, changing the status from "Pending" to "PENDING". The ticket details remain the same, showing it was raised by Ana and assigned to Shei.

Jira Service Management

Your work ▾ Projects ▾ Filters ▾ Dashboards ▾ Teams ▾ Assets Apps ▾ Create

Search

PruebasITSM Service project

You're on the Free plan

UPGRADE

Get started Queues Board Calendar NEW Service requests Incidents Problems Changes Post-incident reviews

OPERATIONS Change calendar Services Alerts On-call

KNOWLEDGE Knowledge base Reports

DIRECTORY Channels Customers Invite agents

Projects / PruebasITSM / PRIUEB-2

Incidente de Phishing

Create subtask Link issue Add form

Ana raised this request via Jira View request in portal

Resolve this issue

Request resolved

Resolution Done

Linked Issues blocks

Issue

Similar requests

Activity Show: All Comments

Add internal note Pro tip: press M

Ana 4 minutes ago Se ruega resolución

Comment Respond to customer Internal comment

Your comments will not be visible to customers on the portal.

El incidente ha sido resuelto exitosamente y la URL ha sido blacklisted.

Resolve this issue Cancel

Resolved

SLAs

30 Jul 09:26 1 Time to first response within 12h

26 1 Time to resolution within 48h

Shei Ana

Emailed request Medium

None None

None None

Add service

Reason None

Labels, Request participants, Time tracking, Approvers, Or... Rule executions Configure

Updated 5 minutes ago

PRUEB-2

Incidente de Phishing

Create subtask Link issue Add form

Resolved

SLAs

Time to close after resolution

Response

Lution

Done

The selected resolution is invalid.

blocks

PRUEB-1

Begin typing to search for issues to link. If you leave it blank, no link will be made.

Respond to customer Internal comment

Your comment will be visible to customers. Embed attachments to make them visible to customers.

Add internal note /

Pro tip: press M to comment

Ana 26 July 2024 at 13:21

Se ruega resolución de incidente

Edit · Delete ·

El incidente ha sido resuelto exitosamente y la URL ha sido blacklisted.

Resolve this issue Cancel

Automation Rule executions

Created 26 July 2024 at 13:26
Updated 26 July 2024 at 13:42

Configure

Incidente de Phishing

Resolved ✓ Done Actions

SLAs

- 07 Aug 09:37 Time to close after re... within 60h
- Today 13:35 Time to first response within 12h
- Today 13:37 Time to resolution within 48h

Pinned fields

Click on the **x** next to a field label to start pinning.

Details

Assignee	Shei
Reporter	Ana
Request Type	Emailed request
Priority	Medium
Urgency	None
Impact	None
Affected services	+ Add service
Pending reason	None

More fields Labels, Request participants, Time tracking, App...

Automation Rule executions

Created 26 July 2024 at 13:26 Updated 26 July 2024 at 13:44 Resolved 26 July 2024 at 13:44

Comments

S Add internal note / Reply to customer

Pro tip: press M to comment

S Shei 26 July 2024 at 13:44
El incidente ha sido resuelto exitosamente y la URL ha sido blackisteadada.
Edit · Delete · ⚙️

A Ana 26 July 2024 at 13:29 • Internal note
Se ruega resolución de incidente y reporte del mismo
Edit · Delete · ⚙️

PRUEB

TO DO

IN PROGRESS

DONE 2

- Spear Phishing detectado a través de URL de cliente RESOLVED PRUEB-1
- Incidente de Phishing RESOLVED PRUEB-2

See older issues

Comprobamos la resolución de la tarea asignada a la compañera. Para ver la tarea que se ha asignado a la compañera, volvemos al proyecto y visualizamos el board.

Incidente de Phising detectado a través de correo electrónico

Resolved Done Actions

SLAs

- 05 Aug 13:37 🕒 Time to close after request within 48h
- Today 13:34 ✓ Time to first response within 8h
- Today 13:37 ✓ Time to resolution within 36h

Pinned fields

Click on the ↗ next to a field label to start pinning.

Details

Assignee	A Ana
Reporter	S Shei
Request Type	Emailed request
Priority	High
Urgency	High
Impact	Minor / Localized
Affected services	+ Add service
Pending reason	None

More fields Labels, Request participants, Time tracking, Approvals

Automation ⚡ Rule executions ⚙️ Configure

Created 1 hour ago
Updated 7 seconds ago
Resolved 35 minutes ago

Podemos comprobar que el incidente ha sido resuelto exitosamente de acuerdo con las instrucciones dadas y los SLAs.