



INGENIERIA DE SISTEMAS – SPTI 2021-1

LABORATORIO 2:

Análisis de Riesgos de Seguridad de la Información

GERSON DAVID QUINTERO RODRIGUEZ

Autor:

Torres Segura Duck James Alexander

INTRODUCTION

In this laboratory we will learn to classify the assets of a company using tools such as Simple Risk, which helps us with the characteristics of the asset and its classification, we will also treat the risks and classify them from a scale where we will see or not affect our assets and we will observe through these scales the impact it can have on our company..

OBJECTIVES

GENERAL

Identify, analyze and evaluate the risks that can compromise the security for the assets, that are critical in the execution of a business process.

SPECIFIC:

- Apply the OWASP Risk Rating Methodology to analyze and evaluate security risks.
- Identify security controls/countermeasures/safeguards that can be needed to mitigate critical security risks.

1. SECTION ONE: SIMPLE RISK CONFIGURATION.

- Start a local instance of SimpleRisk following instructions in Laboratory I and log in using credentials admin/admin.

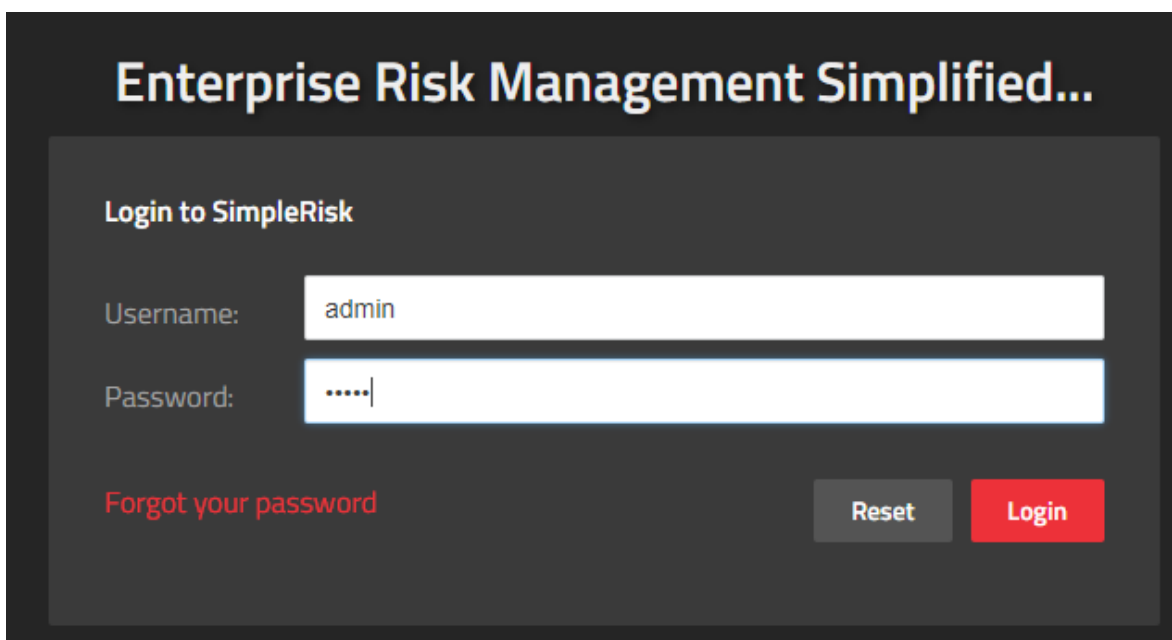


Ilustración 1: accomplished

- In configure, go to “Add and remove values” and in status delete all existing status and create the followings: Accepted, Avoided, Mitigated and Transferred.

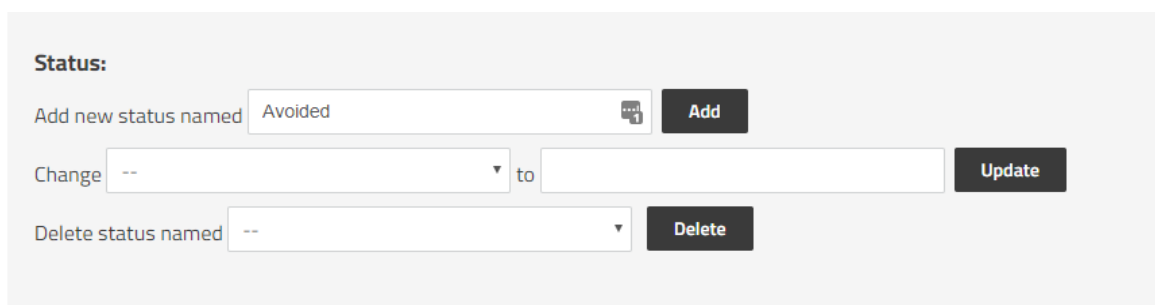


Ilustración 2: configuration to be made.

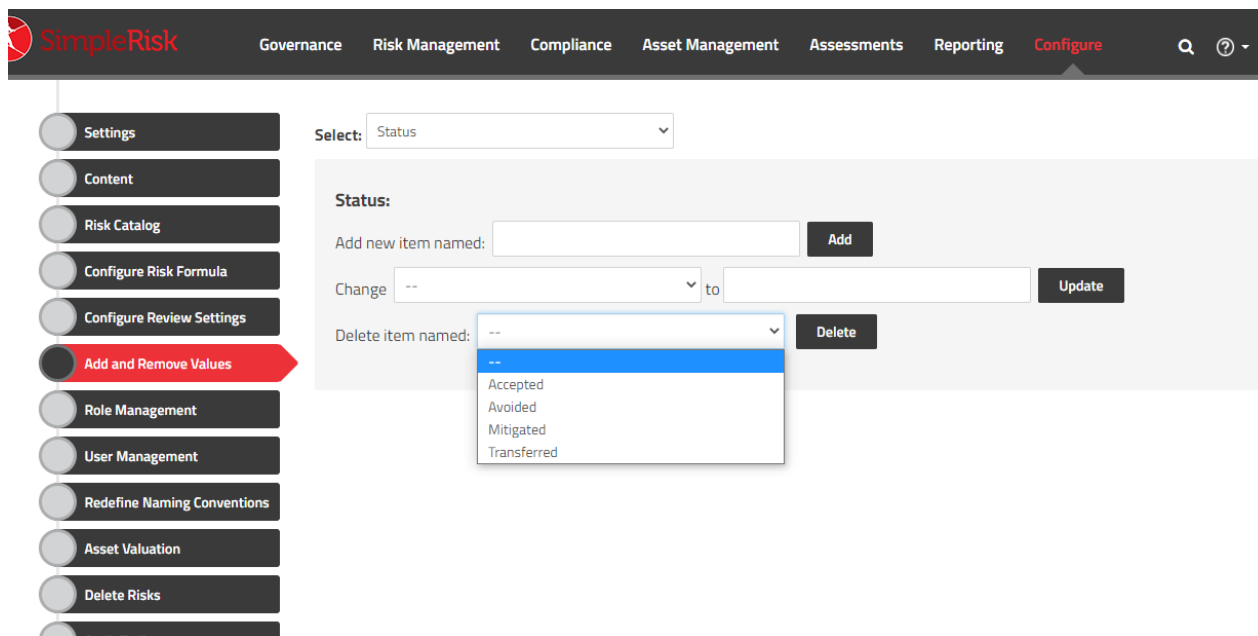


Ilustración 3: accomplished

2. SECTION TWO: ASSET INVENTORY

- Verify the asset information filled out in the “Asset Management” section in SimpleRisk. For each asset fill: Asset name, IP Address, Site/location, Team and Asset Details. In Asset Details you must place the following information:
 - Name of the owner
 - Name of the responsible
 - Name of the custodian
 - Asset users
 - Classification
 - Impact to availability
 - Impact to confidentiality
 - Impact to Integrity
 - Total Impact

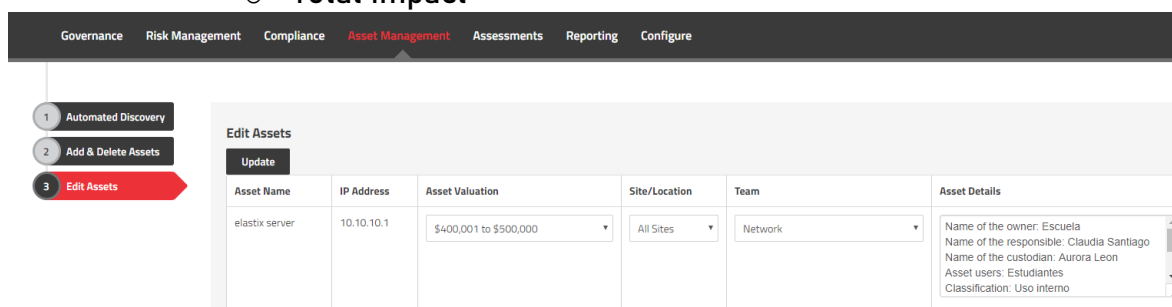


Ilustración 4: configuration to be made.

Centro de redes y servidores	192.168.0.14	\$100,0 ▾	All Sites ▾	Data Center & Storage ▾	Name of the owner: Escuela Name of the responsible: Oswaldo Castillo Name of the custodian: Juana Arco
Database Departamento de Registro	192.168.0.10	\$300,0 ▾	All Sites ▾	Database ▾	Name of the owner: Escuela Name of the responsible: James Torres Name of the custodian: Luis Catros
Network	N/A	\$0 to \$ ▾	-- ▾	None selected ▾	
Servidor Osiris	192.168.0.11	\$200,0 ▾	All Sites ▾	Information Security ▾	Name of the owner: Escuela Name of the responsible: Juan Luis Name of the custodian:
Servidor Salón de redes	192.168.0.12	\$100,0 ▾	All Sites ▾	Network ▾	Name of the owner: Escuela Name of the responsible: Carlos Pinto Name of the custodian:

Ilustración 5: accomplished

3. SECTION THREE: RISK ASSESSMENT

- In the “Assessment” section in Simple Risk start the “Critical Security Controls” and fill out and submit the questionnaire composed of 21 questions without thinking in an asset but the area or the process:

The screenshot shows the 'Critical Security Controls' assessment form. The sidebar on the left includes the following options: Available Assessments (selected), Pending Risks, Create Assessment, Edit Assessment, Send Assessment, Import/Export, Assessment Contacts, Questionnaire Questions, Questionnaire Templates, Questionnaires, Questionnaire Results, and Questionnaire Audit Trail. The main form area has a header 'Critical Security Controls' and an 'Asset Name' field with the value 'Anything'. Below this, there are two questions:

Do you actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access?

☐ Yes
☐ No

Comment

Do you actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution?

☐ Yes
☐ No

Comment

Ilustración 6: configuration to be made.

SimpleRisk Governance Risk Management Compliance Asset Management **Assessments** Reporting Configure

Available Assessments Pending Risks

Critical Security Controls

Asset Name: Servidor Osiris x Servidor Salón de redes x

Do you actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access?

☐ Yes ☒ No

access to unauthorized devices is not restricted and all devices are not actively tracked.

Do you actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution?

☒ Yes

Ilustración 7: accomplished

- After submit the questionnaire, all the suggested risk will appear in the “Pending risks” section.

Submission Date: 2018-01-29 18:52:04

Subject: Attackers can scan for remotely accessible n

Risk Scoring Method: OWASP ▼

Score Using OWASP

Owner: -- ▼

Asset Name: server unix

Risk created using the "Critical Security Controls" assessment.

Additional Notes:

Add **Delete**

Ilustración 8 : configuration to be made.

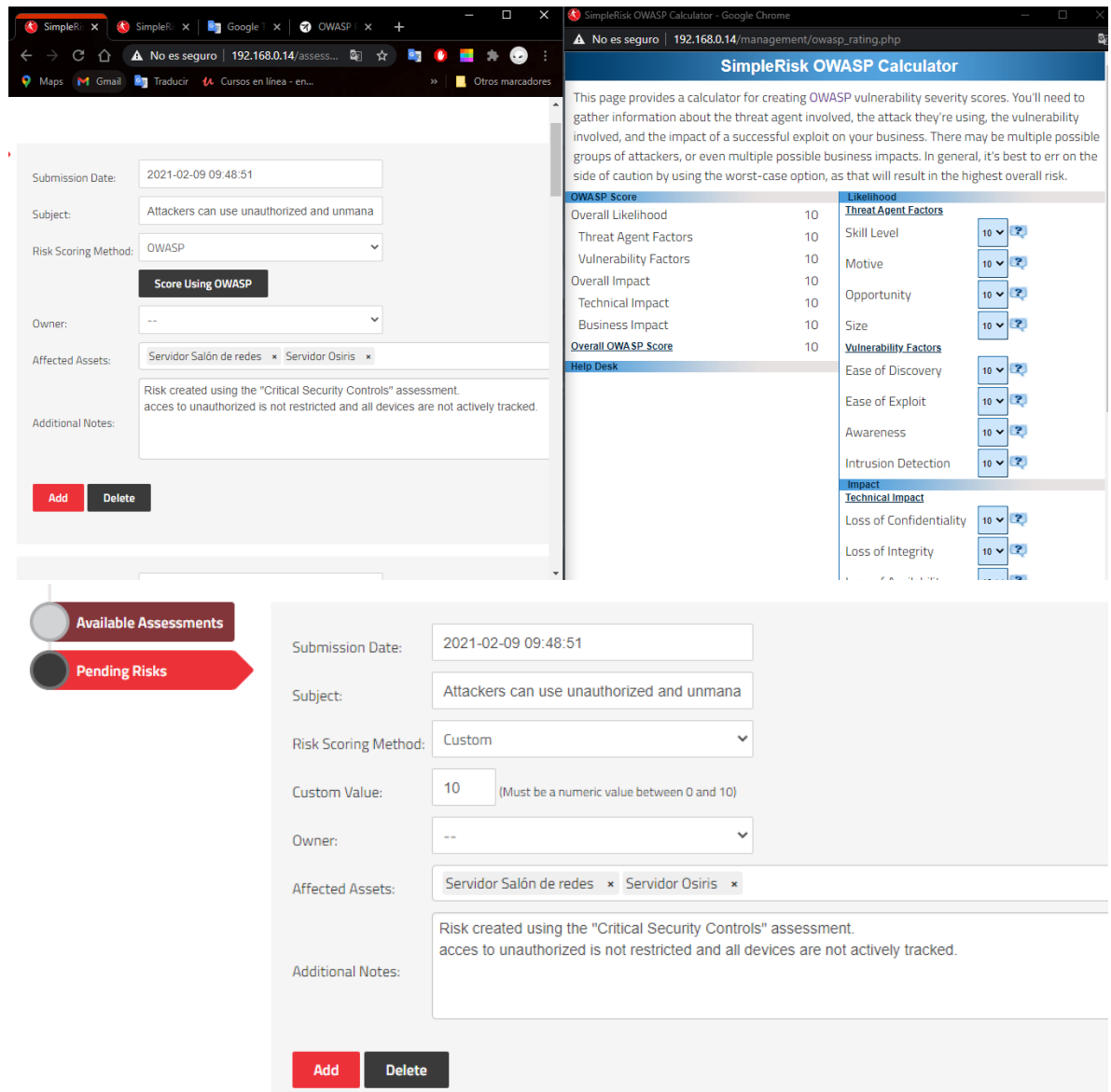


Ilustración 9: accomplished

- Analyze each risk reviewing: 1) The asset over which the risk applies and 2) The risk score using a Risk Scoring Methodology. SimpleRisk can use 4 Risk Scoring Methodology: OWASP, CVSS, DREAD and Classic.

OWASP Risk Rating Methodology calculates the Overall OWASP risk score using the Likelihood and the Impact. The Likelihood depends on the Threat agent and the Vulnerability Factors, and Impact depends on the Technical Impact and the Business Impact. You can click on the interrogation symbol to understand the meaning of the scale values:

SimpleRisk OWASP Calculator - Google Chrome

Seguro | https://cse.simplerisk.com/management/owasp_rating.php

SimpleRisk OWASP Calculator

This page provides a calculator for creating OWASP vulnerability severity scores. You'll need to gather information about the threat agent involved, the attack they're using, the vulnerability involved, and the impact of a successful exploit on your business. There may be multiple possible groups of attackers, or even multiple possible business impacts. In general, it's best to err on the side of caution by using the worst-case option, as that will result in the highest overall risk.

OWASP Score		Likelihood	
Overall Likelihood	9.25	Threat Agent Factors	
Threat Agent Factors	8.5	Skill Level	10 ?
Vulnerability Factors	10	Motive	10 ?
Overall Impact	9.25	Opportunity	10 ?
Technical Impact	8.5	Size	4 ?
Business Impact	10	Vulnerability Factors	
Overall OWASP Score	8.55625	Ease of Discovery	10 ?

Help Desk

How much service could be lost and how vital is it?

1 = Minimal Secondary Services Interrupted

5 = Minimal Primary Services Interrupted

5 = Extensive Secondary Services Interrupted

7 = Extensive Primary Services Interrupted

9 = All Services Completely Lost

Impact

Technical Impact

Loss of Confidentiality 10 ?

Loss of Integrity 10 ?

Loss of Availability 4 ?

Loss of Accountability 10 ?

Business Impact

Financial Damage 10 ?

Reputation Damage 10 ?

Non-Compliance 10 ?

Privacy Violation 10 ?

Submit

Ilustración 10: configuration to be made.

Overall Likelihood	5	Threat Agent Factors	
Threat Agent Factors	5	Skill Level	6 ▼ ?
Vulnerability Factors	5	Motive	4 ▼ ?
Overall Impact	6	Opportunity	4 ▼ ?
Technical Impact	6	Size	6 ▼ ?
Business Impact	6	Vulnerability Factors	
Overall OWASP Score	3	Ease of Discovery	4 ▼ ?
Help Desk		Ease of Exploit	4 ▼ ?
How much personally identifiable information could be disclosed?		Awareness	4 ▼ ?
3 = One Individual		Intrusion Detection	8 ▼ ?
5 = Hundreds of People		Impact	
7 = Thousands of People		Technical Impact	
9 = Millions of People		Loss of Confidentiality	7 ▼ ?
		Loss of Integrity	5 ▼ ?
		Loss of Availability	5 ▼ ?
		Loss of Accountability	7 ▼ ?
		Business Impact	
		Financial Damage	7 ▼ ?
		Reputation Damage	5 ▼ ?
		Non-Compliance	5 ▼ ?

Submission Date: 2021-02-09 09:48:52

Subject: Attackers can impersonate legitimate users b

Risk Scoring Method: Custom ▼

Custom Value: 10 (Must be a numeric value between 0 and 10)

Owner: -- ▼

Affected Assets: Servidor Salón de redes × Servidor Osiris ×

Additional Notes: Risk created using the "Critical Security Controls" assessment. the entire system life cycle is not managed.


✓ Risk ID 1007 submitted successfully!


Ilustración 11: accomplished


- This Overall Owasp Score (8.55) correspond to a High risk according to the heat map:


My Classic Risk Formula Is:

RISK =

I consider VERY HIGH risk to be anything greater than: 

I consider HIGH risk to be less than above, but greater than: 

I consider MEDIUM risk to be less than above, but greater than: 

I consider LOW risk to be less than above, but greater than: 

Update

☒ Very High Risk
 ☒ High Risk
 ☒ Medium Risk
 ☒ Low Risk
 ☐ Insignificant

Impact	Extreme/Catastrophic	5	2	4	6	8	10
	Major	4	1.6	3.2	4.8	6.4	8
	Moderate	3	1.2	2.4	3.6	4.8	6
	Minor	2	0.8	1.6	2.4	3.2	4
	Insignificant	1	0.4	0.8	1.2	1.6	2
			1	2	3	4	5
			Remote	Unlikely	Credible	Likely	Almost Certain
			Likelihood				

* All risk scores are adjusted to fit on a 0-10 scale.

Ilustración 12: configuration to be made.

Risk Catalog

Configure Risk Formula

Configure Review Settings

Add and Remove Values

Role Management

User Management

Redefine Naming Conventions

Asset Valuation

Delete Risks

Audit Trail

Extras

Announcements

Register & Upgrade

Health Check

About

My Classic Risk Formula Is:

RISK =

Update

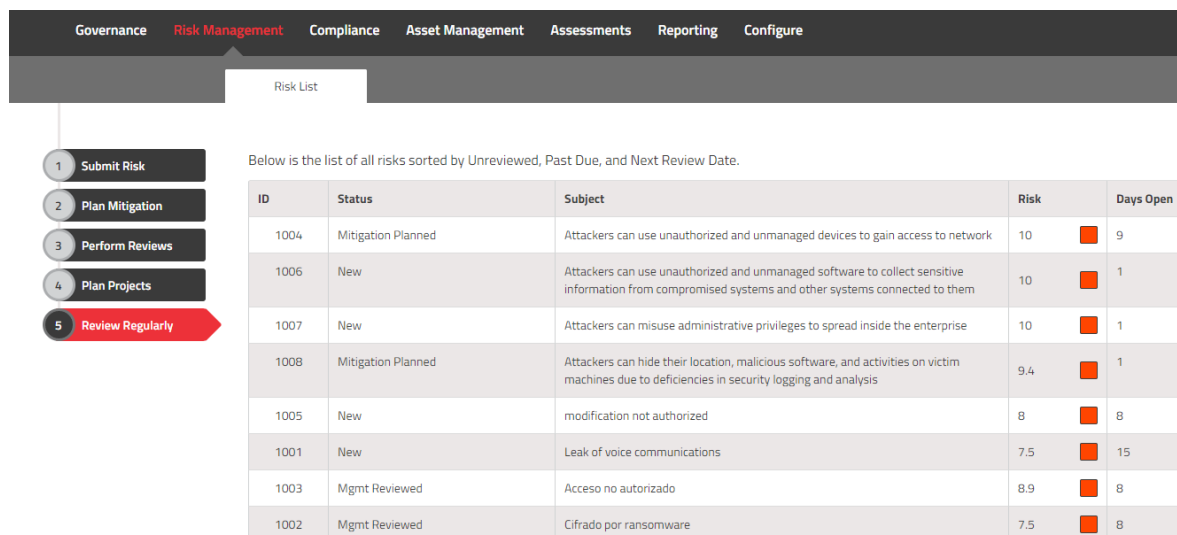
☒ Very High Risk
 ☒ High Risk
 ☒ Medium Risk
 ☒ Low Risk
 ☐ Insignificant

+ -

Impact	Extreme/Catastrophic	5	2	4	6	8	10
	Major	4	1.6	3.2	4.8	6.4	8
	Moderate	3	1.2	2.4	3.6	4.8	6
	Minor	2	0.8	1.6	2.4	3.2	4
	Insignificant	1	0.4	0.8	1.2	1.6	2
			1	2	3	4	5
			Remote	Unlikely	Credible	Likely	Almost Certain
			Likelihood				

Ilustración 13: accomplished

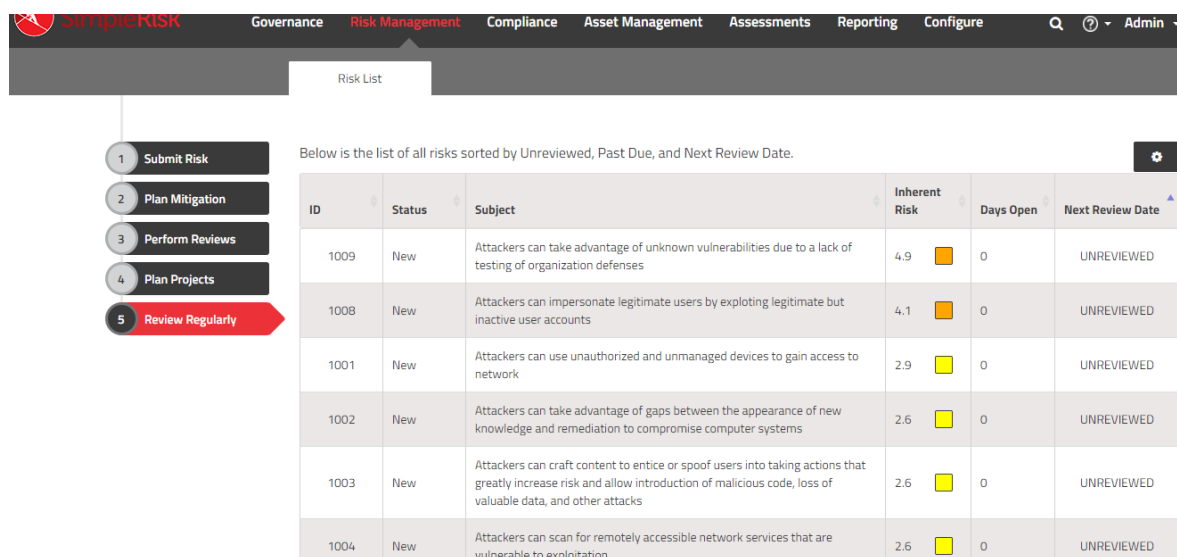
- After setting the Owasp Risk score you can add the risk. In the Risk Management tab you can view the available risks:



Below is the list of all risks sorted by Unreviewed, Past Due, and Next Review Date.

ID	Status	Subject	Risk	Days Open
1004	Mitigation Planned	Attackers can use unauthorized and unmanaged devices to gain access to network	10	9
1006	New	Attackers can use unauthorized and unmanaged software to collect sensitive information from compromised systems and other systems connected to them	10	1
1007	New	Attackers can misuse administrative privileges to spread inside the enterprise	10	1
1008	Mitigation Planned	Attackers can hide their location, malicious software, and activities on victim machines due to deficiencies in security logging and analysis	9.4	1
1005	New	modification not authorized	8	8
1001	New	Leak of voice communications	7.5	15
1003	Mgmt Reviewed	Acceso no autorizado	8.9	8
1002	Mgmt Reviewed	Cifrado por ransomware	7.5	8

Ilustración 14: configuration to be made.



Below is the list of all risks sorted by Unreviewed, Past Due, and Next Review Date.

ID	Status	Subject	Inherent Risk	Days Open	Next Review Date
1009	New	Attackers can take advantage of unknown vulnerabilities due to a lack of testing of organization defenses	4.9	0	UNREVIEWED
1008	New	Attackers can impersonate legitimate users by exploiting legitimate but inactive user accounts	4.1	0	UNREVIEWED
1001	New	Attackers can use unauthorized and unmanaged devices to gain access to network	2.9	0	UNREVIEWED
1002	New	Attackers can take advantage of gaps between the appearance of new knowledge and remediation to compromise computer systems	2.6	0	UNREVIEWED
1003	New	Attackers can craft content to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks	2.6	0	UNREVIEWED
1004	New	Attackers can scan for remotely accessible network services that are vulnerable to exploitation	2.6	0	UNREVIEWED

Ilustración 15: accomplished

- Get in on of the risk and you will see the most important information:

Risk List ID:1006 Attackers... x

Inherent Risk

10

High

Residual Risk

10

High

ID #: 1006

Status: New

Actions

Subject : Attackers can use unauthorized and unmanaged software to collect sensitive information from compromised systems and other systems connected to them

Hide Risk Scoring Details

OWASP Risk Scoring

Update OWASP Score

Risk Scoring Actions

Threat Agent Factors	Vulnerability Factors	Technical Impact	Business Impact
Skill Level: 10	Ease of Discovery: 10	Loss of Confidentiality: 10	Financial Damage: 10
Motive: 10	Ease of Exploit: 10	Loss of Integrity: 10	Reputation Damage: 10
Opportunity: 10	Awareness: 10	Loss of Availability: 10	Non-Compliance: 10
Size: 10	Intrusion Detection: 10	Loss of Accountability: 10	Privacy Violation: 10

Likelihood

Threat Agent Factors = (10 + 10 + 10 + 10) / 4

Vulnerability Factors = (10 + 10 + 10 + 10) / 4

Impact

Technical Impact = (10 + 10 + 10 + 10) / 4

Business Impact = (10 + 10 + 10 + 10) / 4

Full details of the OWASP Risk Rating Methodology can be found [here](#).

Show Risk Score Over Time

Ilustración 16: configuration to be made.

1 Submit Risk

2 Plan Mitigation

3 Perform Reviews

4 Plan Projects

5 Review Regularly

Inherent Risk

4,9

Medium

Residual Risk

4,9

Medium

ID #: 1009

Status: New

Actions

Subject : Attackers can take advantage of unknown vulnerabilities due to a lack of testing of organization defenses

View Risk Scoring Details

Show Risk Score Over Time

Details Mitigation Review

Edit Details

Risk Mapping:

Submitted By: Admin

Submission Date: 02/09/2021

Risk Source:

Category:

Risk Scoring Method: OWASP

Site/Location:

Risk Assessment:

External Reference ID:

Control Regulation:

Additional Notes: Risk created using the "Critical Security Controls" assessment. no, these simulations are performed.

Control Number:

Supporting Documentation: None

Affected Assets:

Servidor Osiris

Servidor:Salón de redes

Technology:

Team:

Ilustración 17: accomplished

- In mitigation tab you can select edit mitigation and select the controls that currently apply to the asset (the existing controls):

Details **Mitigation** Review Cancel Save Mitigation

Mitigation Submission Date: Current Solution:

Planned Mitigation Date: Requirements:

Planning Strategy: Recommendations:

Mitigation Effort:

Mitigation Cost:

Mitigation Owner:

Mitigation Team:

Mitigation Percent:

Supporting Documentation: Choose File 0 File Added Max 5 Mb

Select Mitigating Control(s) +

Select Mitigating Control(s)

☐ Control de Acceso

☒ A.8.1.4. Devolución de Activos

Cancel Add

Ilustración 18: configuration to be made.

Mitigation Submission Current Solution:

Date:

Planned Mitigation Date:

Planning Strategy:

Mitigation Effort:

Mitigation Cost:

Mitigation Owner:

Mitigation Team:

Mitigation Percent:

Mitigation Controls:

Security Requirements:

Security Recommendations:

Supporting Documentation: Choose File 0 File Added Max 5 Mb

Select for Mitigation Controls

☐ A.8.1.1. Auditoria extensa

☐ A.8.1.4. Devolución de

None selected

Ilustración 19: accomplished

- Before selecting a control, you must create it in the tab Governance, going to controls and pressing the plus (+) button:

Control Short Name

A.8.1.4. Devolución de Activos

Control Long Name

A.8.1.4. Devolución de Activos

Control Description

Devolución de Activos. Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

Supplemental Guidance

Ilustración 20: configuration to be made.

Ilustración 21: accomplished

- After selecting the controls, you must choose the “Mitigation percent” [0-100%] which represent how much the selected control reduce the risk. Additionally you must fill out the “current solution”.

Ilustración 22: configuration to be made.

Ilustración 23: accomplished

After refreshing the page, you will see that residual risk gets reduce:

Inherent Risk

10

High

Residual Risk

5

Medium

ID #: 1006

Status: Mitigation Planned

Actions

Subject : Attackers can use unauthorized and unmanaged software to collect sensitive information from compromised systems and other systems connected to them

View Risk Scoring Details

Show Risk Score Over Time

Details

Mitigation

Review

Edit Mitigation

Mitigation Submission Date:

02/07/2018

Planned Mitigation Date:

Planning Strategy:

Mitigation Effort:

Mitigation Cost:

\$0 to \$100,000

Mitigation Owner:

Mitigation Team:

Mitigation Percent:

50%

Current Solution:

Security Requirements:

Security Recommendations:

Supporting Documentation:

None

Ilustración 24: configuration to be made.

ID:1009 Att...

ID: 1009 Attacker...

Inherent Risk

4.9

Medium

Residual Risk

1.47

Low

ID #: 1009

Status: New

Actions

Subject : Attackers can take advantage of unknown vulnerabilities due to a lack of testing of organization defenses

View Risk Scoring Details

Show Risk Score Over Time

Ilustración 25: accomplished

After all risks have been set you should be able to see the resume in the “review regularly” section:

Below is the list of all risks sorted by Unreviewed, Past Due, and Next Review Date.

ID	Status	Subject	Risk	Days Open	Next Review Date
1004	Mitigation Planned	Attackers can use unauthorized and unmanaged devices to gain access to network	10	9	UNREVIEWED
1007	New	Attackers can misuse administrative privileges to spread inside the enterprise	10	1	UNREVIEWED
1008	Mitigation Planned	Attackers can hide their location, malicious software, and activities on victim machines due to deficiencies in security logging and analysis	9.4	1	UNREVIEWED
1005	New	modification not authorized	8	8	UNREVIEWED
1001	New	Leak of voice communications	7.5	15	UNREVIEWED
1006	Mitigation Planned	Attackers can use unauthorized and unmanaged software to collect sensitive information from compromised systems and other systems connected to them	6.8	1	UNREVIEWED
1003	Mgmt Reviewed	Acceso no autorizado	8.9	8	2018-04-29
1002	Mgmt Reviewed	Cifrado por ransomware	7.5	8	2018-04-29

Ilustración 26: configuration to be made.

2 Plan Mitigation	ID	Status	Subject	Risk	Days Open	Next Review Date
3 Perform Reviews	1009	Mitigation Planned	Attackers can take advantage of unknown vulnerabilities due to a lack of testing of organization defenses	4.9 	0	UNREVIEWED
4 Plan Projects	1008	Mitigation Planned	Attackers can impersonate legitimate users by exploiting legitimate but inactive user accounts	4.1 	0	UNREVIEWED
5 Review Regularly	1001	Mitigation Planned	Attackers can use unauthorized and unmanaged devices to gain access to network	2.9 	0	UNREVIEWED
	1002	Mitigation Planned	Attackers can take advantage of gaps between the appearance of new knowledge and remediation to compromise computer systems	2.6 	0	UNREVIEWED
	1003	Mitigation Planned	Attackers can craft content to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks	2.6 	0	UNREVIEWED
	1004	Mitigation Planned	Attackers can scan for remotely accessible network services that are vulnerable to exploitation	2.6 	0	UNREVIEWED
	1005	Mitigation Planned	Attackers can scan for remotely accessible network services that are vulnerable to exploitation	2.6 	0	UNREVIEWED
	1006	Mitigation Planned	Attackers can scan for remotely accessible network services that are vulnerable to exploitation	2.6 	0	UNREVIEWED
	1007	Mitigation Planned	Attackers can gain access to sensitive data, alter important information, or use compromised machines to pose as trusted systems on our network by exploiting vulnerable services and settings	2.5 	0	UNREVIEWED

Ilustración 27:accomplished

Then you must review all the risks to decide what to do next. The treatment option can be:

- **Mitigate:** Apply an additional control to reduce the Residual Risk.
- **Accept:** Accept the risk because the Residual Risk is under the Acceptable Risk Threshold, or because the cost of implementing the control is more expensive that the asset value.
- **Avoid:** Eliminate the origin of the Risk (for example replace the asset for a new one with the vulnerability and in this way, eliminate the origin of the risk).
- **Transfer:** Pass the Residual Risk to a third party (for example an insurance company).

Option	Residual risks	Status	What to to in SimpleRisk?	
Mitigate the risk	i) When $10 > \text{Residual risks} > 4$ AND ii) It is possible to implement a control to mitigate it	Mitigated	Add additional controls in the "Mitigation Tab" or/and adjust the "Mitigation Percent" so the Residual Risk can be < 4	Change risk status to Mitigated

Accept the risk	i) When $4 > \text{Residual risks} > 0$ OR ii) When the cost of implementing the control is more expensive than the asset value.	Accepted	Do nothing because the risk is low	Change risk status to Accepted
Transfer the risk	i) When $10 > \text{Residual risks} > 4$ AND ii) It is NOT possible to implement a control to mitigate it	Transferred	In "Security Recommendations" explain how to transfer the risk	Change risk status to Transferred
Avoid the risk	i) When $10 > \text{Residual risks} > 4$ AND ii) It is NOT possible to implement a control to mitigate it	Avoided	In "Security Recommendations" explain how to avoid the risk	Change risk status to Avoided

The screenshot displays the SimpleRisk web application interface. The top navigation bar includes links for Governance, Risk Management (active), Compliance, Asset Management, Assessments, Reporting, and Configure. A search icon and an Admin link are also present. Below the navigation bar, a sidebar on the left contains a list of actions: 1 Submit Risk, 2 Plan Mitigation, 3 Perform Reviews, 4 Plan Projects, and 5 Review Regularly (highlighted in red). The main content area shows details for a specific risk with ID # 1006, titled "Attacker...". The risk is categorized as "Mitigation Planned". Two yellow boxes display the risk scores: Inherent Risk 2.6 (Low) and Residual Risk 0.39 (Low). The subject of the risk is "Attackers can scan for remotely accessible network services that are vulnerable to exploitation". Below the subject, there are links to "View Risk Scoring Details" and "Show Risk Score Over Time". At the bottom, a dropdown menu allows the user to "Set Risk Status To" with options: Accepted (selected), --, Avoided, Mitigated, and Transferred. An "Update" button is next to the dropdown.

Ilustración 28: accomplished

2 Plan Mitigation	ID	Status	Subject	Inherent Risk	Days Open	Next Review Date
3 Perform Reviews	1009	Mitigated	Attackers can take advantage of unknown vulnerabilities due to a lack of testing of organization defenses	4.9 	0	UNREVIEWED
4 Plan Projects	1008	Mitigated	Attackers can impersonate legitimate users by exploiting legitimate but inactive user accounts	4.1 	0	UNREVIEWED
5 Review Regularly	1001	Accepted	Attackers can use unauthorized and unmanaged devices to gain access to network	2.9 	0	UNREVIEWED
	1002	Accepted	Attackers can take advantage of gaps between the appearance of new knowledge and remediation to compromise computer systems	2.6 	0	UNREVIEWED
	1003	Accepted	Attackers can craft content to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks	2.6 	0	UNREVIEWED
	1004	Accepted	Attackers can scan for remotely accessible network services that are vulnerable to exploitation	2.6 	0	UNREVIEWED
	1005	Accepted	Attackers can scan for remotely accessible network services that are vulnerable to exploitation	2.6 	0	UNREVIEWED
	1006	Accepted	Attackers can scan for remotely accessible network services that are vulnerable to exploitation	2.6 	0	UNREVIEWED
	1007	Accepted	Attackers can gain access to sensitive data, alter important information, or use compromised machines to pose as trusted systems on our network by exploiting vulnerable services and settings	2.5 	0	UNREVIEWED

Ilustración 29: accomplished

4. SECTION FOUR:

- **Executive Summary:** Prepare an Executive Summary where you can resume the most important aspect of the risk analysis that you have just done. You can use graphs, tables, figures or any other element obtained from SimpleRisk. The executive summary must help help to explain to the manager: the higher risks in the company, how many risks where transferred/avoided/accepted/mitigated and the change in the risk value before controls (total risk) and after controls (residual risk).

Some interesting figures can be obtained from the “Reporting” Tab in SimpleRisk:

- Mitigated vs unmitigated
- Level of risks [Very High, High, Medium, Low] from the Risk Dashboard
- Risk status [Accepted, Avoided, Mitigated, Transferred] from the Risk Dashboard
- Risk source [External, People, Process, System] from the Risk Dashboard
- Risk by Asset
- High Risk Report

Executive Summary



Ilustración 30: Executive summary

CONCLUSIONS

In the course of this laboratory we learned the use of different tools for the identification of risks, their classifications and impacts in the business field, as well as we learned to use Simple Risk to be able to carry out the steps in risk mitigation, thus lowering its criticality.

REFERENCES

- Trendmicro, cybercriminals, <https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals>
- Samsungmobile, securityupdate <https://security.samsungmobile.com/securityUpdate.smsb>
- First, cvss, <https://www.first.org/cvss/v3.0/specification-document>
- Android, security bulletin, <https://source.android.com/security/bulletin/2021-01-01>
- Ncsc, cyberaware, <https://www.ncsc.gov.uk/cyberaware/home>
- BBC, technology, <https://www.bbc.com/news/technology>
- OWASP, OWASP Risk Rating Methodology, https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology