The objective of this document is to show in a general way the proposal of a risk assessment model to professionals related to the cybersecurity world. This in order to collect and analyze relevant expert opinions on the possible application and timeliness of the proposed model.

RISK ASSESSMENT MODEL PROPOSAL

This risk assessment proposal has two different perspectives, one qualitative and the other quantitative, due to the possible differences in the maturity, size and resources of the organizations. For both models, the following variables were identified as the main ones:

Table S1. Variables summarizing

Variables	Qualitative Proposal	Quantitative proposal
Relevance of the asset in the process (RAP)	Defined by the owner of the asset	RAP Low =1, RAP Medium =2, RAP High = 3
Monetary value of the asset in dollars (MVA)		Proposed by the owner of the asset
Value of the information contained in the asset in dollars (VICA)		Proposed by the owner of the asset
Economic value of the asset (EVA)	EVA = RAP	$\mathrm{EVA} = (\mathrm{MVA} + \mathrm{VICA}) * \mathrm{RA¨P}$
Value of vulnerabilities (V)	NIST algorithm CVSS: "Low" = (0-3.9) "Medium" = (4 -6.9) "High" = (7 to 10)	V= CVSS quantitative version
Countermeasure Maturity (CM)	Low: Change or not effective Low: (0-3) times effective Medium: (4-8) times effective High: (9-10) times effective	CM = number of times the control/countermeasure has been effective (max. 10).
Countermeasure effectiveness (CE)	CE = CM	$\mathrm{CE} = (IM_{t-1} - IM_t) * CM$
Asset Exposure (AE)	CM and V Related by table	Percentage measure defined by the SANS institute model
Information available on the asset (AAI)	" Low" = Incidents <1 per year "Medium" =Incidents >1, <2 per year "High" = Incidents > 2 per year	Number of incidents published per year
Threat value (T)	AAI and V Related by table	$\mathrm{T} = [(\mathrm{V} + \mathrm{AAI})/2] * \mathrm{EVA}$
Number of occurrences (ON)	Low: 1 to 4 incidents per year Medium: 5 to 9 incidents per year High: 10 incidents or more per year	Number of negative events related to the asset with public information.
Registered years (YR)		Years of existence of the asset
likelihood (ARO)	ARO = ON	$\mathrm{ARO} = \frac{\mathrm{ON}}{\mathrm{YR}}$
Impact (IM)	T and AE Related by table	$\mathrm{IM} = \mathrm{T} * \mathrm{AE}$
Risk exposure value (R)	IM and ARO Related by table	$R_1 = \mathrm{IM} * \mathrm{ARO}$ $R_2 = [(T/EVA) * \mathrm{ARO}]/2$
Acceptable risk value (ARV)	Value of the risk immediately lower than the current one	Defined by the organization
Residual risk (RR)	R y CM Related by table	$RR = (R_t - R_{t-1})$

1) Qualitative proposal

These variables are approached from a qualitative point of view using three scales for each of the variables and related sub-variables, "High", "Medium" and "Low".

The economic value of the asset (EVA): Directly defined by the relevance of the assets in the processes (RAP) they support or in which they participate.

1. "High", if the loss or impairment of the asset has a high economic impact on the operation of the company.

2. "Medium", if the loss of the asset has a temporary impact of the operation and economic losses to be considered.

3. "Low" if the commitment or loss of the asset does not directly affect the operation and has economic repercussions that are not representative for the organization.

Value of vulnerabilities (V) was defined using the CVSS algorithm. For this calculation, the vulnerability calculation link provided by the National Institute of Standard and Technology (NIST) https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator (NIST, 2022)

The CVSS algorithm itself contemplates values from 0 to 10, and includes a scale for assessing vulnerabilities:

- 0 to 3.9 = "low
- 4 to 6.9 = "medium".
- 7 to 10 = "high".

Countermeasure efficiency (CE): It is directly related to the maturity of the countermeasure (CM) and therefore the following relationship is defined:

1. If it receives any change, is recently implemented or is detected as ineffective (Low)
2. High (between 9 and 10 continuous reviews of the control where it is effective)
3. Medium (between 4 and 8 continuous reviews of the control where effective)
4. Low (<=3 continuous reviews of the control where it is effective)

Available asset information (AAI): Is related with the information published online about vulnerabilities of certain assets

- Web information of less than one security incident per year = low
- Web reporting of 1 to 2 incidents per year = medium
- Web reporting of more than 2 incidents per year = high

Asset exposure (AE): This variable is directly related to two other variables 1) Control maturity, 2) Asset vulnerabilities (See Table S2).

Table S2 Exposure values of the asset

Vulnerability and control maturity			
Maturity → *Vulnerability ↓*	***Low***	***Medium***	***High***
Low	*Medium*	*Low*	*Low*
Medium	*High*	*Medium*	*Low*
High	*High*	*High*	*Medium*

Threat value (T): The threat value is directly related to the vulnerabilities of the asset and the information available in the asset's cyberspace. The relationship can be seen in Table S3.

Table S3 Threat value

Vulnerability and asset information			
Information → *Vulnerability ↓*	***Bajo***	***Medio***	***High***
High	*Medium*	*Medium*	*High*
Medium	*Low*	*Medium*	*Medium*
Low	*Low*	*Low*	*Medium*

Probability value (ARO): Transferring the calculation model proposed by the SANS Institute, the following relationship with the **number of occurrences (ON)** was established**:**

- 10 incidents or more in a high year
- 5 to 9 incidents in a medium year
- 1 to 4 incidents per year low.

Impact value (IM): The impact relates the variables threat and exposure of the asset as shown in Table S4.

Table S4 Impact value

Asset exposure and threat value			
Threat → *Exposition ↓*	**Low**	***Medium***	**High**
High	*Medium*	*Medium*	*High*
Medium	*Low*	*Medium*	*Medium*
Low	*Low*	*Low*	*Medium*

Risk exposure value (R): a classical relationship between impact and probability as shown in Table S5 will be considered.

Table S5 Risk exposure value

Impact and Probability			
Likelihood → *Impact ↓*	***Bajo***	***Medio***	***Alto***
Alto	*Medio*	*Alto*	*Alto*
Medio	*Bajo*	*Medio*	*Alto*
Bajo	*Bajo*	*Bajo*	*Medio*

Acceptable value of the risk (AVR): This value is determined according to the desired value of the risk in a new execution, being a mobile value, the organization will seek to obtain the value next lower than the value of the risk calculated previously:

- If the calculated risk is high the desired risk will be a medium value.
- If the calculated risk value is medium, a low desired risk value will be expected.
- If the calculated risk value is low, the value will be sought to be kept as low.

Residual risk (RR): Relationship between control maturity and risk exposure as shown in Table S6.

Table S6 Risk exposure value

Control maturity and risk			
Control maturity → *Risk ↓*	***Low***	***Medium***	***High***
High	*Medium*	*High*	*High*
Medium	*Low*	*Medium*	*High*
Low	*Low*	*Low*	*Medium*

Quantitative proposal

Economic value of the asset (EVA): The relevance of a quantitative calculation of the economic value of the asset lies in being able to value it in monetary terms, so the following relationship is proposed:

1) Monetary value of the asset in dollars = MVA
2) Value of the information contained in the asset in dollars = VICA
3) Relevance of the asset in the process = RAP

Where **EVA** and **VICA** will be defined by the owner or person responsible for the assets and for the **RAP** the following relationship will be established.

- Low RAP =1
- Medium RAP =2
- High RAP = 3

Finally, to calculate the economic value of the asset, we have the following relationship

$$Economical\ Value\ of\ Asset\ (EVA) = (MVA + VICA\ ) * RPA$$

Vulnerability value (V): For the vulnerability value, the CVSS algorithm has been selected in its version 3, which integrates variables such as integrity, availability, and availability of an information asset for its

calculation. This proposal includes the calculation model automated by NIST. The result is a weighted scale with values from 0 to 10.

URL for the NIST CVSS calculation algorithm: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator (NIST, 2022)

Countermeasure maturity (CM): Directly related to the number of reviews where the countermeasure has been assessed as effective.

CM = number of revisions where the control has been effective with a maximum value of 10 and a minimum of 1.

Countermeasure effectiveness (CE): The effectiveness of the countermeasure lies in its ability to maximize or reduce a risk, so it can only be measured after its implementation in relation to the impact and its maturity as follows:

$$\mathrm{CE} = (IM_{t-1} - IM_t) * CM$$

Asset exposure (AE): It is defined according to the step-by-step Quantitative Risk Analysis of the SANS Institute: https://www.sans.org/white-papers/849/ (SANS Institute, 2002)

Available Asset Information (AAI): Directly related to the number of negative events related to the asset with public information per year.

Threat value (TV): The same variables of the quantitative model are considered, including the economic value of the asset.

- Vulnerabilities value (V)
- Available asset information on the internet (AAI)
- Economic Value of the Asset (EVA)

$$\mathrm{TV} = [(\mathrm{V} + \mathrm{AAI})/2] * \mathrm{EVA}$$

Number of occurrences (ON): Number of negative events related to the asset with public information.

Years registered (YR): Years of existence of the asset.

Number of occurrences (OR): Number of incidents related to the asset.

Years registered (YR): Number of years of operation of the asset.

Probability value (ARO): For the probability value, the calculation ratio created by SANS Institute was considered. The annualized rate of occurrence (ARO) is formulated as follows:

$$Probability = ARO = \frac{Number\ of\ occurrence\ (OR)}{Years\ registered\ (YR)}$$

Impact value (IM): The impact value is a function of variables related to the asset and the threats to the asset, considering the previous relationships, the following relationship is proposed:

$$Impact\ (IM) = T * AE$$

Risk exposure value (R): The calculation of risk is proposed as a direct and proportional relationship between impact and probability, which, in turn, are calculated taking into account other variables previously defined to give a non-economic value.

$$R_1(\mathrm{Economical}) = \mathrm{IM} * \mathrm{ARO}$$

$$R_2(\text{No economical}) = [(TV/EVA) * \text{ARO}]/2$$

Acceptable value of risk (ARV): Target value of risk established by the owners of the asset.

Residual risk (RR): Risk value resulting from the difference between the risk exposure value before applying a countermeasure and after applying it.

$$RR = (R_t - R_{t-1})$$

References

NIST. (2022). *Common Vulnerability Scoring System Calculator V3.1*. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

SANS Institute. (2002). *Quantitative Risk Analysis Step-By-Step*. https://sansorg.egnyte.com/dl/arTGfdKrUg