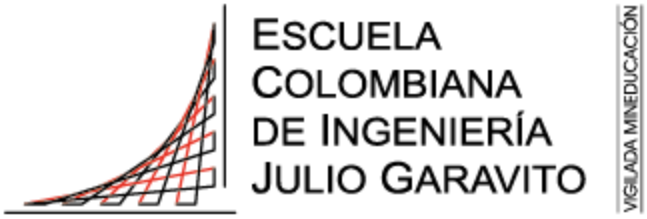


SPTI

Laboratorio 3 – Gestión de Riesgos (Procesos y Activos de TI)

Nicolas Piñeros

Juan Monroy

Febrero 2022

2)

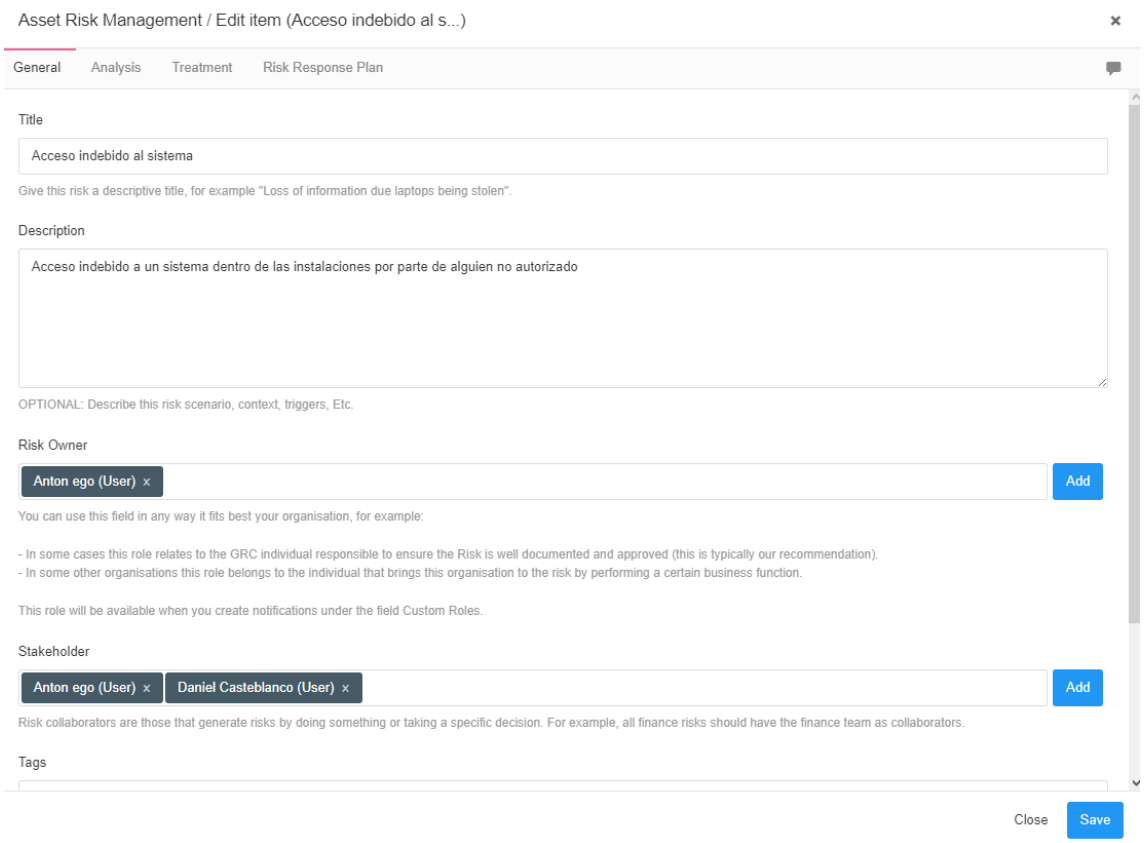
Objetivos: Documentar el proceso de gestión de riesgos con base en el diagrama de activos realizado anteriormente, además de crear mecanismos de control y políticas para poder mitigar los riesgos a un nivel aceptable

3)

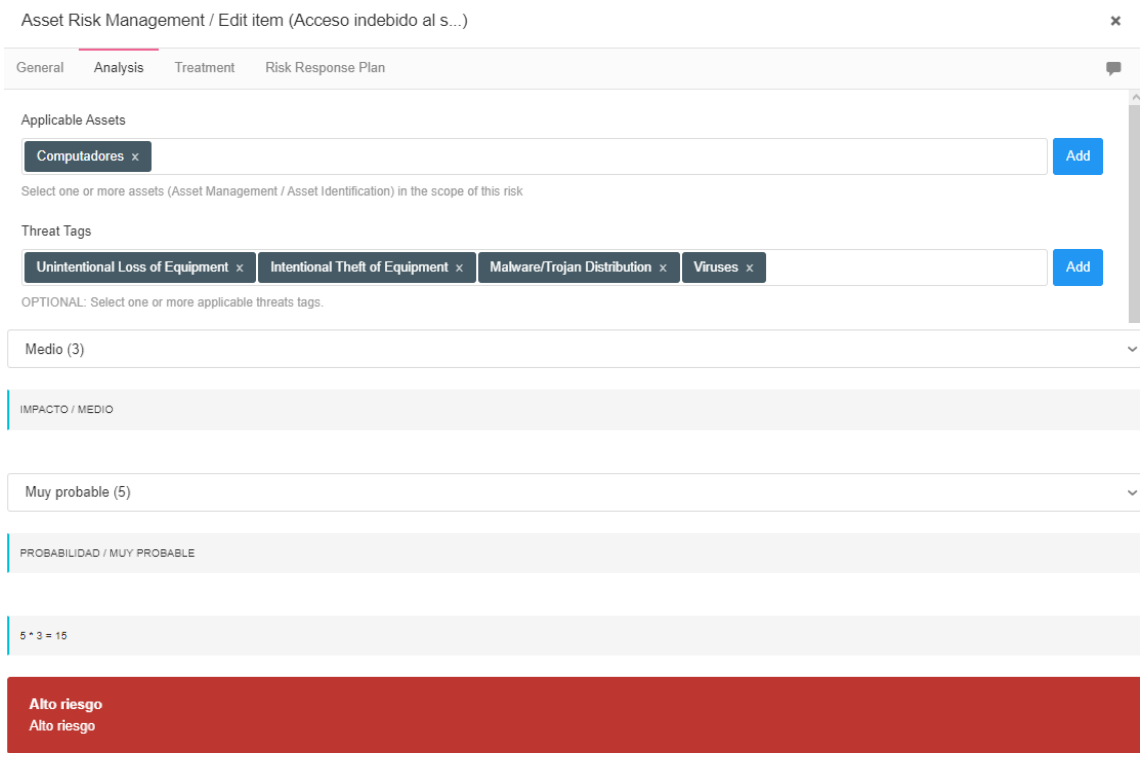
3.1) Primero debemos identificar los riesgos, (y darles una descripción si es necesario), hacer un análisis de este donde pondremos a que activos afecta y que amenazas puede conllevar que suceda el riesgo, luego haremos un tratamiento del riesgo donde pondremos que haremos con el riesgo, aceptarlo, transferirlo, mitigarlo o evadirlo, después podremos poner controles y políticas para controlar el riesgo.

Actions	Status	Reviews	Title	Description
≡	OK	2	Acceso indebido al sistema	Acceso indebido a un sistema dentro de las instalaciones por parte de alguien no autorizado
≡	OK	2	Daño en el proyector	Daño en el videobeam
≡	OK	2	Desastre natural	
≡	OK	2	Daño en el sensor del colisionador	
≡	OK	2	Ataque fisico al servidor	
≡	OK	2	Ciberataque	Robo de informacion
≡	OK	2	Acceso no permitido a la base de datos	
≡	OK	2	Escape de helio liquido	
≡	OK	2	Bugs del Software en el centro de control	

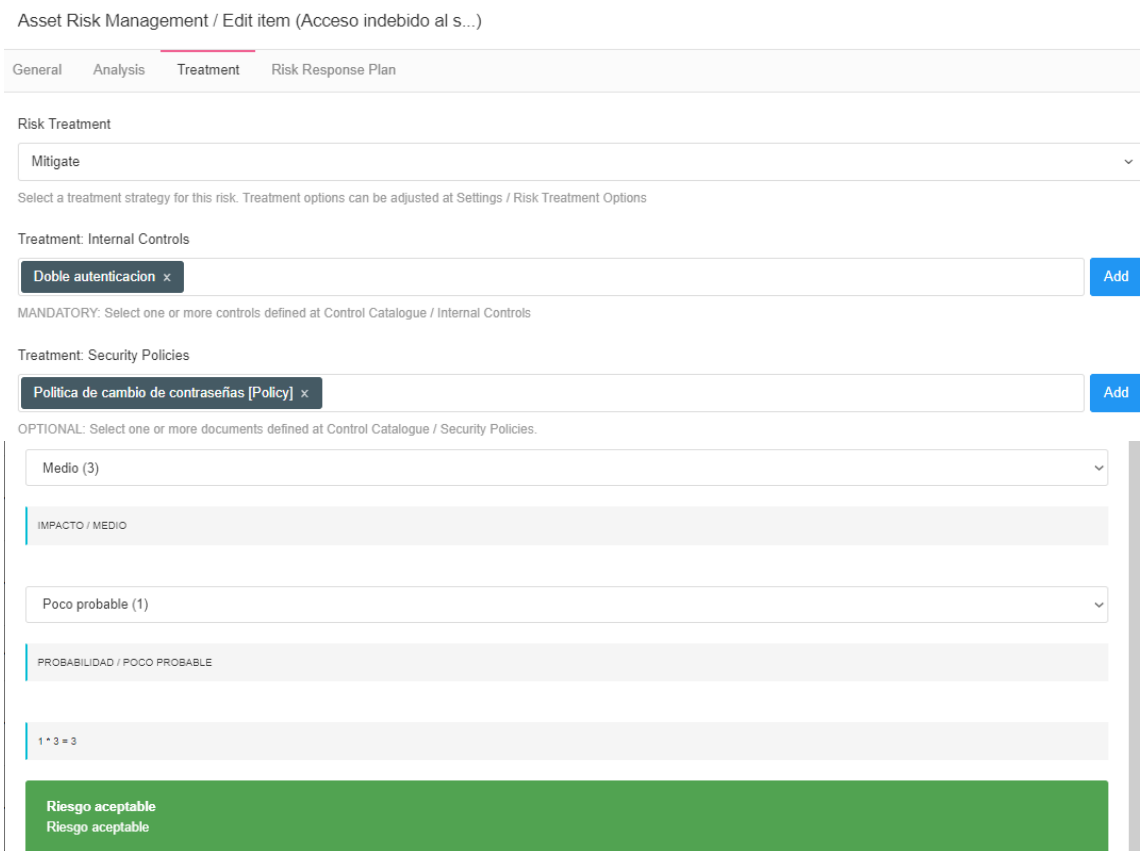
Riesgo 1
General



Analisis

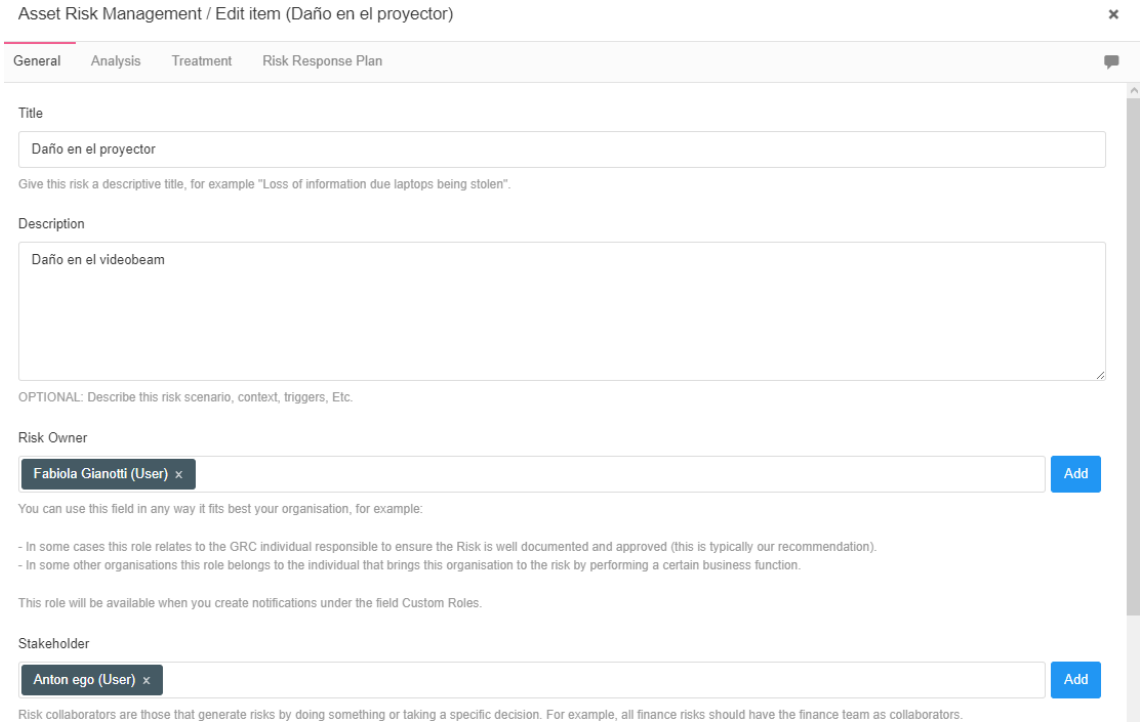


Tratamiento del riesgo

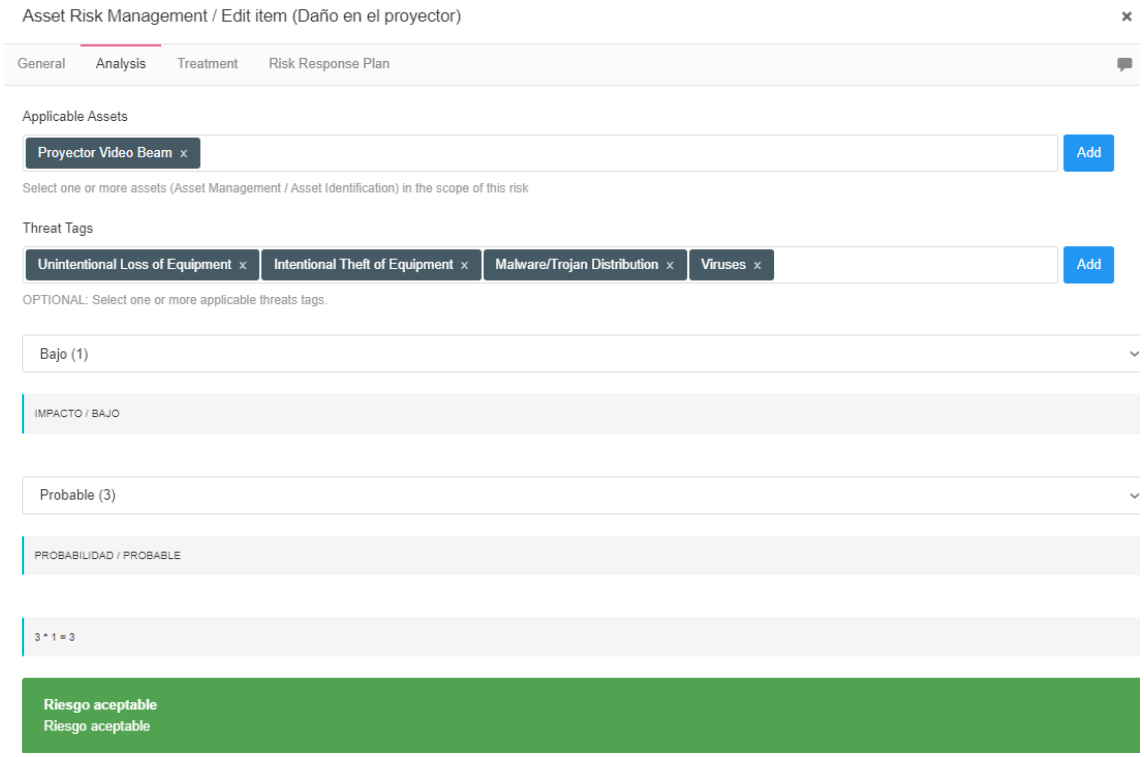


Riesgo 2

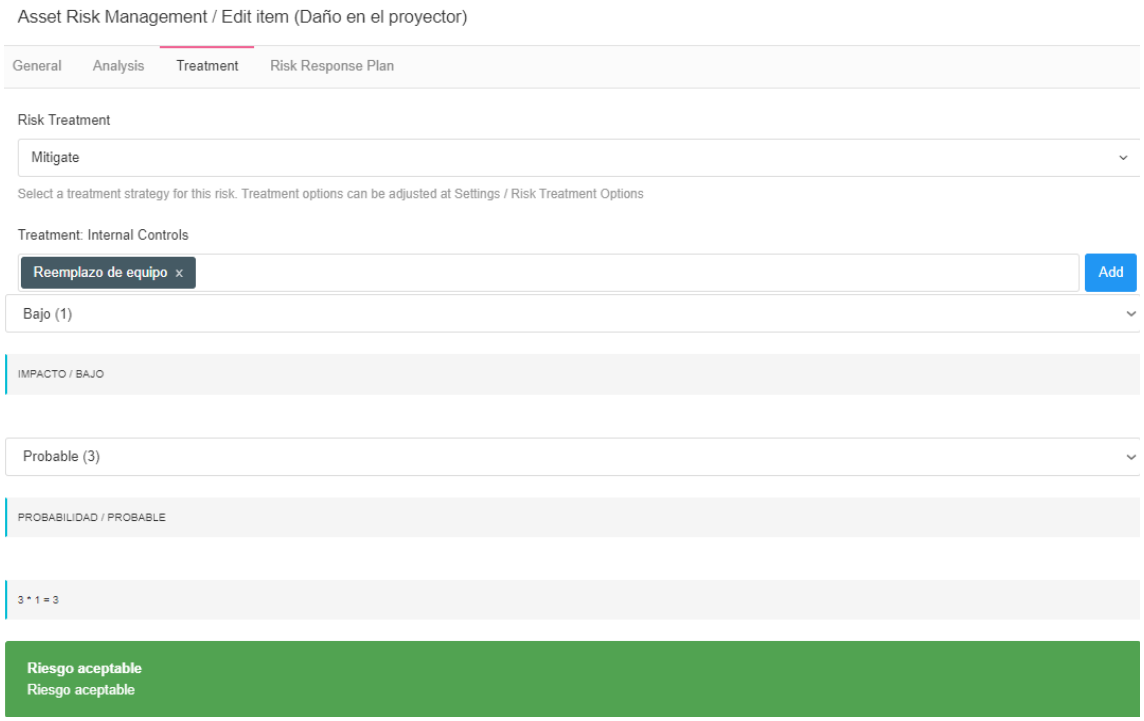
General



Analisis

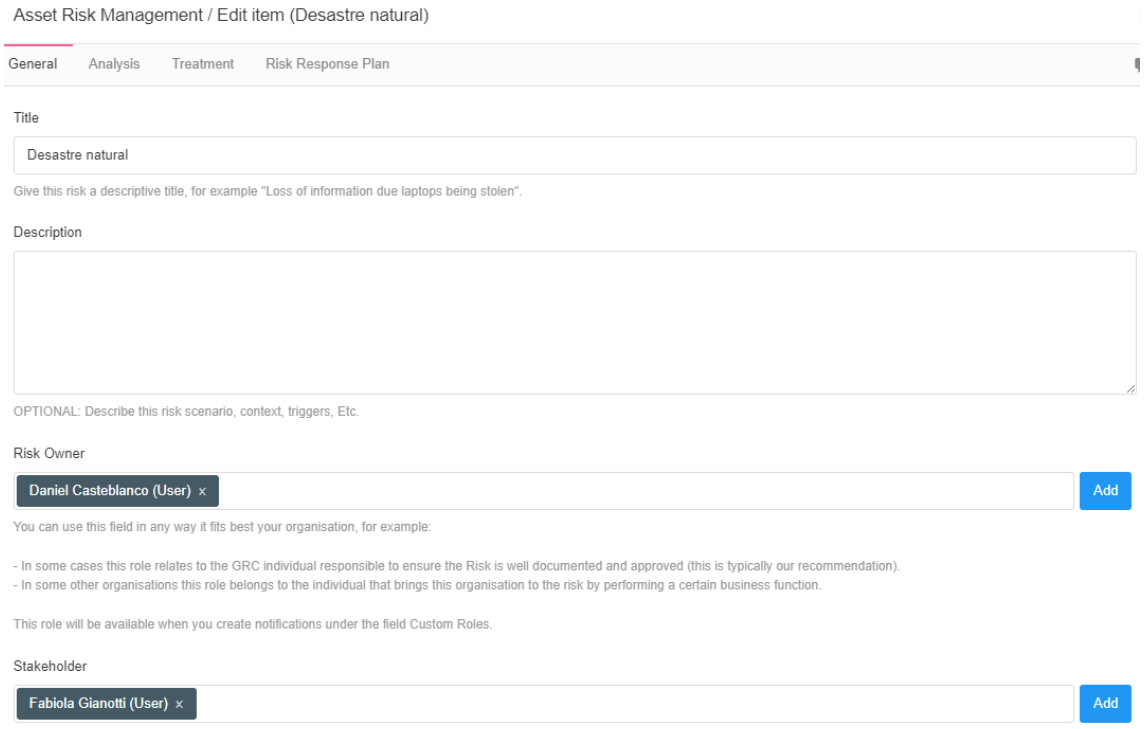


Tratamiento del riesgo

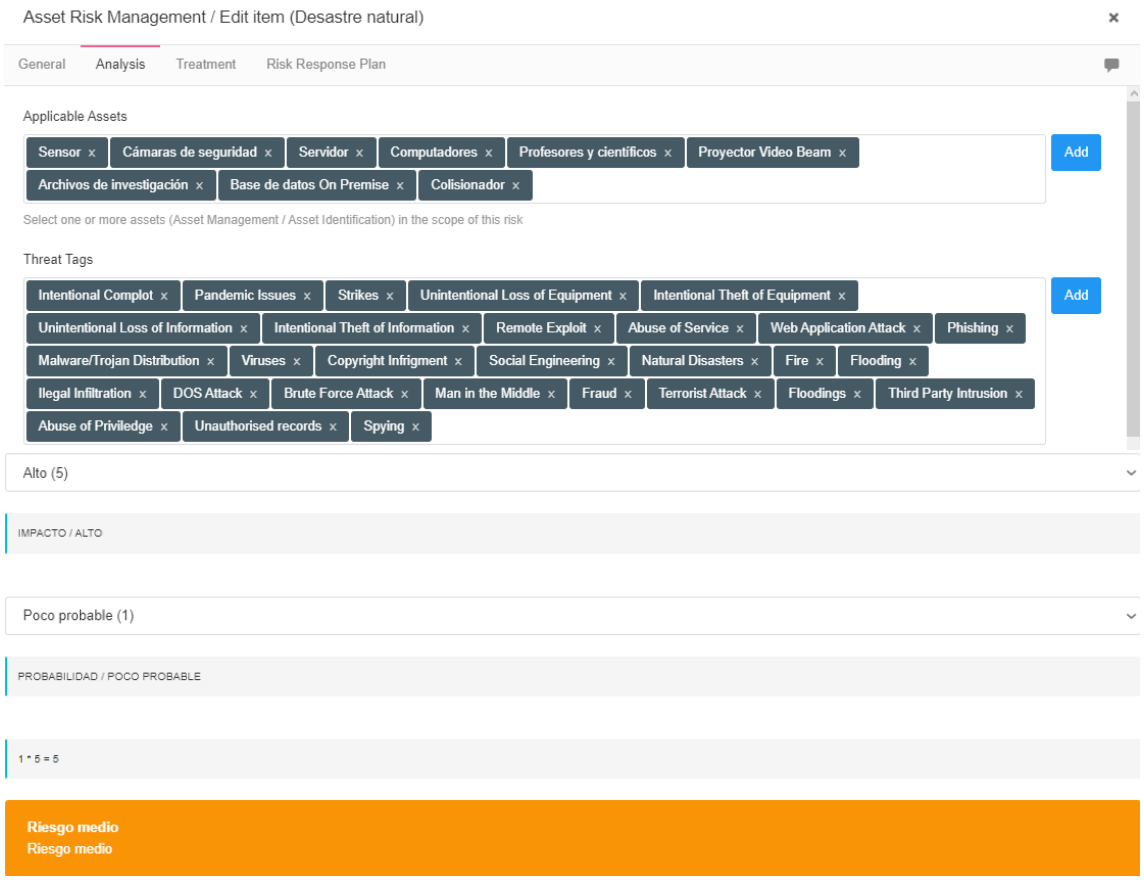


Riesgo 3

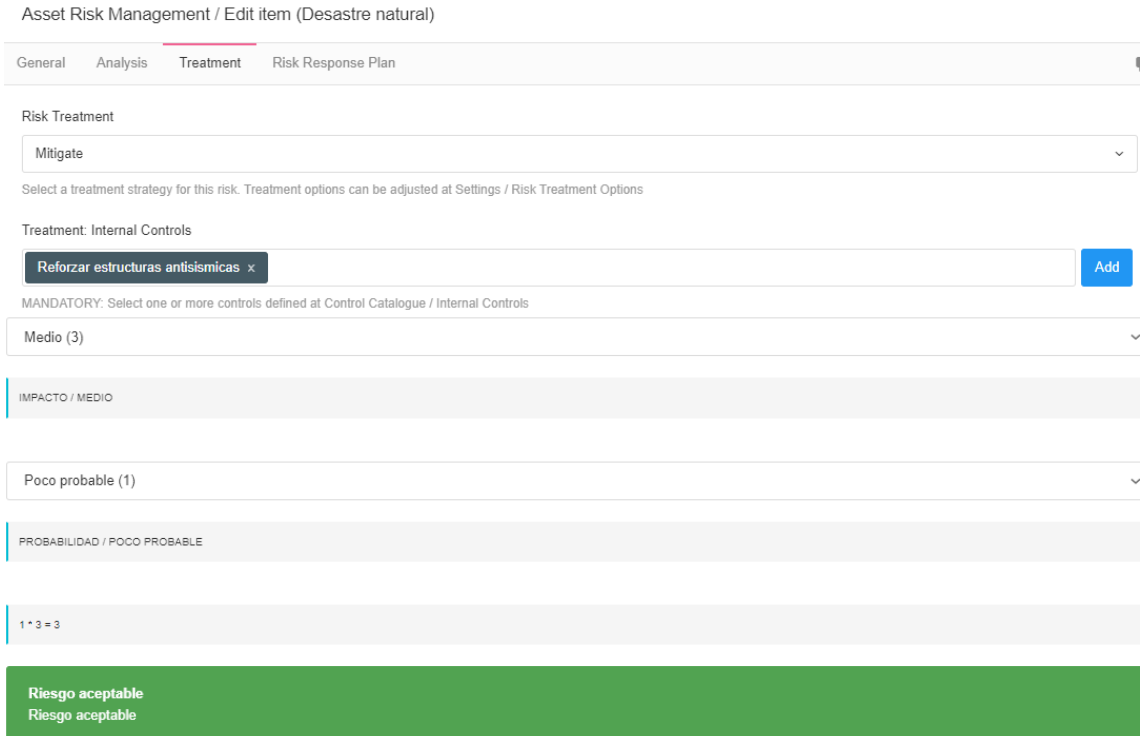
General



Analisis

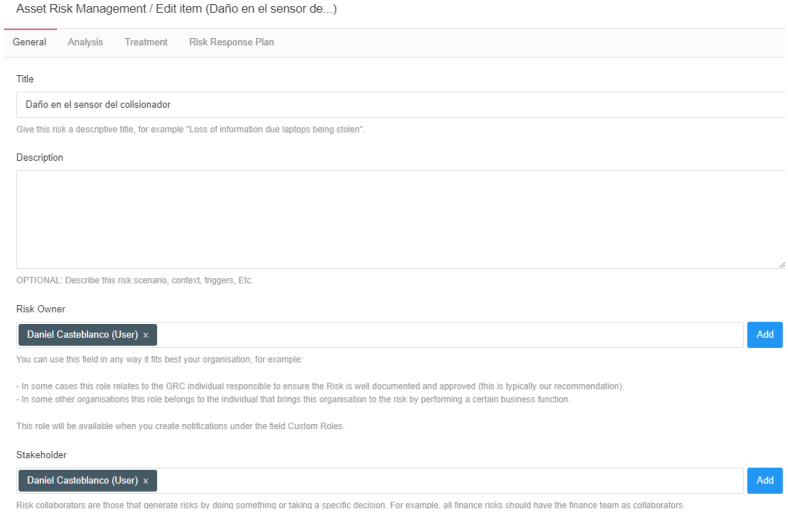


Tratamiento del riesgo



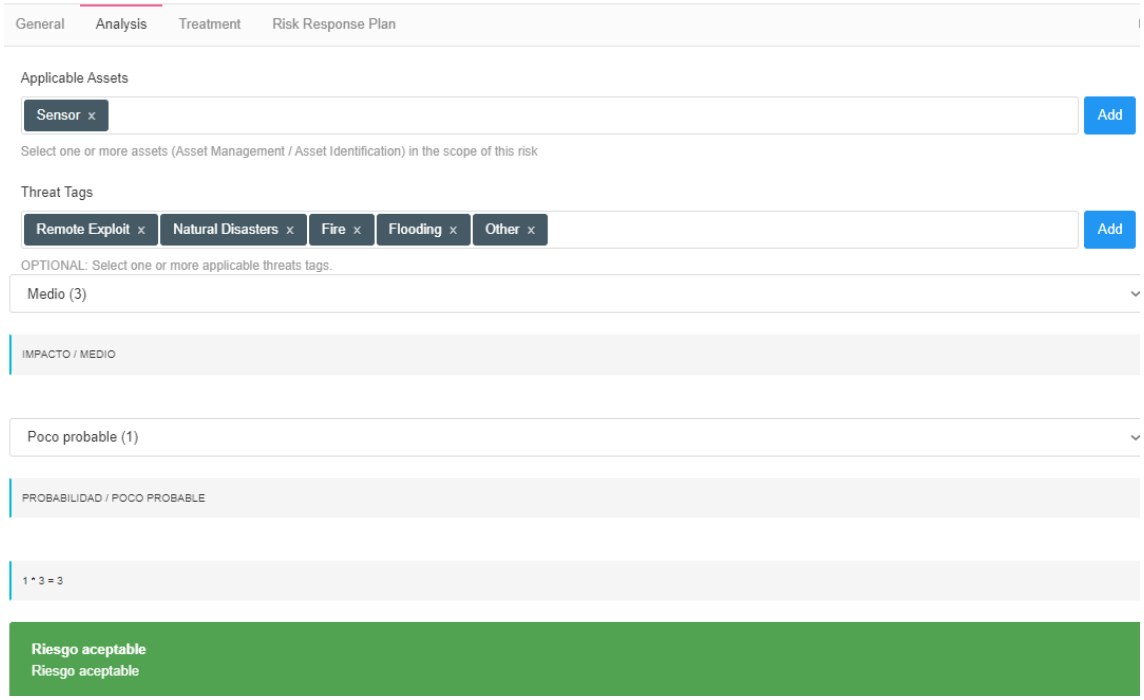
Riesgo 4

General



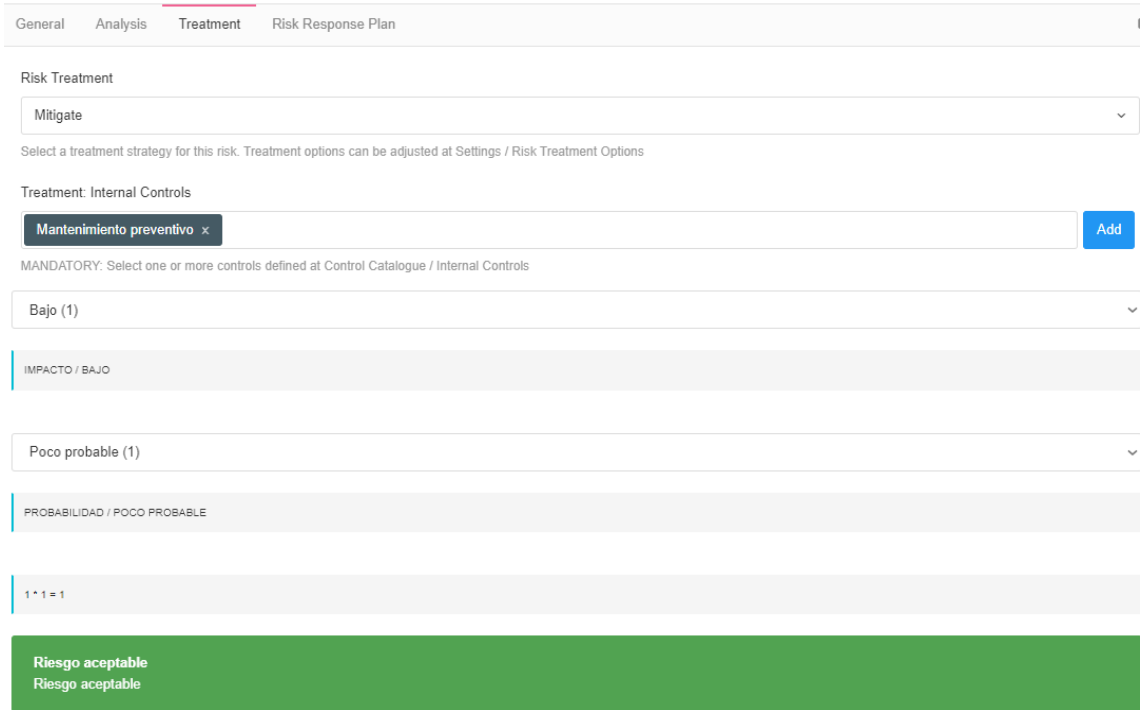
Analisis

Asset Risk Management / Edit item (Daño en el sensor de...)



Tratamiento del riesgo

Asset Risk Management / Edit item (Daño en el sensor de...)



Riesgo 5

General

Asset Risk Management / Edit item (Ataque fisico al ser...)

General | Analysis | Treatment | Risk Response Plan

Title

Ataque fisico al servidor

Give this risk a descriptive title, for example "Loss of information due laptops being stolen".

Description

OPTIONAL: Describe this risk scenario, context, triggers, Etc.

Risk Owner

Fabiola Gianotti (User) ×

Add

You can use this field in any way it fits best your organisation, for example:

- In some cases this role relates to the GRC individual responsible to ensure the Risk is well documented and approved (this is typically our recommendation).
- In some other organisations this role belongs to the individual that brings this organisation to the risk by performing a certain business function.

This role will be available when you create notifications under the field Custom Roles.

Stakeholder

Anton ego (User) ×

Add

Risk collaborators are those that generate risks by doing something or taking a specific decision. For example, all finance risks should have the finance team as collaborators.

Analisis

Asset Risk Management / Edit item (Ataque fisico al ser...)

General | Analysis | Treatment | Risk Response Plan

Applicable Assets

Servidor ×

Add

Select one or more assets (Asset Management / Asset Identification) in the scope of this risk

Threat Tags

Unintentional Loss of Equipment × | Intentional Theft of Equipment × | Malware/Trojan Distribution × | Viruses ×

Add

OPTIONAL: Select one or more applicable threats tags.

Alto (5)

IMPACTO / ALTO

Poco probable (1)

PROBABILIDAD / POCO PROBABLE

1 * 5 = 5

Riesgo medio
Riesgo medio

Tratamiento del riesgo

Asset Risk Management / Edit item (Ataque fisico al ser...)

General | Analysis | Treatment | Risk Response Plan

Risk Treatment

Mitigate

Select a treatment strategy for this risk. Treatment options can be adjusted at Settings / Risk Treatment Options

Treatment: Internal Controls

Detectores de fuego y movimiento ×

Add

MANDATORY: Select one or more controls defined at Control Catalogue / Internal Controls

Medio (3)

IMPACTO / MEDIO

Poco probable (1)

PROBABILIDAD / POCO PROBABLE

1 * 3 = 3

Riesgo aceptable
Riesgo aceptable

Riesgo 6

General

Asset Risk Management / Edit item (Ciberataque)

General | Analysis | Treatment | Risk Response Plan

Title

Ciberataque

Give this risk a descriptive title, for example "Loss of information due laptops being stolen".

Description

Robo de informacion

OPTIONAL: Describe this risk scenario, context, triggers, Etc.

Risk Owner

Anton ego (User) ×

Add

You can use this field in any way it fits best your organisation, for example:

- In some cases this role relates to the GRC individual responsible to ensure the Risk is well documented and approved (this is typically our recommendation).
- In some other organisations this role belongs to the individual that brings this organisation to the risk by performing a certain business function.

This role will be available when you create notifications under the field Custom Roles.

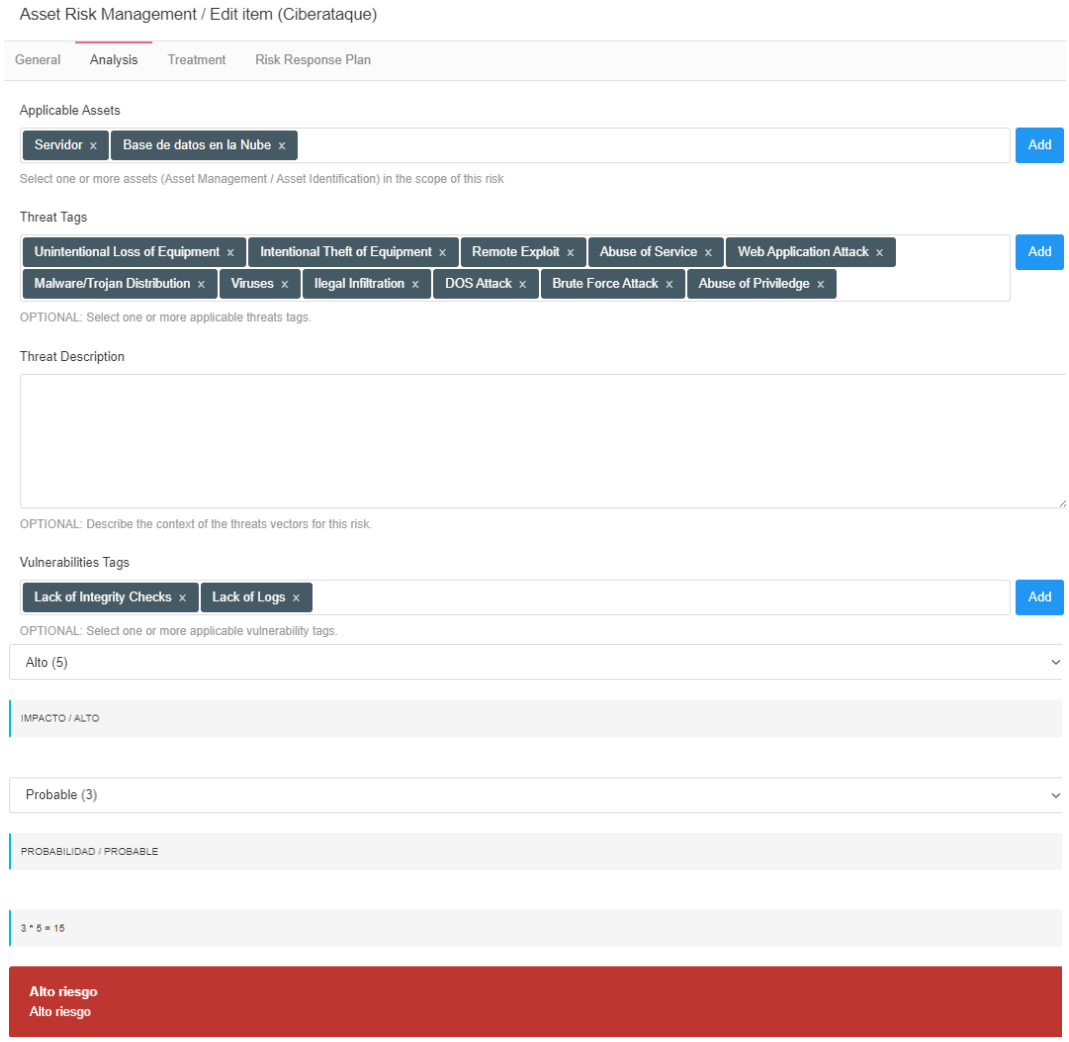
Stakeholder

Anton ego (User) ×

Add

Risk collaborators are those that generate risks by doing something or taking a specific decision. For example, all finance risks should have the finance team as collaborators.

Analisis



Tratamiento del riesgo

Medio (3)

IMPACTO / MEDIO

Probable (3)

PROBABILIDAD / PROBABLE

3 * 3 = 9

Medio riesgo
Medio riesgo

Riesgo 7

General

Asset Risk Management / Edit item (Acceso no permitido ...)

General | Analysis | Treatment | Risk Response Plan

Title

Acceso no permitido a la base de datos

Give this risk a descriptive title, for example "Loss of information due laptops being stolen".

Description

OPTIONAL: Describe this risk scenario, context, triggers, Etc.

Risk Owner

Anton ego (User) ×

Add

You can use this field in any way it fits best your organisation, for example:

- In some cases this role relates to the GRC individual responsible to ensure the Risk is well documented and approved (this is typically our recommendation).
- In some other organisations this role belongs to the individual that brings this organisation to the risk by performing a certain business function.

This role will be available when you create notifications under the field Custom Roles.

Stakeholder

Anton ego (User) ×

Add

Risk collaborators are those that generate risks by doing something or taking a specific decision. For example, all finance risks should have the finance team as collaborators.

Analisis

Asset Risk Management / Edit item (Acceso no permitido ...)

General | Analysis | Treatment | Risk Response Plan

Applicable Assets

Servidor × | Base de datos en la Nube ×

Add

Select one or more assets (Asset Management / Asset Identification) in the scope of this risk

Threat Tags

Unintentional Loss of Equipment × | Intentional Theft of Equipment × | Remote Exploit × | Abuse of Service × | Web Application Attack ×
Malware/Trojan Distribution × | Viruses × | Illegal Infiltration × | DOS Attack × | Brute Force Attack × | Abuse of Privilledge ×

Add

OPTIONAL: Select one or more applicable threats tags.

Threat Description

OPTIONAL: Describe the context of the threats vectors for this risk.

Vulnerabilities Tags

Lack of Integrity Checks × | Lack of Logs ×

Add

OPTIONAL: Select one or more applicable vulnerability tags.

Alto (5)

IMPACTO / ALTO

Probable (3)

PROBABILIDAD / PROBABLE

3 * 5 = 15

Alto riesgo
Alto riesgo

Tratamiento del riesgo

Alto (5)

IMPACTO / ALTO

Poco probable (1)

PROBABILIDAD / POCO PROBABLE

1 * 5 = 5

Riesgo medio
Riesgo medio

Asset Risk Management / Edit item (Acceso no permitido ...)

General | Analysis | Treatment | Risk Response Plan

Risk Treatment

Mitigate

Select a treatment strategy for this risk. Treatment options can be adjusted at Settings / Risk Treatment Options

Treatment: Internal Controls

Firewalls × Add

MANDATORY: Select one or more controls defined at Control Catalogue / Internal Controls

Treatment: Security Policies

Politica de cambio de contraseñas [Policy] × Add

Riesgo 8

General

Asset Risk Management / Edit item (Escape de helio liquido)

General | Analysis | Treatment | Risk Response Plan

Title

Escape de helio liquido

Give this risk a descriptive title, for example "Loss of information due laptops being stolen".

Description

OPTIONAL: Describe this risk scenario, context, triggers, Etc.

Risk Owner

Daniel Casteblanco (User) x

Add

You can use this field in any way it fits best your organisation, for example:

- In some cases this role relates to the GRC individual responsible to ensure the Risk is well documented and approved (this is typically our recommendation).
- In some other organisations this role belongs to the individual that brings this organisation to the risk by performing a certain business function.

This role will be available when you create notifications under the field Custom Roles.

Stakeholder

Daniel Casteblanco (User) x

Add

Analisis

Asset Risk Management / Edit item (Escape de helio liquido)

General | Analysis | Treatment | Risk Response Plan

Applicable Assets

Colisionador x

Add

Select one or more assets (Asset Management / Asset Identification) in the scope of this risk

Threat Tags

Pandemic Issues x | Strikes x | Natural Disasters x | Fire x | Flooding x | Terrorist Attack x | Floodings x | Third Party Intrusion x

Add

OPTIONAL: Select one or more applicable threats tags.

Medio (3)

IMPACTO / MEDIO

Probable (3)

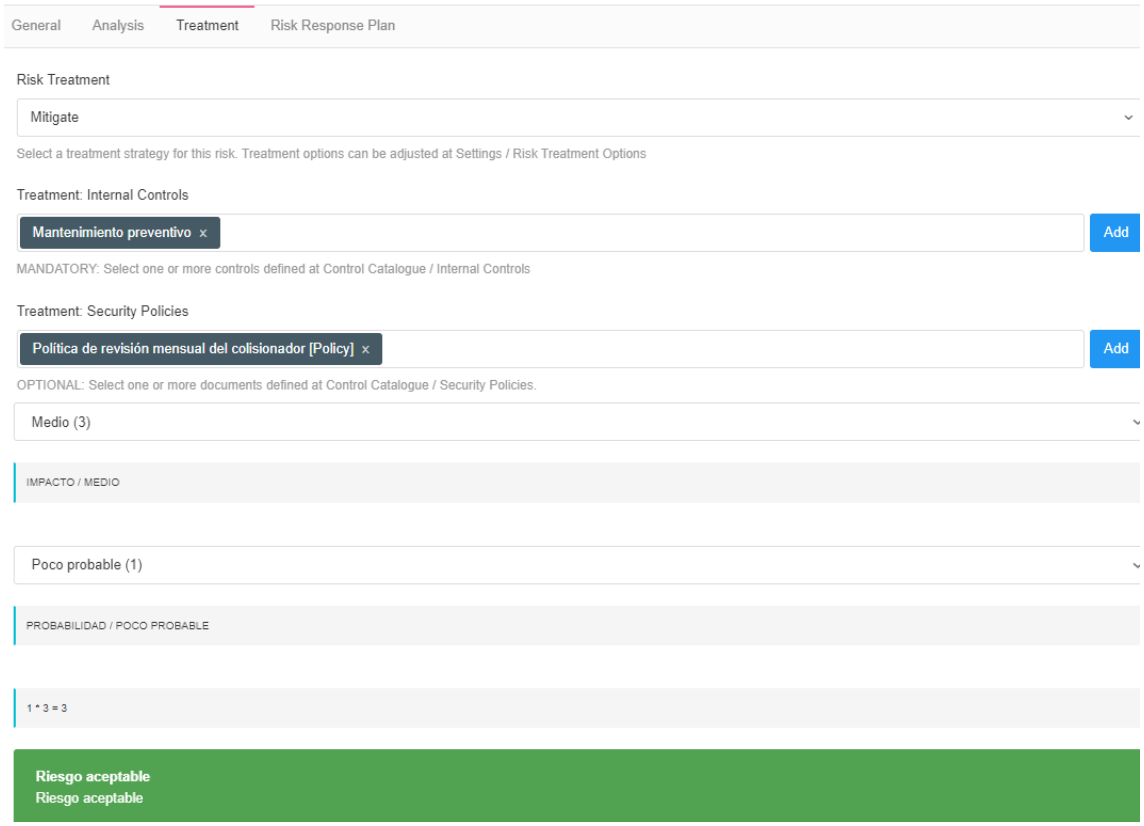
PROBABILIDAD / PROBABLE

3 * 3 = 9

Medio riesgo
Medio riesgo

Tratamiento del riesgo

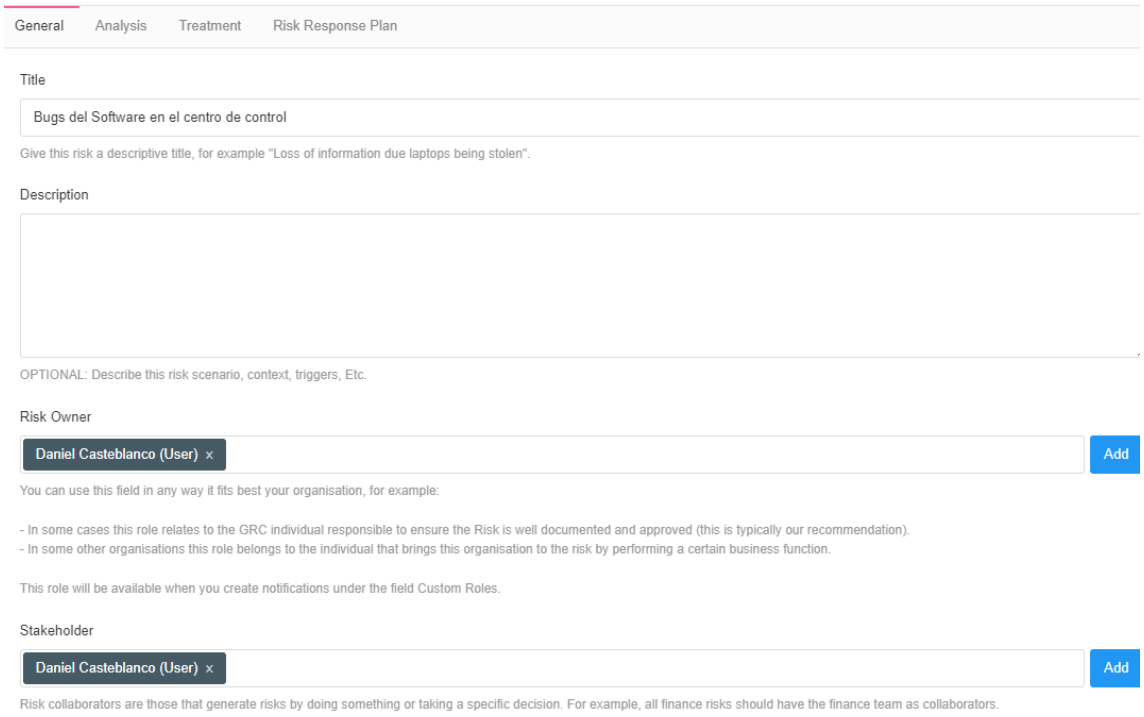
Asset Risk Management / Edit item (Escape de helio liquido)



Riesgo 9

General

Asset Risk Management / Edit item (Bugs del Software en...)



Analisis

Asset Risk Management / Edit item (Bugs del Software en...)

General | Analysis | Treatment | Risk Response Plan

Applicable Assets

Computadores ×

Add

Select one or more assets (Asset Management / Asset Identification) in the scope of this risk

Threat Tags

Unintentional Loss of Equipment × | Intentional Theft of Equipment × | Malware/Trojan Distribution × | Viruses ×

Add

OPTIONAL: Select one or more applicable threats tags.

Threat Description

OPTIONAL: Describe the context of the threats vectors for this risk.

Vulnerabilities Tags

Lack of Information × | Software Malfunction ×

Add

OPTIONAL: Select one or more applicable vulnerability tags.

Alto (5)

IMPACTO / ALTO

Probable (3)

PROBABILIDAD / PROBABLE

3 * 5 = 15

Alto riesgo
Alto riesgo

Tratamiento del riesgo

Asset Risk Management / Edit item (Bugs del Software en...)

General | Analysis | Treatment | Risk Response Plan

Risk Treatment

Mitigate

Select a treatment strategy for this risk. Treatment options can be adjusted at Settings / Risk Treatment Options

Treatment: Internal Controls

Mantenimiento preventivo ×

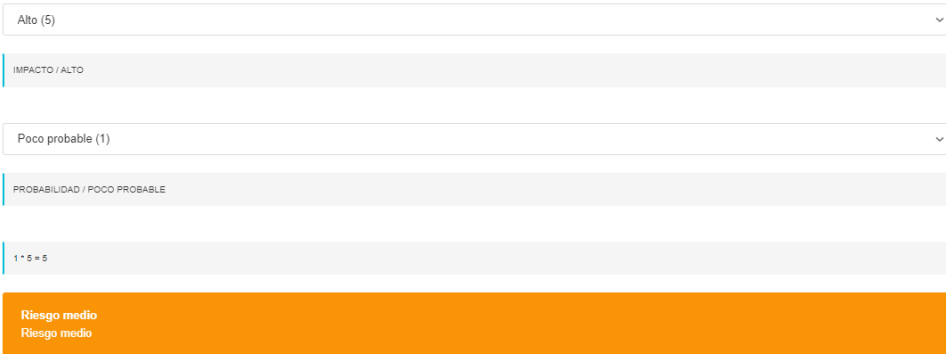
Add

MANDATORY: Select one or more controls defined at Control Catalogue / Internal Controls

Treatment: Security Policies

Política de Mantenimiento de Software [Policy] ×

Add



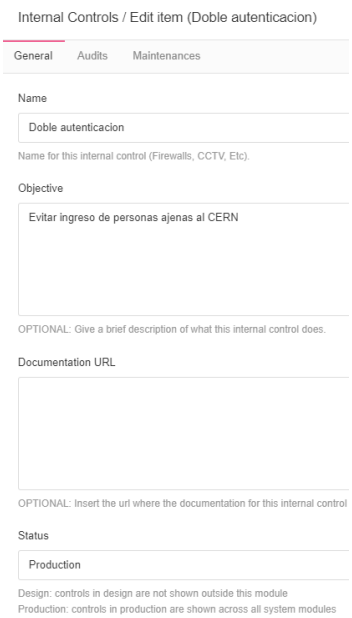
3.3) Internal Control

Crearemos controles internos para hacer que el impacto del riesgo se reduzca a un nivel aceptable y reducir su impacto y/o su probabilidad

	Actions	Status	Issues	Audits	Maintenances	Name	Objective
☐	≡	OK	0	0	0	Doble autenticacion	Evitar ingreso de personas ajenas al CERN
☐	≡	OK	0	0	0	Reemplazo de equipo	
☐	≡	OK	0	0	0	Reforzar estructuras antisismicas	
☐	≡	OK	0	0	0	Detectores de fuego y movimiento	
☐	≡	OK	0	0	0	Backups	
☐	≡	OK	0	0	0	Firewalls	
☐	≡	OK	0	0	0	Mantenimiento preventivo	

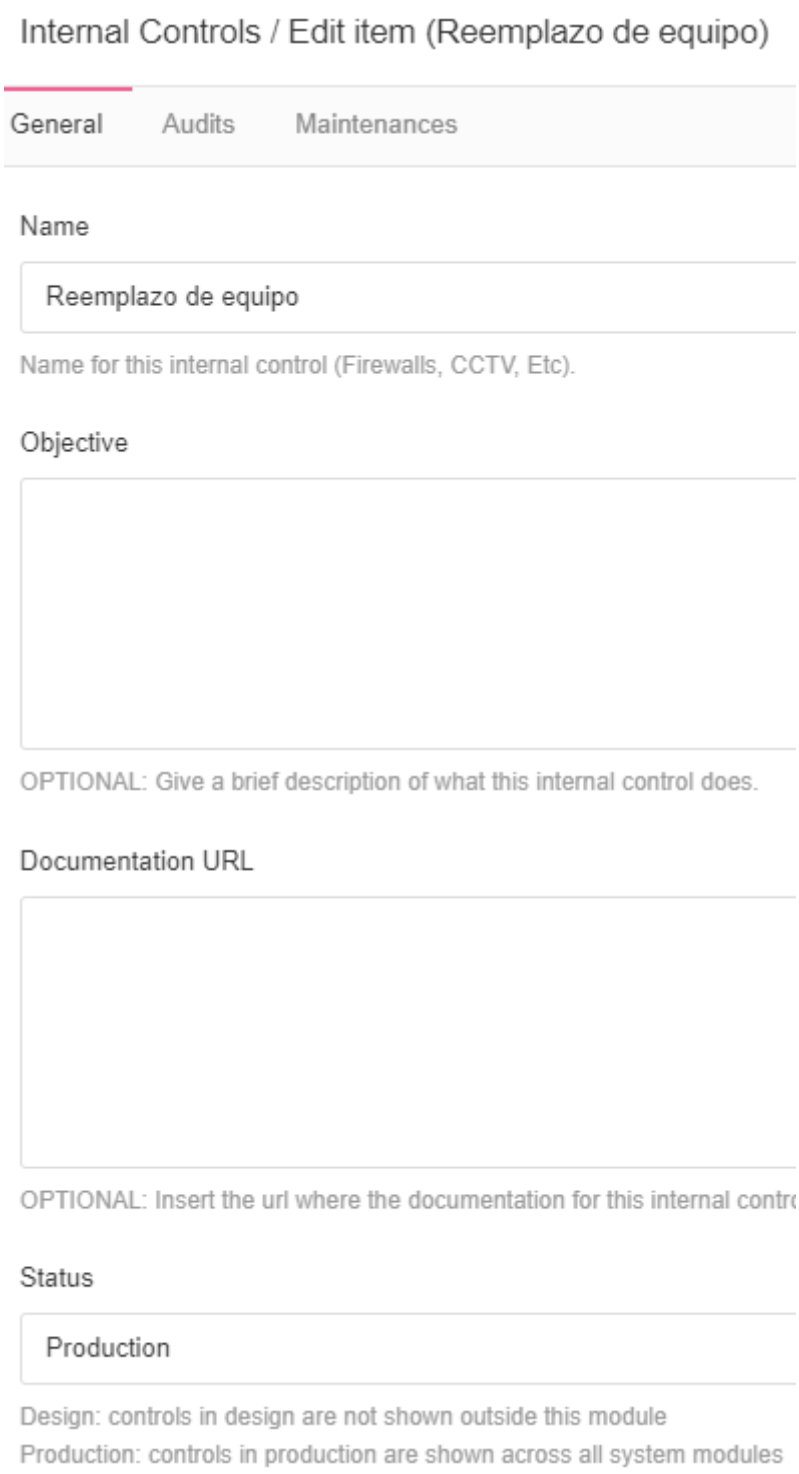
Control 1

General



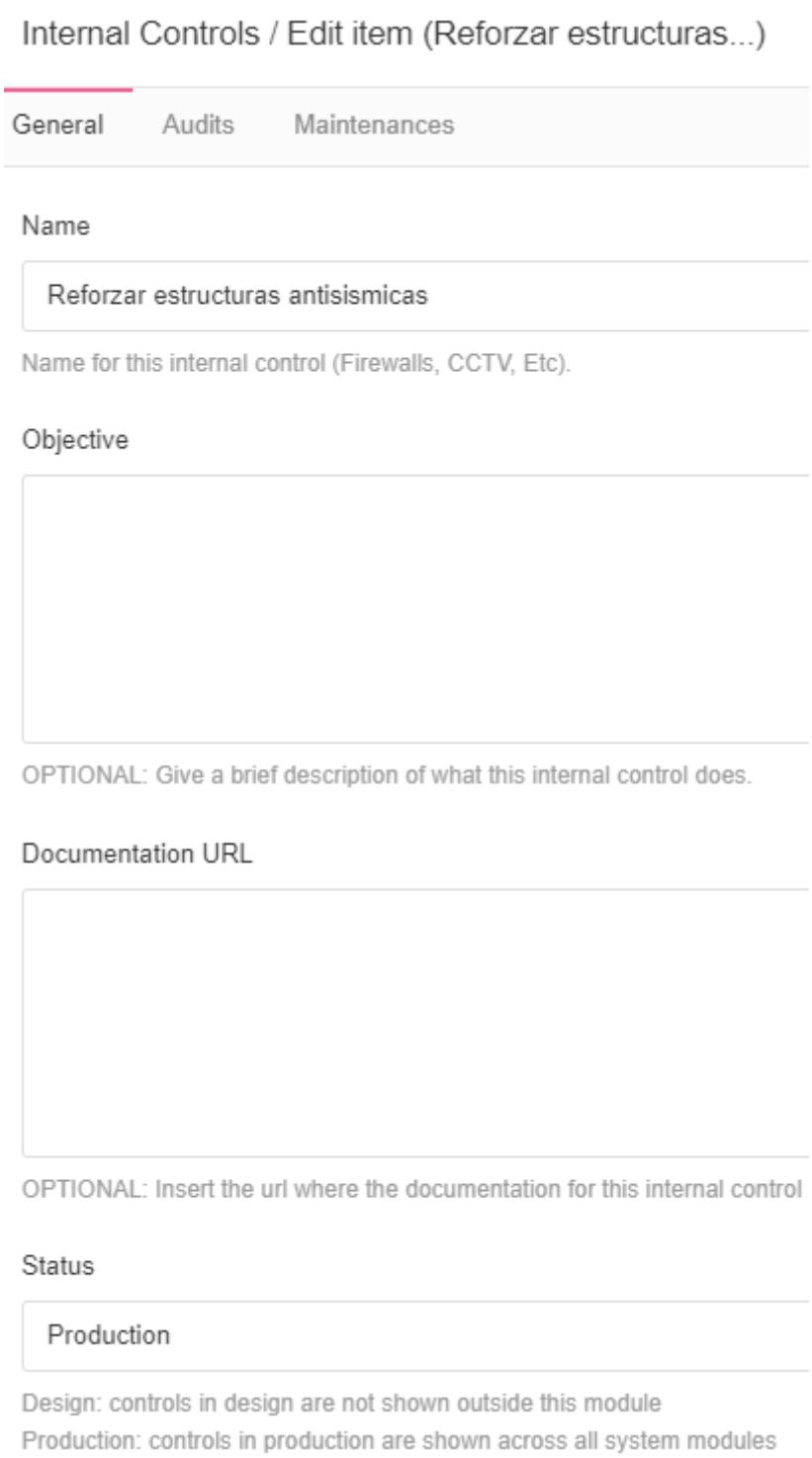
Control 2

General



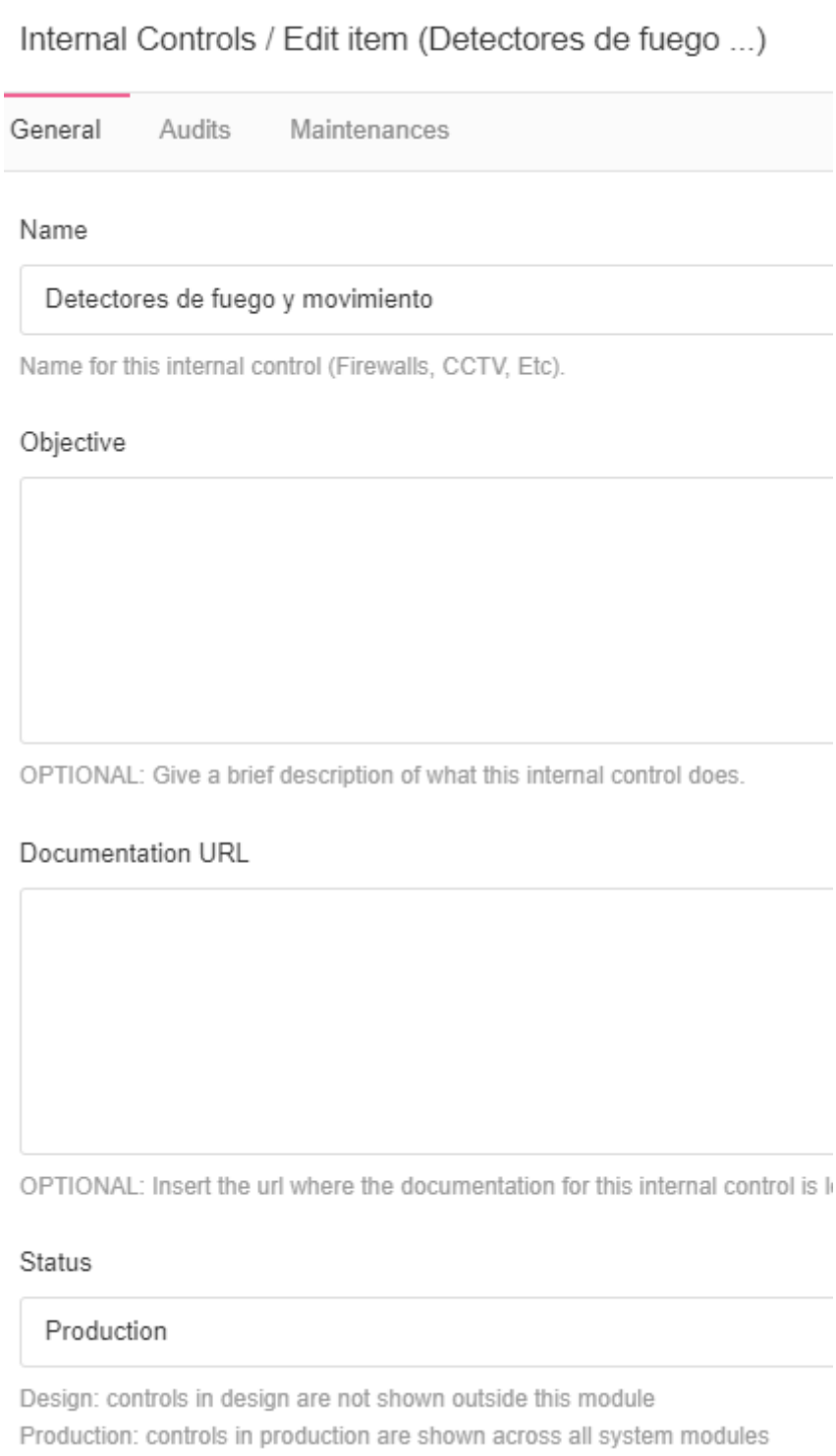
Control 3

General



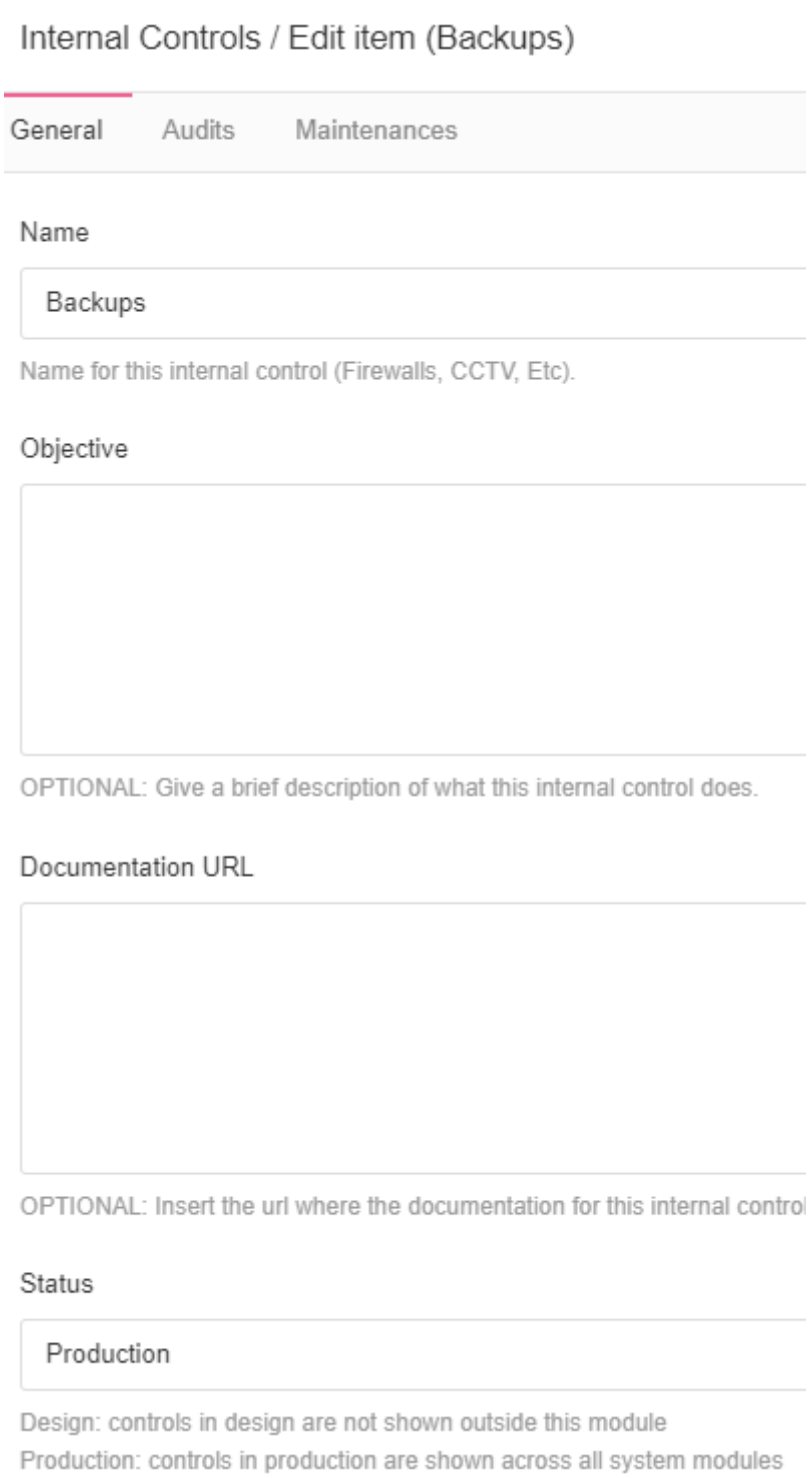
Control 4

General



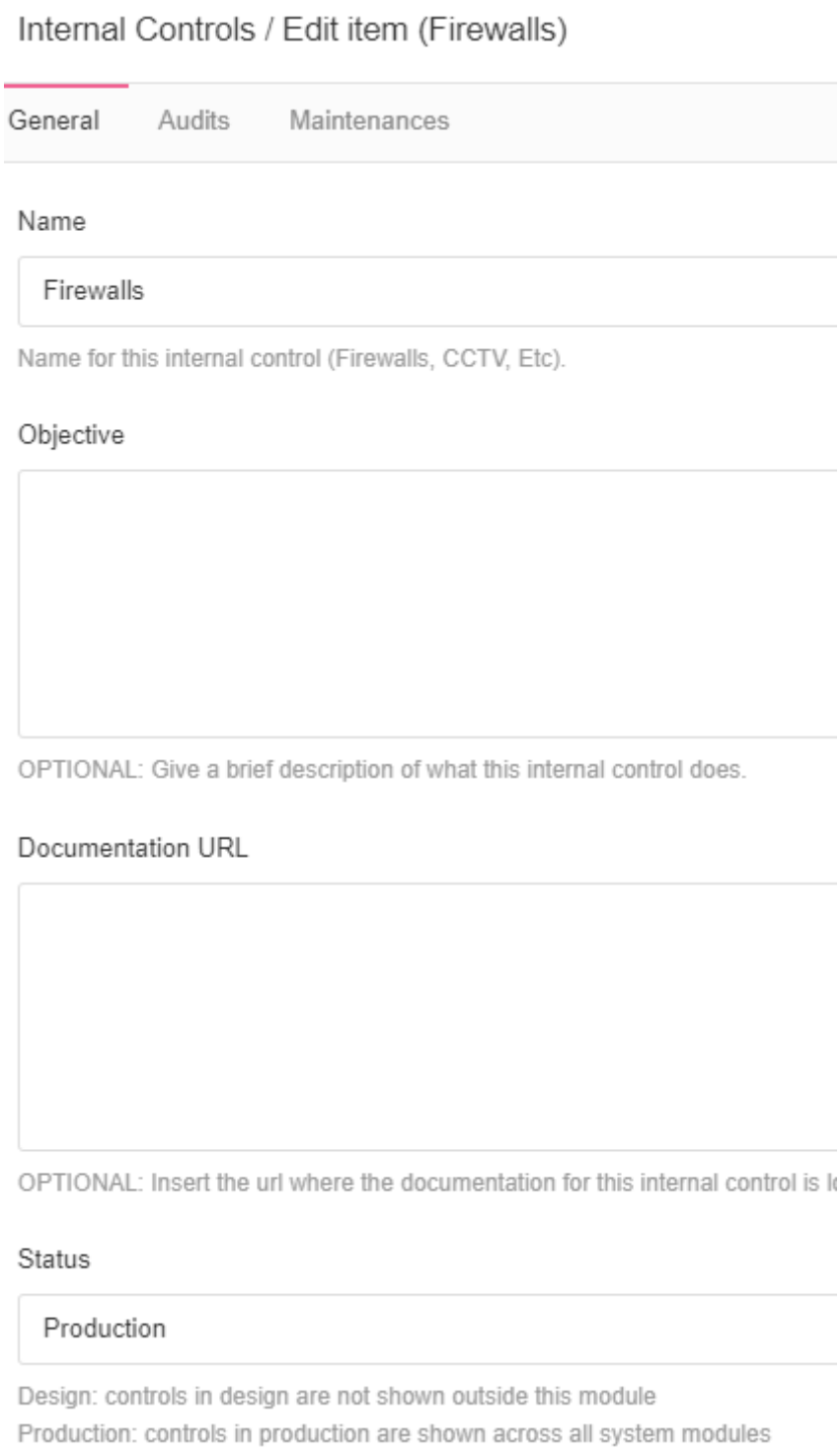
Control 5

General



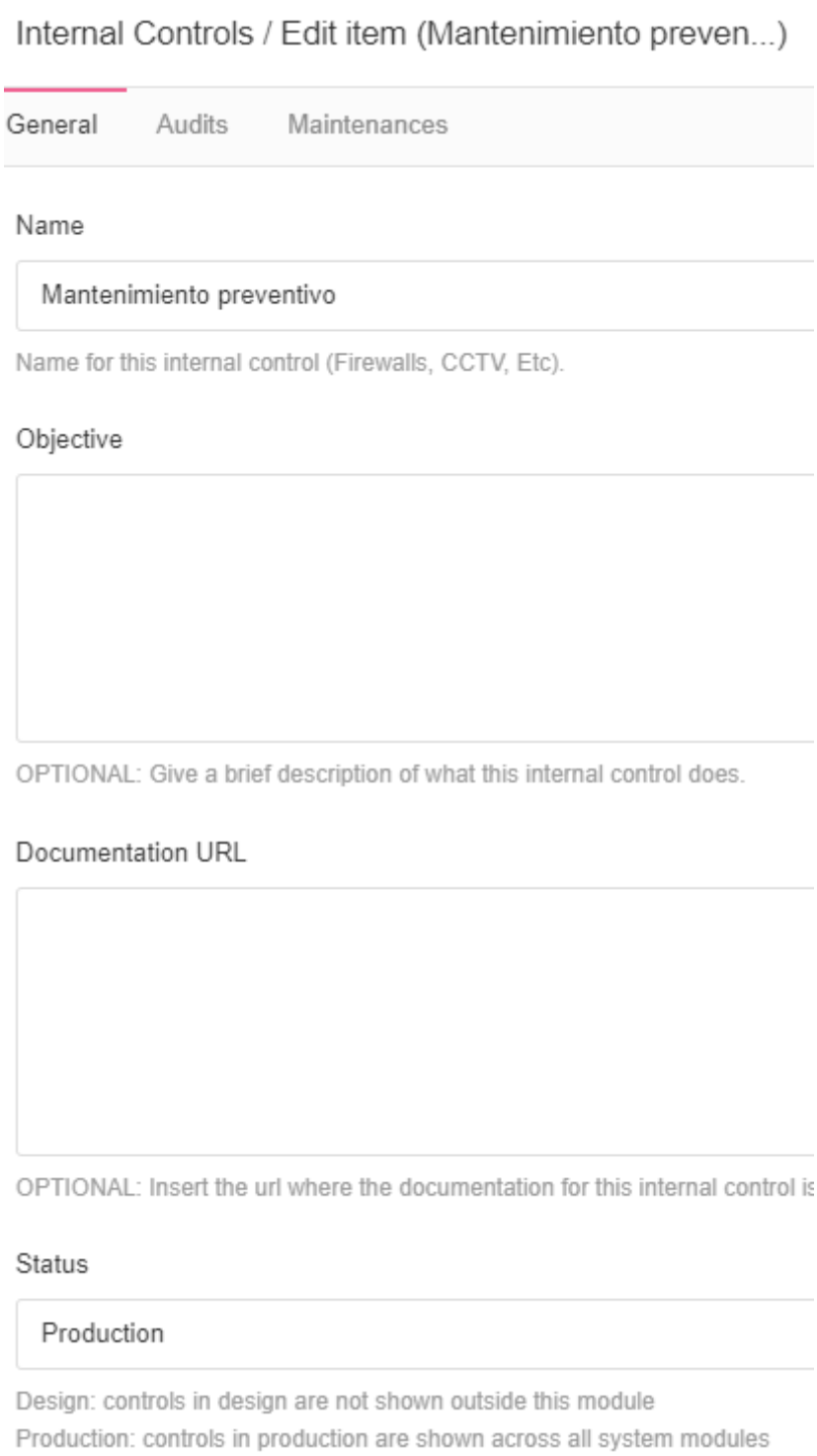
Control 6

General



Control 7

General



3.4) Security Policies

Crearemos políticas cuyo propósito es prevenir los riesgos y así proteger los activos de amenazas internas o externas

Actions	Status	Reviews	Title	Short Description
≡	OK	2	Política de Mantenimiento de Software	Mantenimiento del Software cada 6 meses
≡	OK	2	Política de revisión mensual del colisionador	Revisión mensual de los componentes del colisionador
≡	OK	2	Política de encriptación de datos sensibles de investigación	
≡	OK	2	Política de cambio de contraseñas	Cambiar la contraseña cada cierto tiempo de todos los usuarios para prevenir ataques de fuerza bruta
≡	OK	2	Políticas de Backups	

Política 1

General

Security Policies / Edit item (Política de Mantenim...)

General | Policy Content | Access Restrictions | Related Documents

Title

Política de Mantenimiento de Software

This is usually the title of the policy, for example: "Network Policies".

Short Description

Mantenimiento del Software cada 6 meses

OPTIONAL: Describe the scope of this document

Owner

Anton ego (User) × Daniel Casteblanco (User) × Add

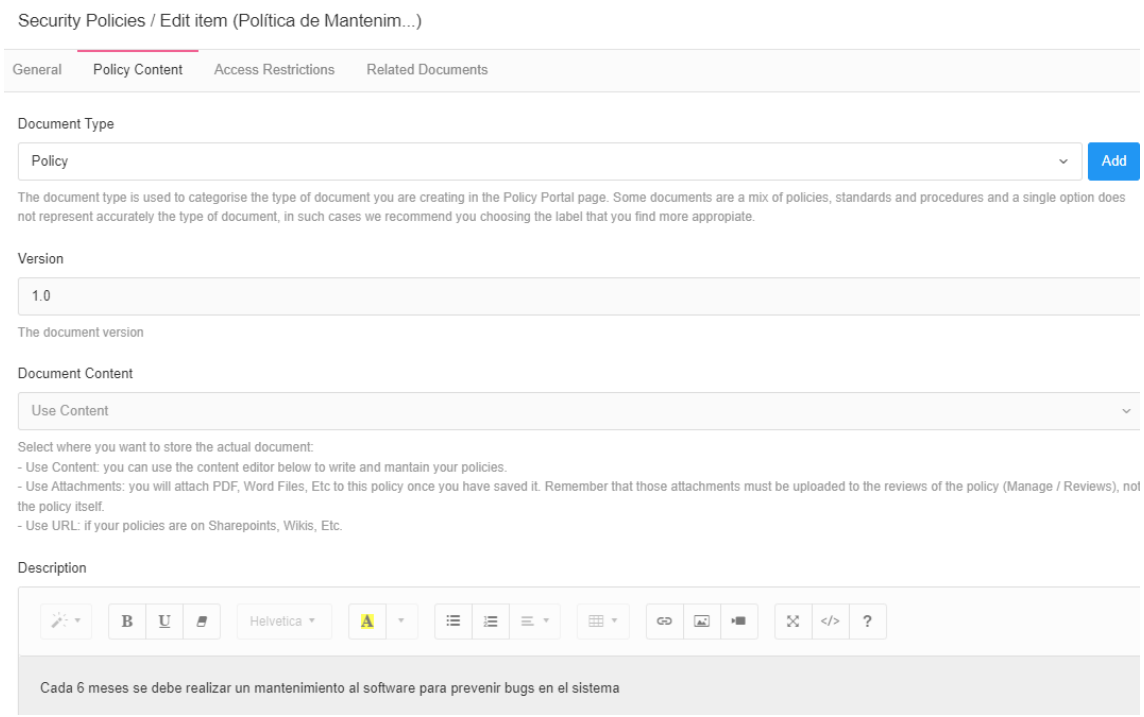
The owner is the GRC team member that will be responsible to ensure this policy is well documented in eramba and its always reviewed (by the collaborators)

Reviewer

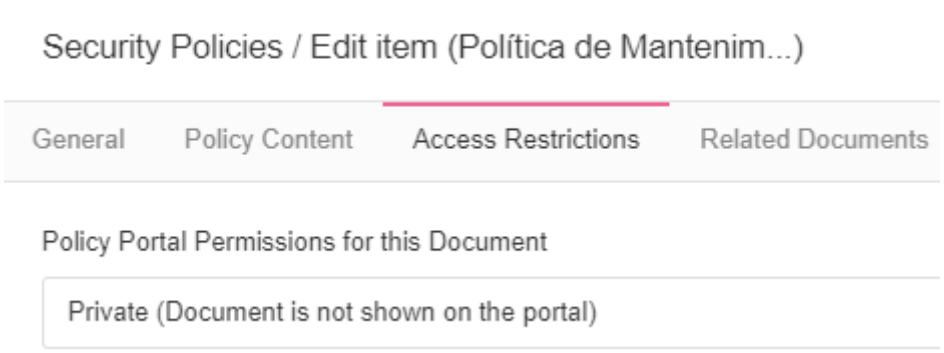
Daniel Casteblanco (User) × Add

Reviewers are those that are actually responsible for reviewing policies at set intervals. If this is a network policy, then is likely that the reviewers are those that work on that team.

Policy Content

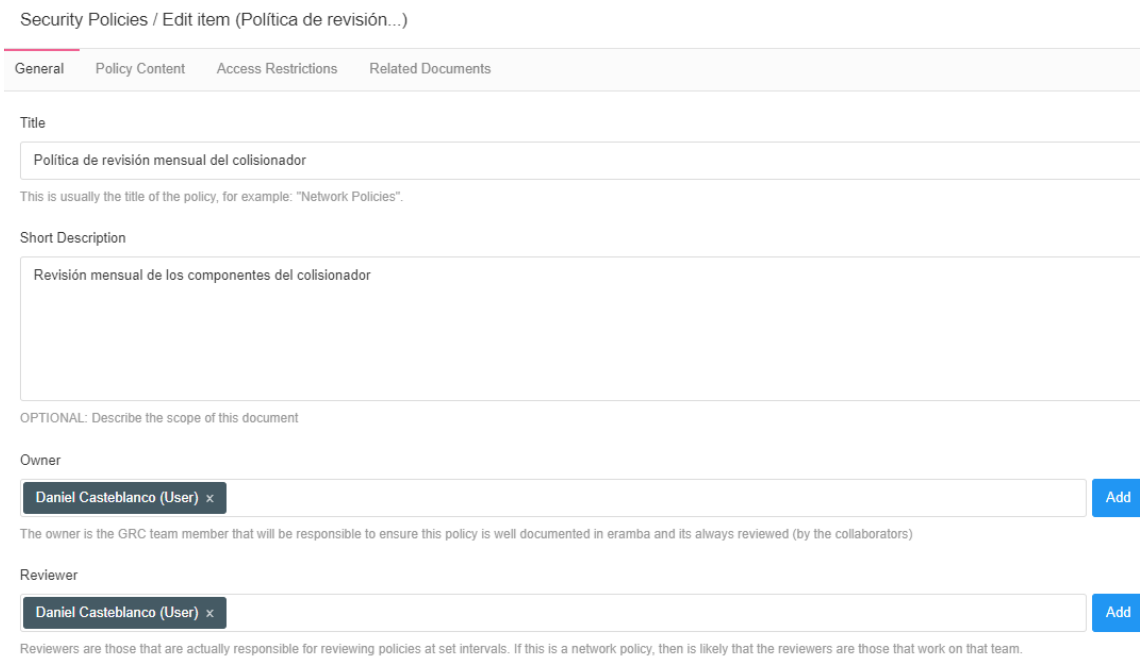


Access Restrictions

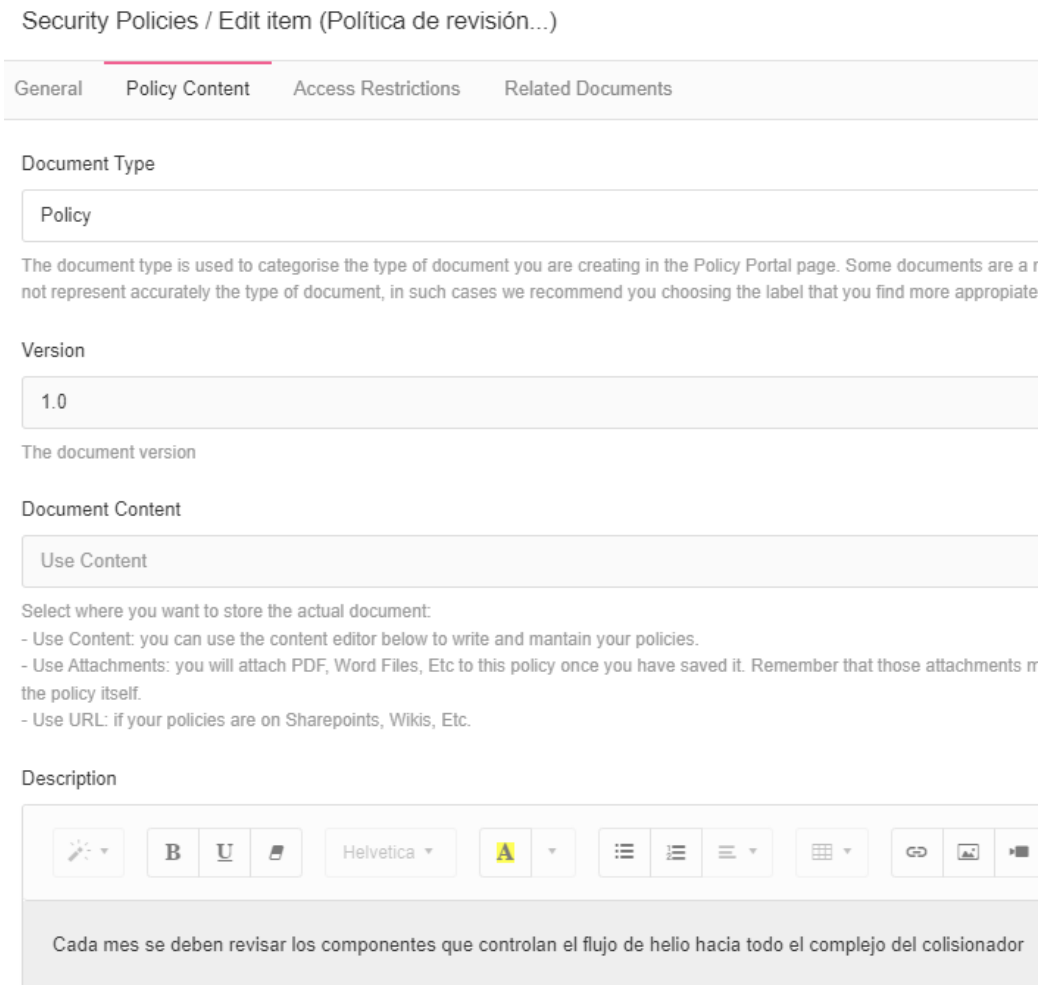


Política 2

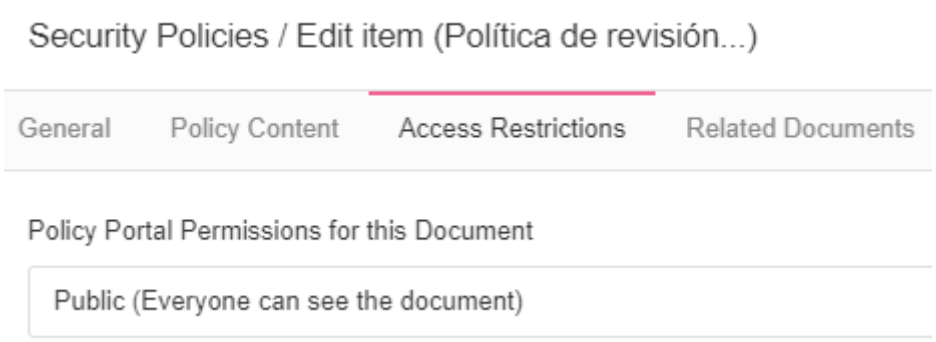
General



Policy Content

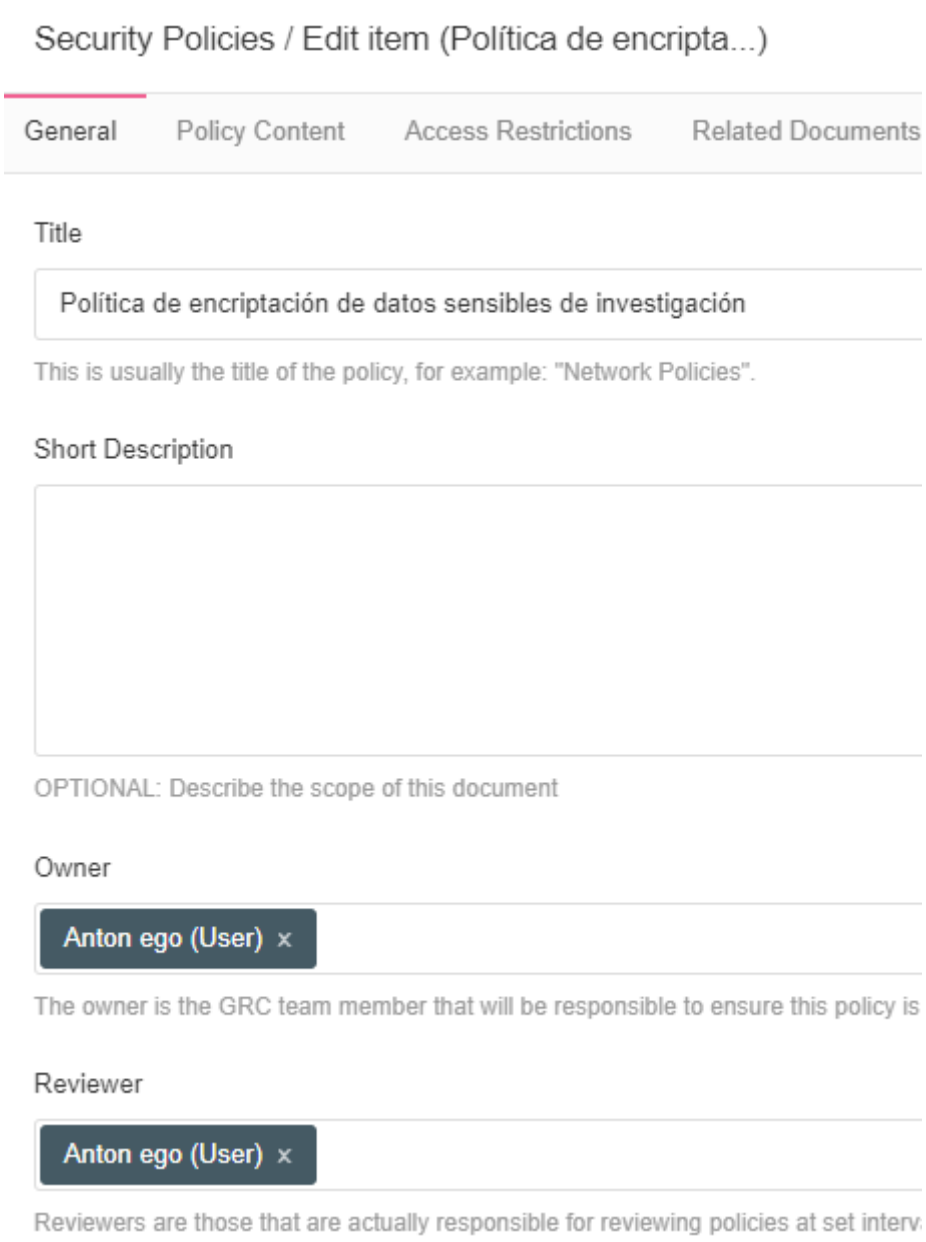


Access Restrictions

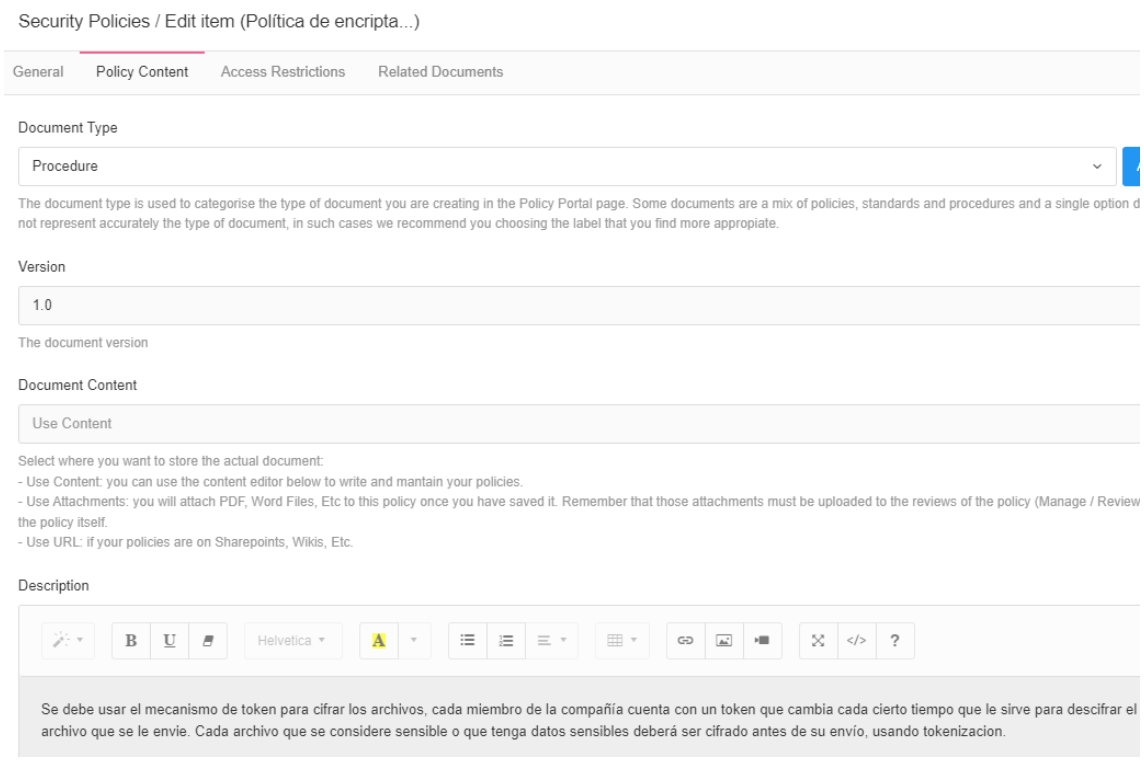


Política 3

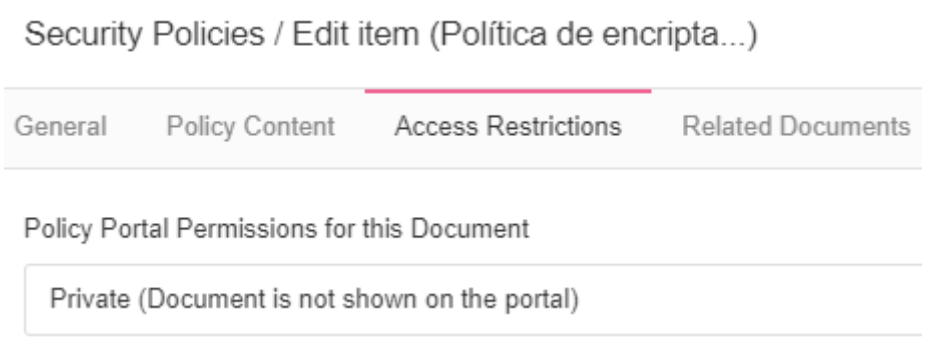
General



Policy Content

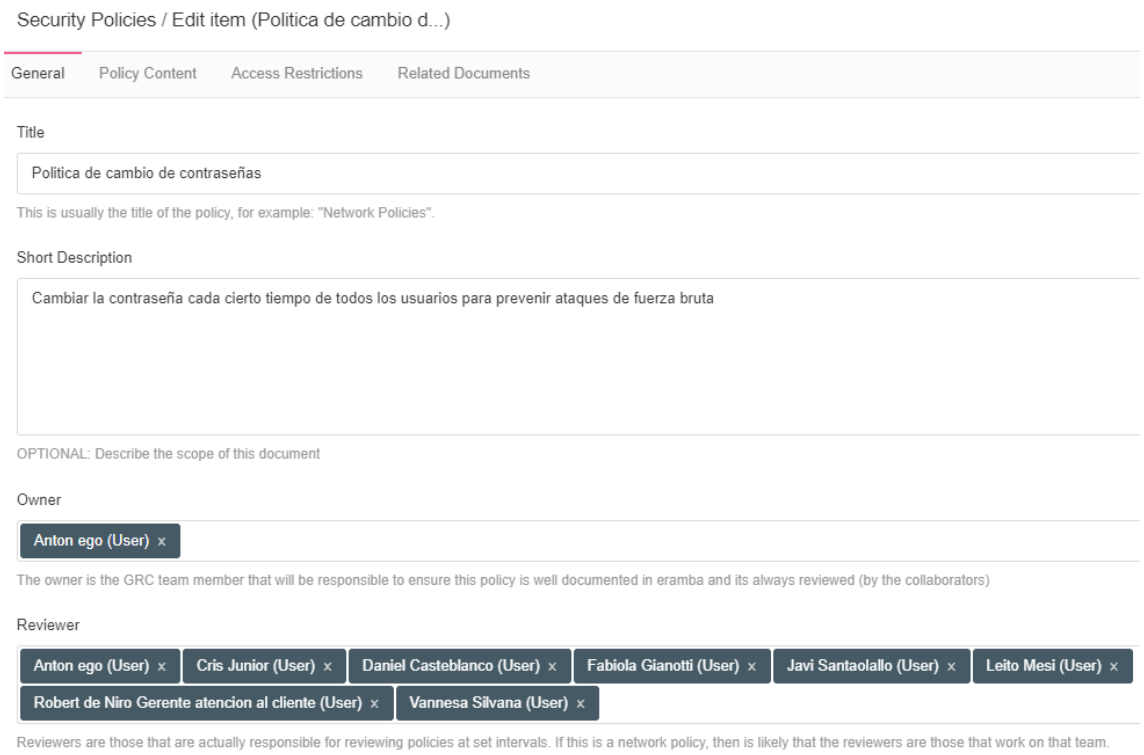


Access Restrictions

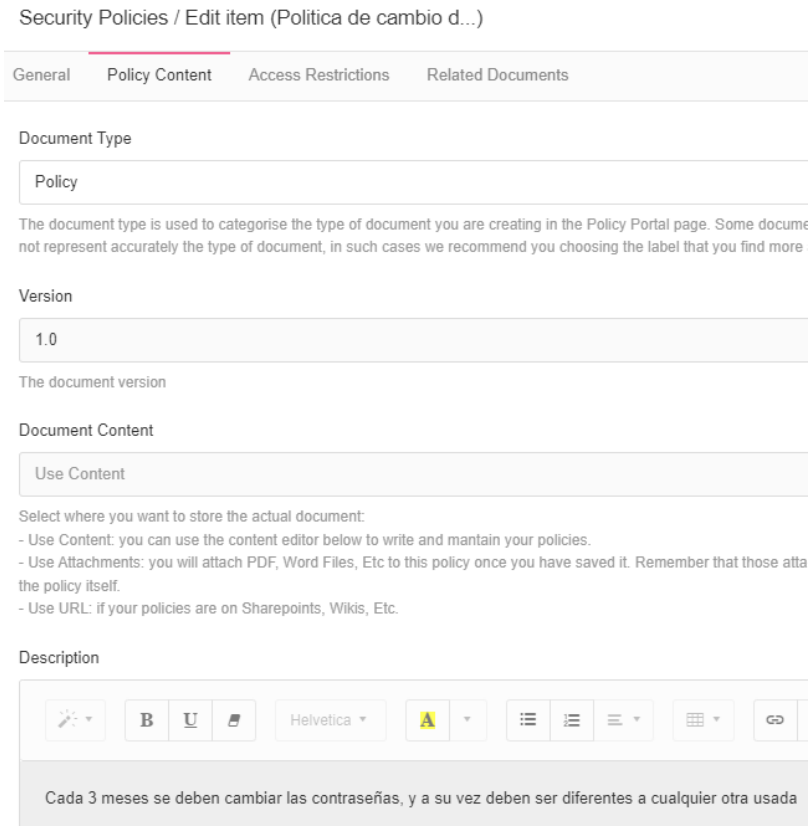


Política 4

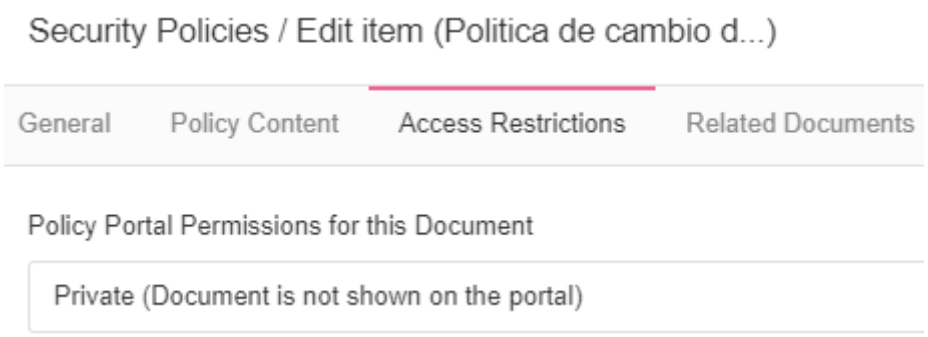
General



Policy Content

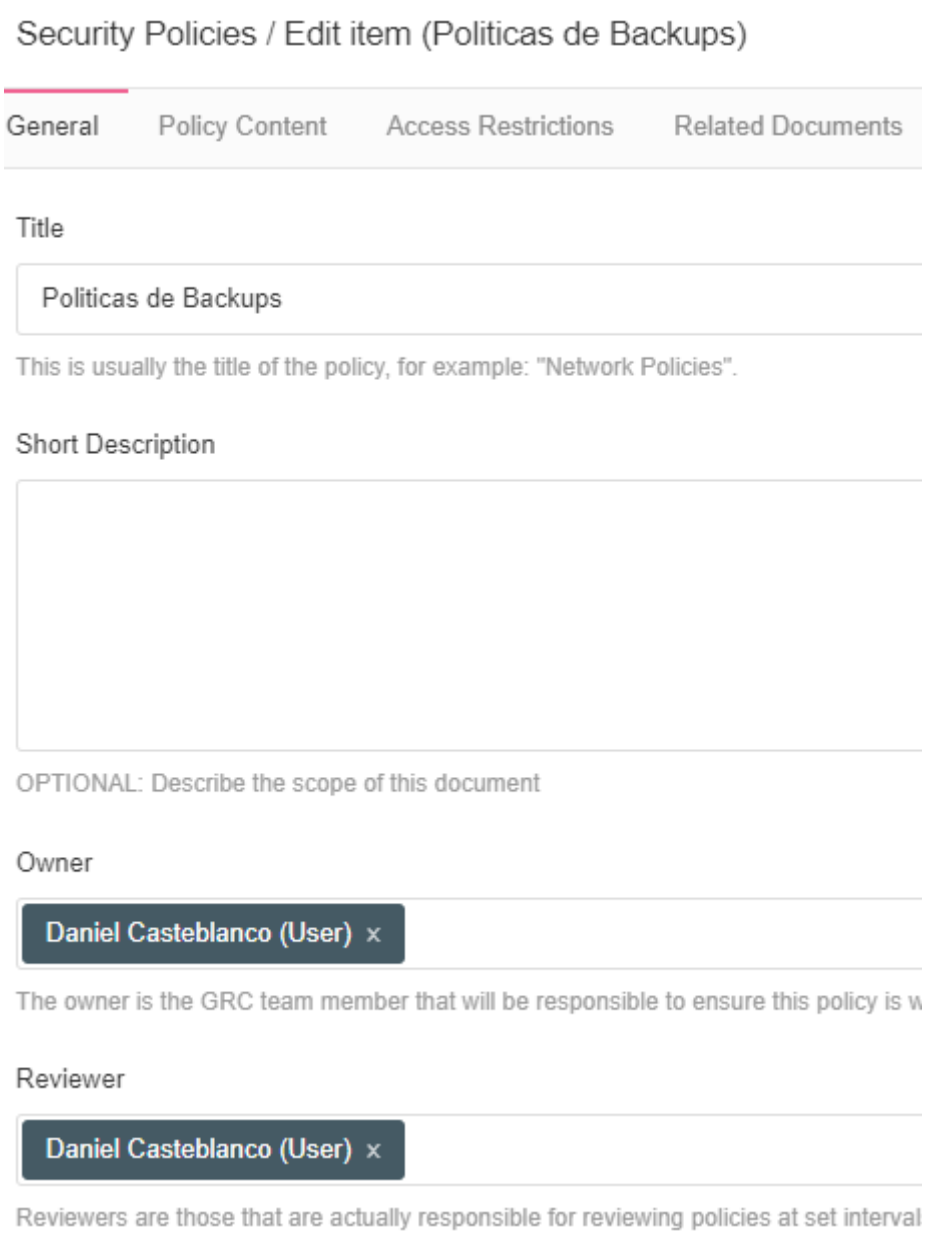


Access Restrictions

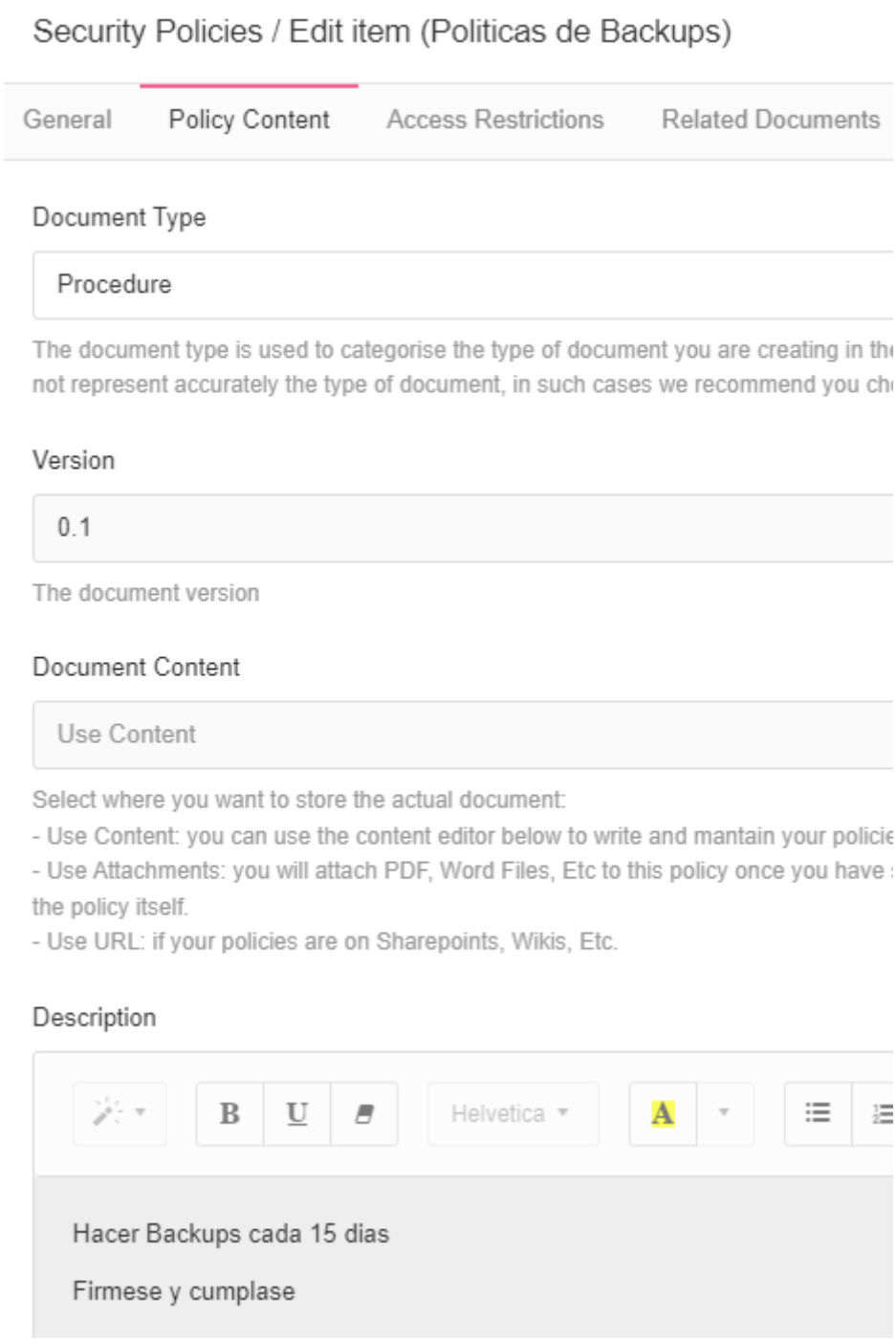


Política 5

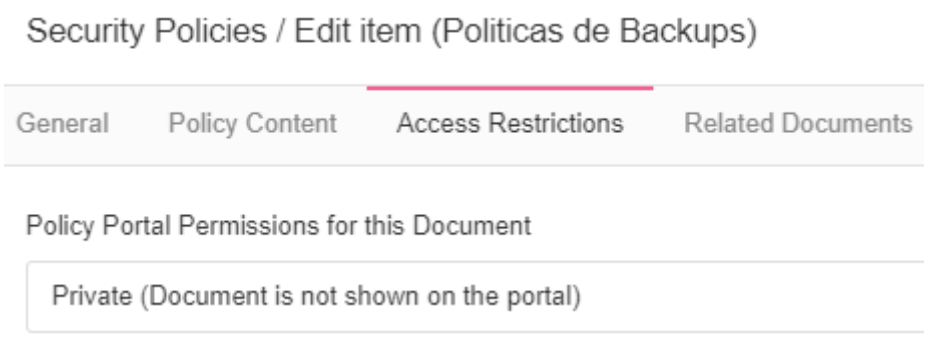
General



Policy Content



Access Restrictions



5. Conclusiones

Para poder realizar una efectiva gestión de riesgos se debe conocer que se tiene, es decir se debe conocer con que activos cuenta la organización, así se pueden realizar estudios para determinar que vulnerabilidades, amenazas y riesgos existen. Luego de esto podremos implementar políticas para prevenir futuros riesgos, u controles para mitigar los riesgos hasta un nivel aceptable y que no produzca un gran impacto en la organización.