



VIGILADA MINEDUCACIÓN

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.

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

Riesgo 1

General

Asset Risk Management / Edit item (Acceso indebido al s...)

General

Analysis

Treatment

Risk Response Plan

Title

Acceso indebido al sistema

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

Description

Acceso indebido a un sistema dentro de las instalaciones por parte de alguien no autorizado

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

Risk Owner

Anton ego (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

Anton ego (User) xDaniel Casteblanco (User) x

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.

Tags

CloseSave

Analysis

Asset Risk Management / Edit item (Acceso indebido al s...)

General

Analysis

Treatment

Risk Response Plan

Applicable Assets

Computadores x

Add

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

Threat Tags

Unintentional Loss of Equipment xIntentional Theft of Equipment xMalware/Trojan Distribution xViruses x

Add

OPTIONAL: Select one or more applicable threats tags.

Medio (3)

IMPACTO / MEDIO

Muy probable (5)

PROBABILIDAD / MUY PROBABLE

5 * 3 = 15

Alto riesgo

Alto riesgo

Tratamiento del riesgo

Asset Risk Management / Edit item (Acceso indebido al s...)

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

Doble autentificación

Add

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

Treatment: Security Policies

Política de cambio de contraseñas [Policy]

Add

OPTIONAL: Select one or more documents defined at Control Catalogue / Security Policies.

Medio (3)

IMPACTO / MEDIO

Poco probable (1)

PROBABILIDAD / POCO PROBABLE

1 * 3 = 3

Riesgo aceptable

Riesgo aceptable

Riesgo 2

General

Asset Risk Management / Edit item (Daño en el proyector)

General

Analysis

Treatment

Risk Response Plan

Title

Daño en el proyector

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

Description

Daño en el videobeam

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.

Analysis

Asset Risk Management / Edit item (Daño en el proyector) ✕

General

Analysis

Treatment

Risk Response Plan

Applicable Assets

Proyector Video Beam ✕

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.

Bajo (1)

▼

IMPACTO / BAJO

Probable (3)

▼

PROBABILIDAD / PROBABLE

3 * 1 = 3

Riesgo acceptable

Riesgo acceptable

Tratamiento del riesgo

Asset Risk Management / Edit item (Daño en el proyector)

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

Reemplazo de equipo ✕

Add

Bajo (1)

▼

IMPACTO / BAJO

Probable (3)

▼

PROBABILIDAD / PROBABLE

3 * 1 = 3

Riesgo acceptable

Riesgo acceptable

Riesgo 3

General

Asset Risk Management / Edit item (Desastre natural)

General

Analysis

Treatment

Risk Response Plan

Title

Desastre natural

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)

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

Fabiola Gianotti (User)

Add

Analysis

Asset Risk Management / Edit item (Desastre natural)

General

Analysis

Treatment

Risk Response Plan

Applicable Assets

Sensor x

Cámaras de seguridad x

Servidor x

Computadores x

Profesores y científicos x

Proyector Video Beam x

Archivos de investigación x

Base de datos On Premise x

Colisionador x

Add

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

Threat Tags

Intentional Complot x

Pandemic Issues x

Strikes x

Unintentional Loss of Equipment x

Intentional Theft of Equipment x

Unintentional Loss of Information x

Intentional Theft of Information x

Remote Exploit x

Abuse of Service x

Web Application Attack x

Phishing x

Malware/Trojan Distribution x

Viruses x

Copyright Infringment x

Social Engineering x

Natural Disasters x

Fire x

Flooding x

Illegal Infiltration x

DOS Attack x

Brute Force Attack x

Man in the Middle x

Fraud x

Terrorist Attack x

Floodings x

Third Party Intrusion x

Abuse of Privilege x

Unauthorised records x

Spying x

Add

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 (Desastre natural)

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

Reforzar estructuras antisismicas x

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 acceptable

Riesgo acceptable

Riesgo 4

General

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

General

Analysis

Treatment

Risk Response Plan

Title

Daño en el sensor del colisionador

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 Castebianco (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 Castebianco (User) x

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.

Analysis

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

General

Analysis

Treatment

Risk Response Plan

Applicable Assets

Sensor x

Add

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

Threat Tags

Remote Exploit x

Natural Disasters x

Fire x

Flooding x

Other x

Add

OPTIONAL: Select one or more applicable threats tags.

Medio (3)

IMPACTO / MEDIO

Poco probable (1)

PROBABILIDAD / POCO PROBABLE

1 * 3 = 3

Riesgo aceptable

Riesgo aceptable

Tratamiento del riesgo

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

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 x

Add

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

Bajo (1)

IMPACTO / BAJO

Poco probable (1)

PROBABILIDAD / POCO PROBABLE

1 * 1 = 1

Riesgo aceptable

Riesgo aceptable

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) 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

Anton ego (User) x

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.

Analysis

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

General

Analysis

Treatment

Risk Response Plan

Applicable Assets

Servidor x

Add

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

Threat Tags

Unintentional Loss of Equipment x

Intentional Theft of Equipment x

Malware/Trojan Distribution x

Viruses x

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.

Analysis

Asset Risk Management / Edit item (Ciberataque)

General

Analysis

Treatment

Risk Response Plan

Applicable Assets

Servidor x

Base de datos en la Nube x

Add

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

Threat Tags

Unintentional Loss of Equipment x

Intentional Theft of Equipment x

Remote Exploit x

Abuse of Service x

Web Application Attack x

Malware/Trojan Distribution x

Viruses x

Illegal Infiltration x

DOS Attack x

Brute Force Attack x

Abuse of Privilege x

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 x

Lack of Logs x

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 (Ciberataque)

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

Backups x

Add

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

Treatment: Security Policies

Política de encriptación de datos sensibles de investigación [Procedure] x

Políticas de Backups [Procedure] x

Add

OPTIONAL: Select one or more documents defined at Control Catalogue / Security Policies.

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

Acesso 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) 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

Anton ego (User) x

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.

Analysis

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

General

Analysis

Treatment

Risk Response Plan

Applicable Assets

Servidor x Base de datos en la Nube x

Add

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

Threat Tags

Unintentional Loss of Equipment x Intentional Theft of Equipment x Remote Exploit x Abuse of Service x Web Application Attack x

Malware/Trojan Distribution x Viruses x Illegal Infiltration x DOS Attack x Brute Force Attack x Abuse of Privilege x

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 x Lack of Logs x

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 x

Add

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

Treatment: Security Policies

Política de cambio de contraseñas [Policy] x

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

Analysis

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)

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 x

Add

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

Treatment: Security Policies

Política de revisión mensual del colisionador [Policy] x

Add

OPTIONAL: Select one or more documents defined at Control Catalogue / Security Policies.

Medio (3)

IMPACTO / MEDIO

Poco probable (1)

PROBABILIDAD / POCO PROBABLE

1 * 3 = 3

Riesgo aceptable

Riesgo aceptable

Riesgo 9

General

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

General

Analysis

Treatment

Risk Response Plan

Title

Bugs del Software en el centro de control

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

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.

Analysis

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

General

Analysis

Treatment

Risk Response Plan

Applicable Assets

Computadores x

Add

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

Threat Tags

Unintentional Loss of Equipment x

Intentional Theft of Equipment x

Malware/Trojan Distribution x

Viruses x

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 x

Software Malfunction x

Add

OPTIONAL: Select one or more applicable vulnerability tags.

Alto (5) v

IMPACTO / ALTO

Probable (3) v

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 v

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

Treatment: Internal Controls

Mantenimiento preventivo x

Add

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

Treatment: Security Policies

Política de Mantenimiento de Software [Policy] x

Add

Alto (5)

IMPACTO / ALTO

Poco probable (1)

PROBABILIDAD / POCO PROBABLE

1 * 5 = 5

Riesgo medio

Riesgo medio

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

<input type="checkbox"/>	Actions	▼ Status	Issues	Audits	Maintenances	Name	Objective
<input type="checkbox"/>	≡	OK	0 ▼	0 ▼	0 ▼	Doble autentificacion	Evitar ingreso de personas ajenas al CERN
<input type="checkbox"/>	≡	OK	0 ▼	0 ▼	0 ▼	Reemplazo de equipo	
<input type="checkbox"/>	≡	OK	0 ▼	0 ▼	0 ▼	Reforzar estructuras antisismicas	
<input type="checkbox"/>	≡	OK	0 ▼	0 ▼	0 ▼	Detectores de fuego y movimiento	
<input type="checkbox"/>	≡	OK	0 ▼	0 ▼	0 ▼	Backups	
<input type="checkbox"/>	≡	OK	0 ▼	0 ▼	0 ▼	Firewalls	
<input type="checkbox"/>	≡	OK	0 ▼	0 ▼	0 ▼	Mantenimiento preventivo	

Control 1

General

Internal Controls / Edit item (Doble autentificacion)

General

Audits

Maintenances

Name

Doble autentificacion

Name for this internal control (Firewalls, CCTV, Etc).

Objective

Evitar ingreso de personas ajenas al CERN

OPTIONAL: Give a brief description of what this internal control does.

Documentation URL

OPTIONAL: Insert the url where the documentation for this internal control

Status

Production

Design: controls in design are not shown outside this module

Production: controls in production are shown across all system modules

Control 2

General

Internal Controls / Edit item (Reemplazo de equipo)

General	Audits	Maintenances
---------	--------	--------------

Name

Reemplazo de equipo

Name for this internal control (Firewalls, CCTV, Etc).

Objective

OPTIONAL: Give a brief description of what this internal control does.

Documentation URL

OPTIONAL: Insert the url where the documentation for this internal control is located.

Status

Production

Design: controls in design are not shown outside this module

Production: controls in production are shown across all system modules

Control 3

General

Internal Controls / Edit item (Reforzar estructuras...)

General Audits Maintenances

Name

Reforzar estructuras antisismicas

Name for this internal control (Firewalls, CCTV, Etc).

Objective

OPTIONAL: Give a brief description of what this internal control does.

Documentation URL

OPTIONAL: Insert the url where the documentation for this internal control

Status

Production

Design: controls in design are not shown outside this module

Production: controls in production are shown across all system modules

Control 4

General

Internal Controls / Edit item (Detectores de fuego ...)

General Audits Maintenances

Name

Detectores de fuego y movimiento

Name for this internal control (Firewalls, CCTV, Etc).

Objective

OPTIONAL: Give a brief description of what this internal control does.

Documentation URL

OPTIONAL: Insert the url where the documentation for this internal control is located

Status

Production

Design: controls in design are not shown outside this module

Production: controls in production are shown across all system modules

Control 5

General

Internal Controls / Edit item (Backups)

General	Audits	Maintenances
---------	--------	--------------

Name

Backups

Name for this internal control (Firewalls, CCTV, Etc).

Objective

OPTIONAL: Give a brief description of what this internal control does.

Documentation URL

OPTIONAL: Insert the url where the documentation for this internal control

Status

Production

Design: controls in design are not shown outside this module
Production: controls in production are shown across all system modules

Control 6

General

Internal Controls / Edit item (Firewalls)

General

Audits

Maintenances

Name

Firewalls

Name for this internal control (Firewalls, CCTV, Etc).

Objective

OPTIONAL: Give a brief description of what this internal control does.

Documentation URL

OPTIONAL: Insert the url where the documentation for this internal control is located

Status

Production

Design: controls in design are not shown outside this module

Production: controls in production are shown across all system modules

Control 7

General

Internal Controls / Edit item (Mantenimiento preven...)

General Audits Maintenances

Name

Mantenimiento preventivo

Name for this internal control (Firewalls, CCTV, Etc).

Objective

OPTIONAL: Give a brief description of what this internal control does.

Documentation URL

OPTIONAL: Insert the url where the documentation for this internal control is

Status

Production

Design: controls in design are not shown outside this module

Production: controls in production are shown across all system modules

3.4) Security Policies

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

<input type="checkbox"/>	Actions	Status	Reviews	Title	Short Description
<input type="checkbox"/>		<div>OK</div>	2	Política de Mantenimiento de Software	Mantenimiento del Software cada 6 meses
<input type="checkbox"/>		<div>OK</div>	2	Política de revisión mensual del colisionador	Revisión mensual de los componentes del colisionador
<input type="checkbox"/>		<div>OK</div>	2	Política de encriptación de datos sensibles de investigación	
<input type="checkbox"/>		<div>OK</div>	2	Política de cambio de contraseñas	Cambiar la contraseña cada cierto tiempo de todos los usuarios para prevenir ataques de fuerza bruta
<input type="checkbox"/>		<div>OK</div>	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) x

Daniel Castebianco (User) x

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 Castebianco (User) x

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

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

General

Policy Content

Access Restrictions

Related Documents

Document Type

Policy

Add

The document type is used to categorise the type of document you are creating in the Policy Portal page. Some documents are a mix of policies, standards and procedures and a single option does not represent accurately the type of document, in such cases we recommend you choosing the label that you find more appropriate.

Version

1.0

The document version

Document Content

Use Content

Select where you want to store the actual document:
- Use Content: you can use the content editor below to write and maintain your policies.
- Use Attachments: you will attach PDF, Word Files, Etc to this policy once you have saved it. Remember that those attachments must be uploaded to the reviews of the policy (Manage / Reviews), not the policy itself.
- Use URL: if your policies are on Sharepoints, Wikis, Etc.

Description

B

U

Helvetica

GO

Cada 6 meses se debe realizar un mantenimiento al software para prevenir bugs en el sistema

Access Restrictions

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

General

Policy Content

Access Restrictions

Related Documents

Policy Portal Permissions for this Document

Private (Document is not shown on the portal)

Política 2

General

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

General

Policy Content

Access Restrictions

Related Documents

Title

Política de revisión mensual del colisionador

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

Short Description

Revisión mensual de los componentes del colisionador

OPTIONAL: Describe the scope of this document

Owner

Daniel Castebianco (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 Castebianco (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

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

General

Policy Content

Access Restrictions

Related Documents

Document Type

Policy

The document type is used to categorise the type of document you are creating in the Policy Portal page. Some documents are a r not represent accurately the type of document, in such cases we recommend you choosing the label that you find more appropriate

Version

1.0

The document version

Document Content

Use Content

Select where you want to store the actual document:

- Use Content: you can use the content editor below to write and maintain your policies.

- Use Attachments: you will attach PDF, Word Files, Etc to this policy once you have saved it. Remember that those attachments rr the policy itself.

- Use URL: if your policies are on Sharepoints, Wikis, Etc.

Description

B

U

Helvetica

A

Cada mes se deben revisar los componentes que controlan el flujo de helio hacia todo el complejo del colisionador

Access Restrictions

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

General	Policy Content	Access Restrictions	Related Documents
---------	----------------	---------------------	-------------------

Policy Portal Permissions for this Document

Public (Everyone can see the document)

Política 3

General

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

General	Policy Content	Access Restrictions	Related Documents
---------	----------------	---------------------	-------------------

Title

Política de encriptación de datos sensibles de investigación

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

Short Description

OPTIONAL: Describe the scope of this document

Owner

Anton ego (User) x

The owner is the GRC team member that will be responsible to ensure this policy is

Reviewer

Anton ego (User) x

Reviewers are those that are actually responsible for reviewing policies at set interv.

Policy Content

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

General

Policy Content

Access Restrictions

Related Documents

Document Type

Procedure

The document type is used to categorise the type of document you are creating in the Policy Portal page. Some documents are a mix of policies, standards and procedures and a single option d not represent accurately the type of document, in such cases we recommend you choosing the label that you find more appropriate.

Version

1.0

The document version

Document Content

Use Content

Select where you want to store the actual document:
- Use Content: you can use the content editor below to write and maintain your policies.
- Use Attachments: you will attach PDF, Word Files, Etc to this policy once you have saved it. Remember that those attachments must be uploaded to the reviews of the policy (Manage / Review the policy itself.
- Use URL: if your policies are on Sharepoints, Wikis, Etc.

Description

B

U

Helvetica

A

GD

Se debe usar el mecanismo de token para cifrar los archivos, cada miembro de la compañía cuenta con un token que cambia cada cierto tiempo que le sirve para descifrar el archivo que se le envíe. Cada archivo que se considere sensible o que tenga datos sensibles deberá ser cifrado antes de su envío, usando tokenización.

Access Restrictions

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

General

Policy Content

Access Restrictions

Related Documents

Policy Portal Permissions for this Document

Private (Document is not shown on the portal)

Política 4

General

Security Policies / Edit item (Politica de cambio d...)

[General](#)
[Policy Content](#)
[Access Restrictions](#)
[Related Documents](#)

Title

Política de cambio de contraseñas

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

Short Description

Cambiar la contraseña cada cierto tiempo de todos los usuarios para prevenir ataques de fuerza bruta

OPTIONAL: Describe the scope of this document

Owner

Anton ego (User) x

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

Anton ego (User) x Cris Junior (User) x Daniel Casteblanco (User) x Fabiola Gianotti (User) x Javi Santaolallo (User) x Leito Mesi (User) x Robert de Niro Gerente atencion al cliente (User) x Vannessa Silvana (User) x

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

Security Policies / Edit item (Politica de cambio d...)

General Policy Content Access Restrictions Related Documents

Document Type

Policy	
--------	--

The document type is used to categorise the type of document you are creating in the Policy Portal page. Some documents may not represent accurately the type of document, in such cases we recommend you choosing the label that you find more appropriate.

Version

The document version

Document Content

Use Content

Select where you want to store the actual document:

- Use Content: you can use the content editor below to write and maintain your policies.
- Use Attachments: you will attach PDF, Word Files, Etc to this policy once you have saved it. Remember that those attachments are not part of the policy itself.
- Use URL: if your policies are on Sharepoints, Wikis, Etc.

Description

Cada 3 meses se deben cambiar las contraseñas, y a su vez deben ser diferentes a cualquier otra usada

Access Restrictions

Security Policies / Edit item (Politica de cambio d...)

General Policy Content **Access Restrictions** Related Documents

Policy Portal Permissions for this Document

Private (Document is not shown on the portal)

Política 5

General

Security Policies / Edit item (Políticas de Backups)

General Policy Content Access Restrictions **Related Documents**

Title

Políticas de Backups

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

Short Description

OPTIONAL: Describe the scope of this document

Owner

Daniel Casteblanco (User) x

The owner is the GRC team member that will be responsible to ensure this policy is w

Reviewer

Daniel Casteblanco (User) x

Reviewers are those that are actually responsible for reviewing policies at set interval

Security Policies / Edit item (Políticas de Backups)

General	Policy Content	Access Restrictions	Related Documents
---------	----------------	---------------------	-------------------

Document Type

Procedure

The document type is used to categorise the type of document you are creating in the system. It does not necessarily represent accurately the type of document, in such cases we recommend you choose the most appropriate one.

Version

0.1

The document version

Document Content

Use Content

Select where you want to store the actual document:

- Use Content: you can use the content editor below to write and maintain your policies.
- Use Attachments: you will attach PDF, Word Files, Etc to this policy once you have created the policy itself.
- Use URL: if your policies are on Sharepoints, Wikis, Etc.

Description

B

U

Helvetica

Hacer Backups cada 15 dias

Firmese y cumplase

Access Restrictions

Security Policies / Edit item (Políticas de Backups)

General	Policy Content	Access Restrictions	Related Documents
---------	----------------	---------------------	-------------------

Policy Portal Permissions for this Document

Private (Document is not shown on the portal)

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.