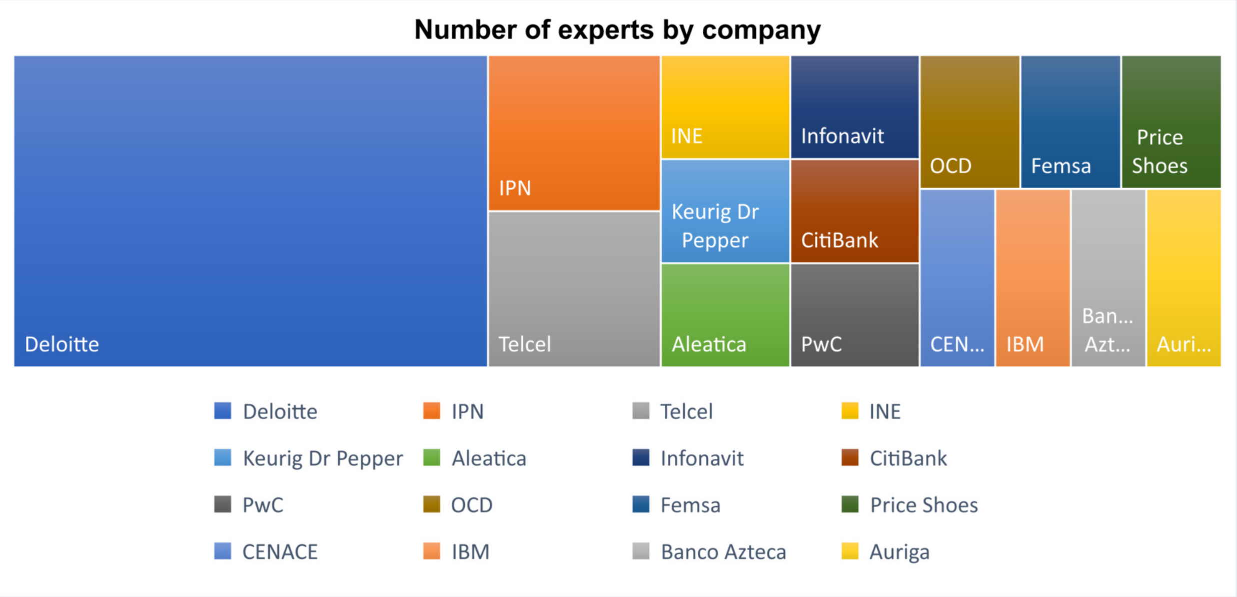
Cybersecurity Risk Assessment Model (TARAMCyber)

Additional information

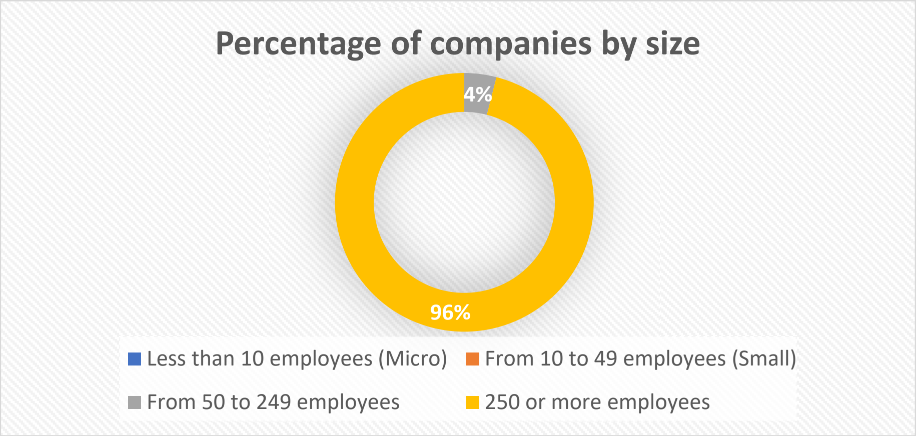
Isaac D. Sánchez-García, Jezreel Mejía, Tomás San Feliu and Mirna A. Muñoz

Section I: Demographic results

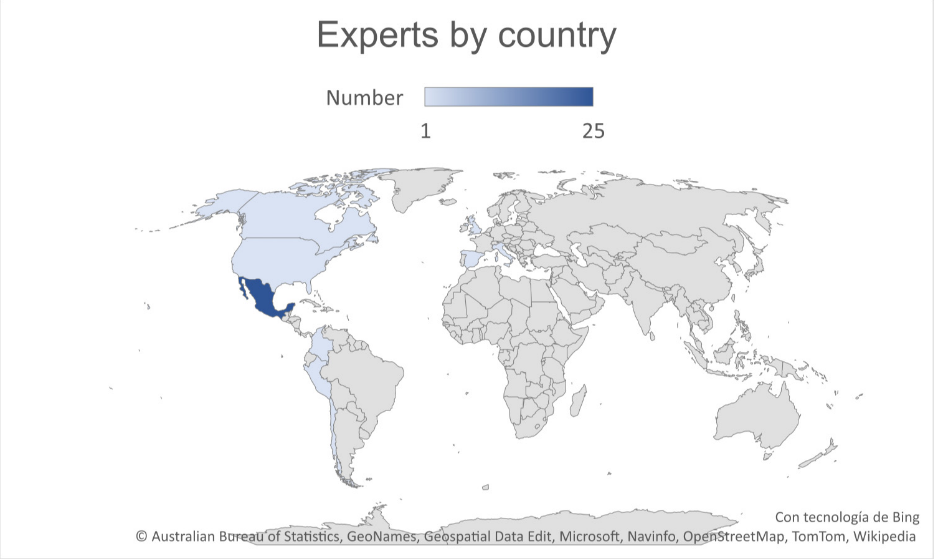
1.- What is the name of your organization?



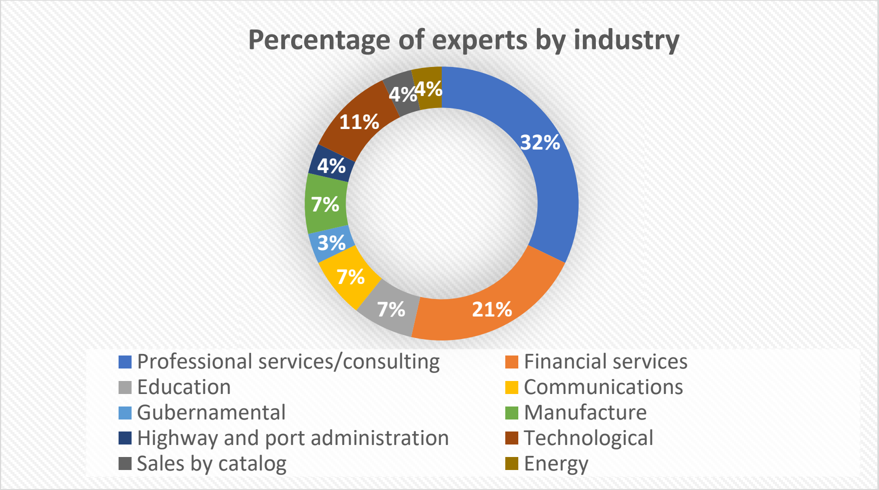
2.- What is the size of your organization?



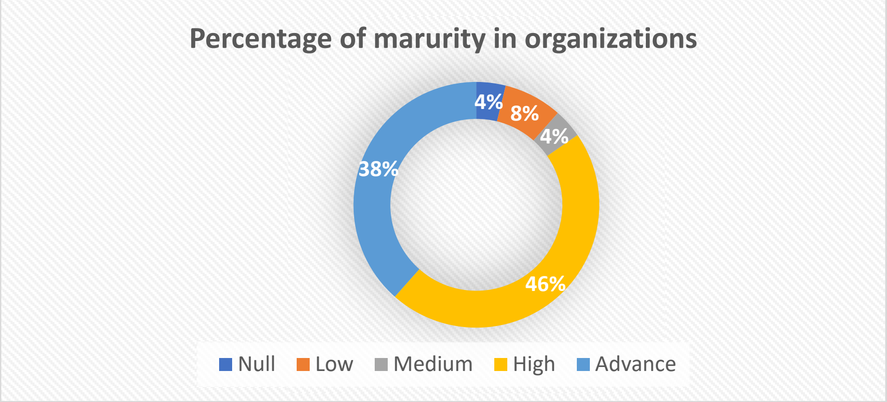
3.-What is the country where you work?


Experts by country
Number
1
25
Con tecnología de Bing
© Australian Bureau of Statistics, GeoNames, Geospatial Data Edit, Microsoft, Navinfo, OpenStreetMap, TomTom, Wikipedia

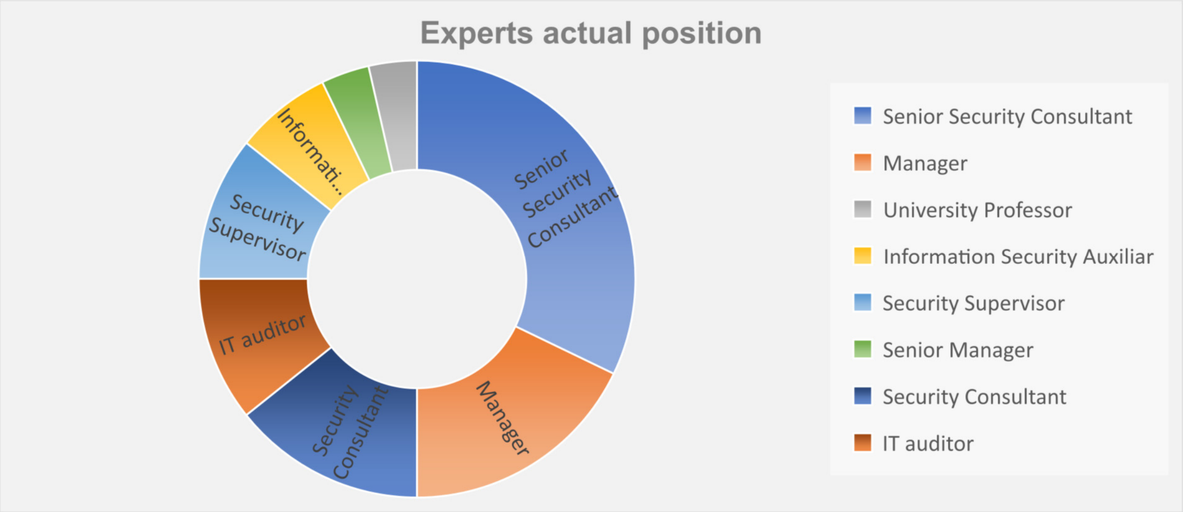
4.-Which industry is your organization primarily in?



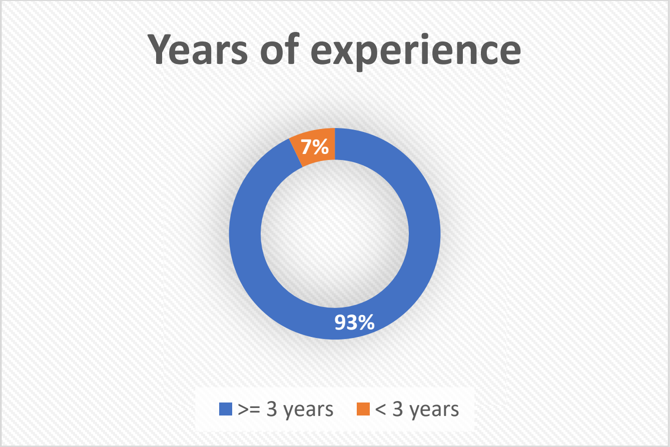
5.- At which cybersecurity maturity level would you classify your organization?



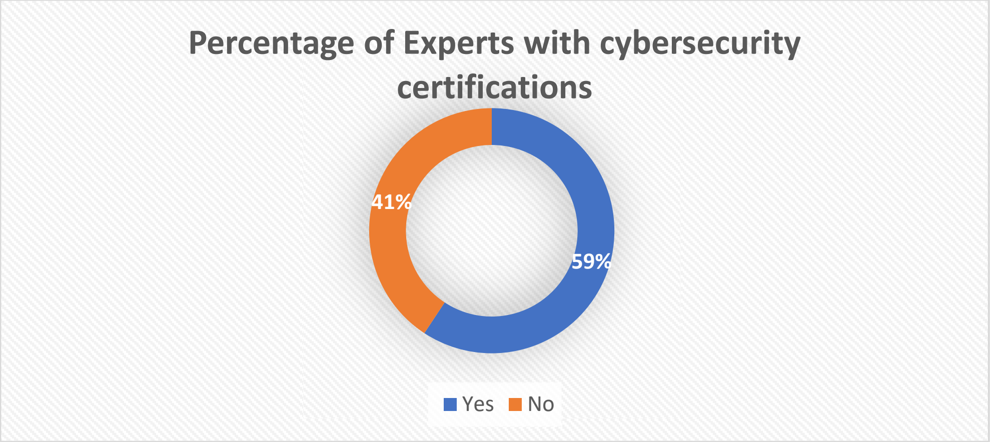
6.-What is your current position?



7.- How many years of experience do you have in information security or cybersecurity?



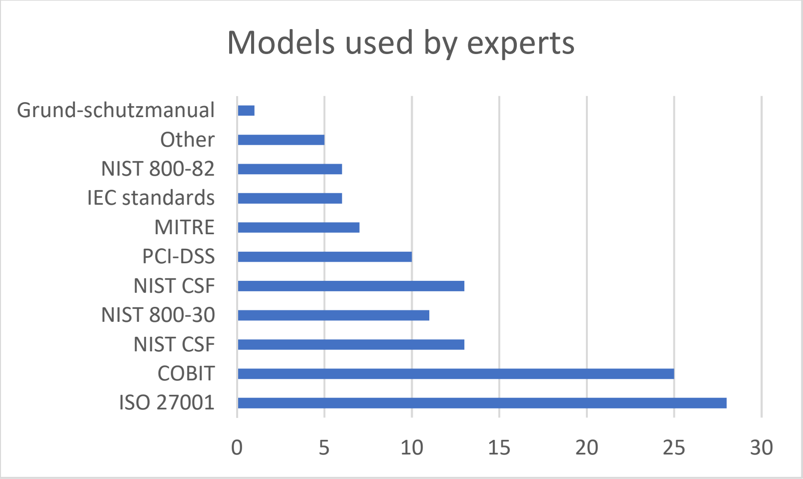
8.- Do you have information security or cybersecurity certifications?



Section II: Risk management practices

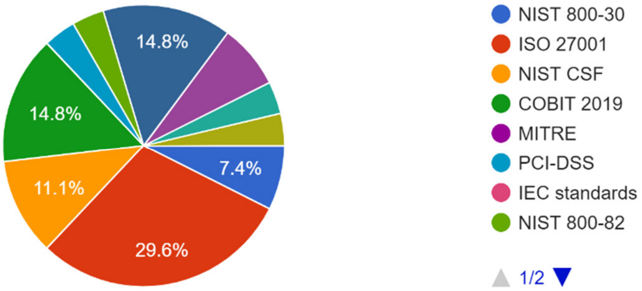
9.- Indicate which of the following risk management models you are familiar with or have used

- NIST 800-30
- ISO 27001
- NIST CSF
- COBIT
- MITRE
- PCI-DSS
- IEC standards
- NIST 800-82
- Grund-schutzmanual
- Other



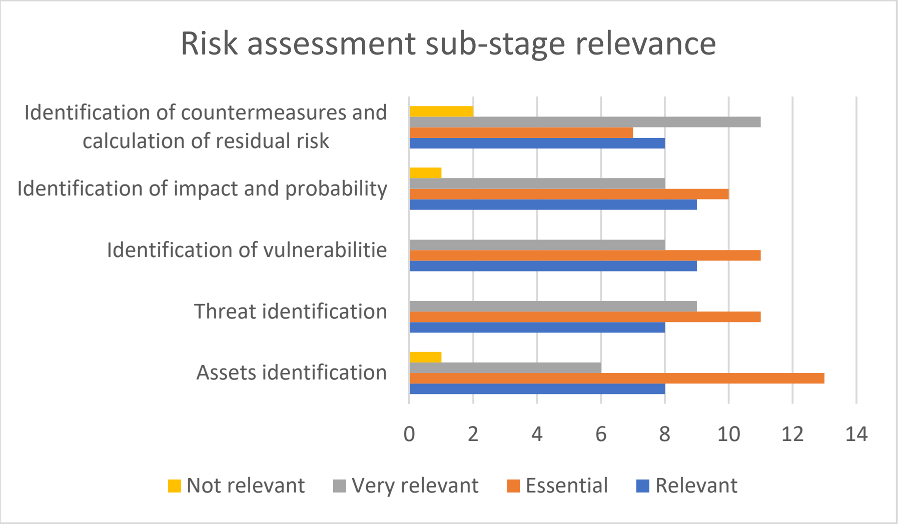
10.- Indicate which of the following risk management models you are familiar with or have used

- NIST 800-30
- ISO 27001
- NIST CSF
- COBIT
- MITRE
- PCI-DSS
- IEC standards
- NIST 800-82
- Grund-schutzmanual
- Independent model
- There is no ISMS in the organization



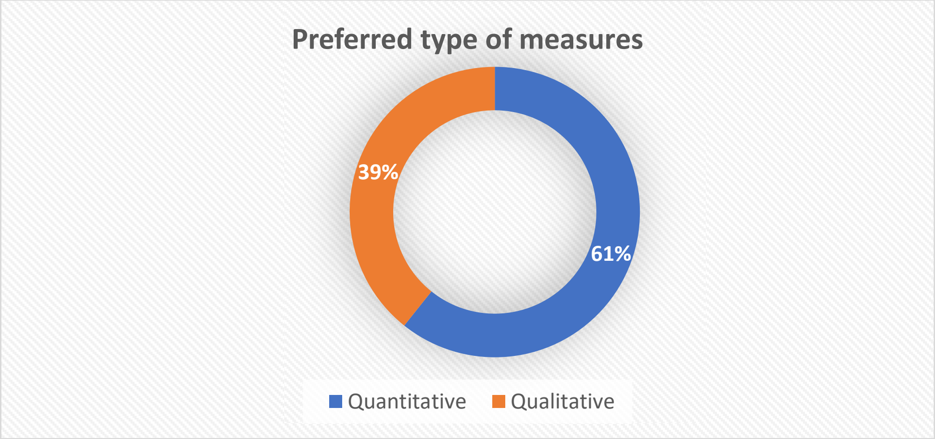
11.- Indicate according to your perspective what is the relevance of each sub-step of risk management?

- Asset identification
- Threat identification
- Identification of vulnerabilities
- Identification of impact and probability
- Identification of countermeasures and calculation of residual risk



12.- What type of risk calculation do you prefer in a risk assessment model?

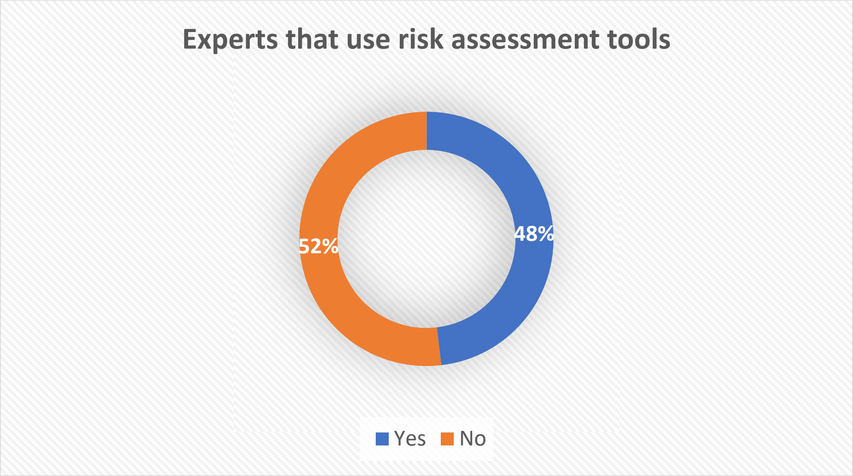
- Qualitative
- Quantitative



13.- Add a comment justifying your previous answer

Open answers

14.- Do you or would you use a tool to automate the risk assessment process?



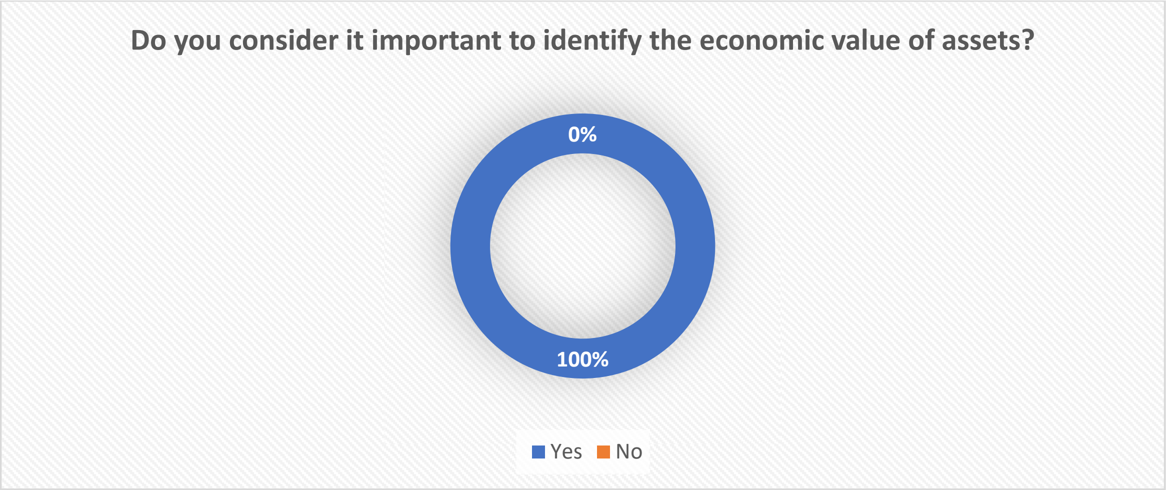
15.- If the above answer is "Yes", please mention which tool you use or would use in your organization.

Open answers

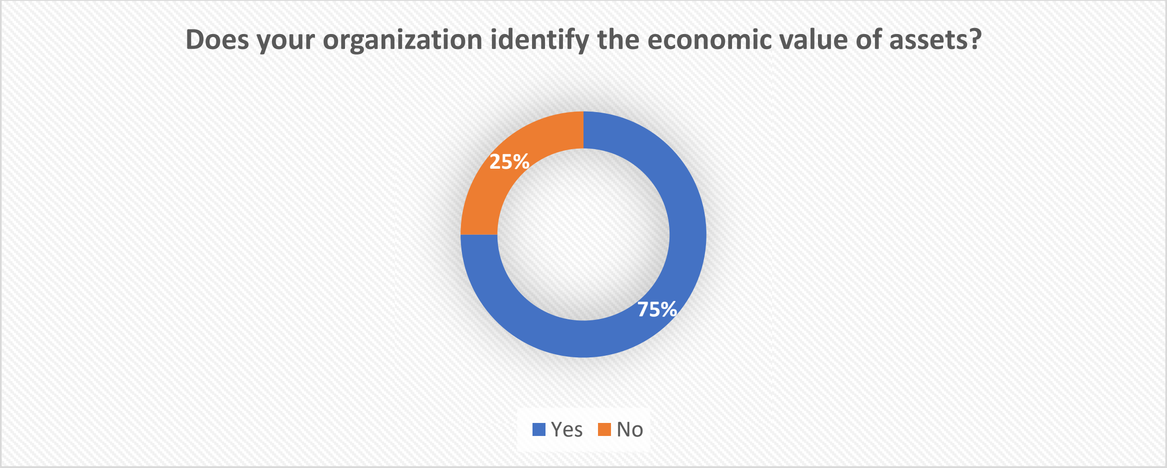
Section III: Comments on Risk Assessment Variables

Identification and evaluation of assets

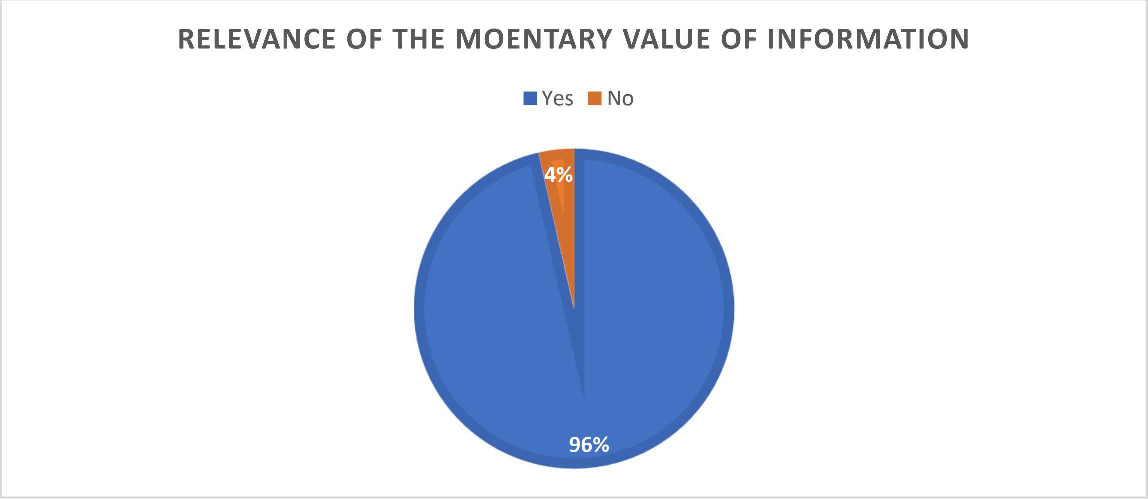
16.- Do you consider it important to identify the economic value of assets?



17.- Does your organization identify the economic value of assets?

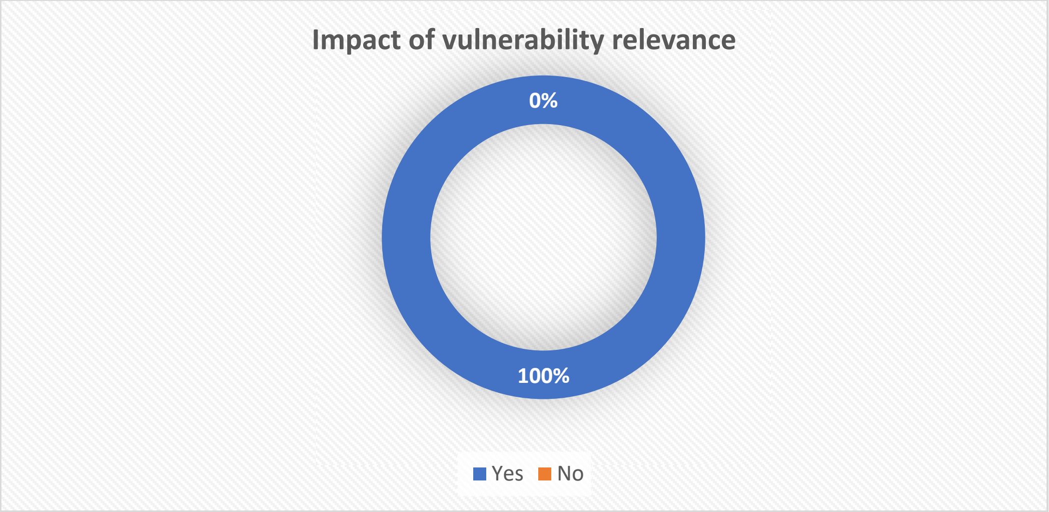


18.- Do you consider that the value of the information contained in the asset and its relevance in the process helps to know the monetary value of the asset?

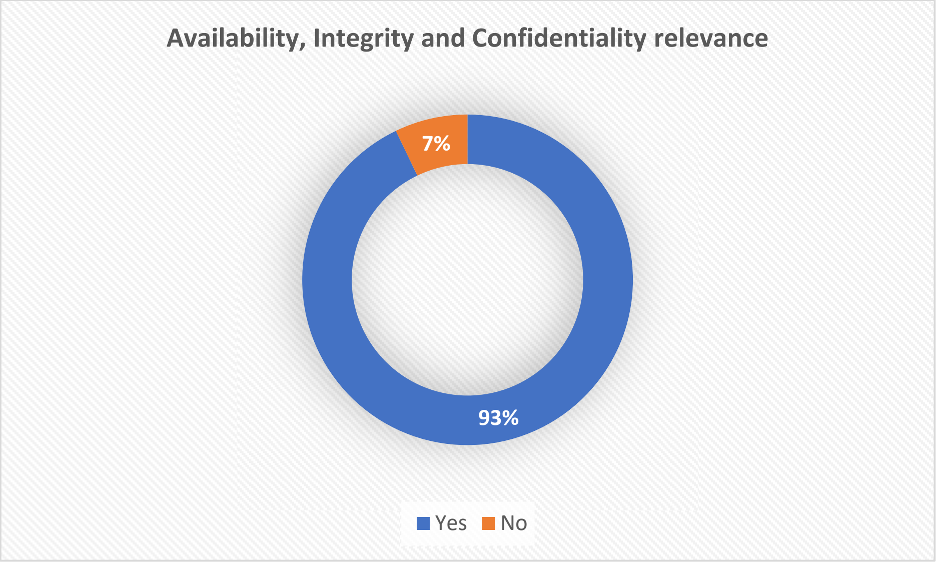


Identification and evaluation of vulnerabilities

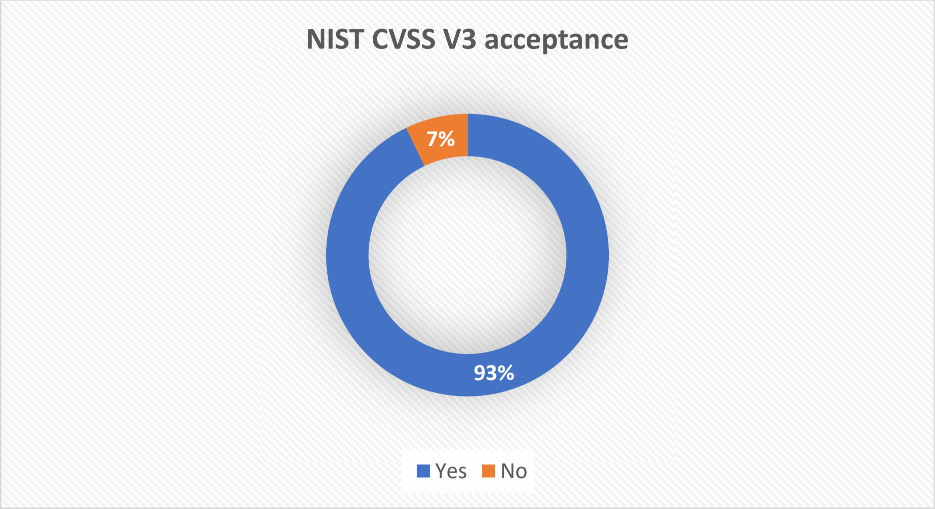
19.- Do you consider it important to measure the impact of vulnerability?



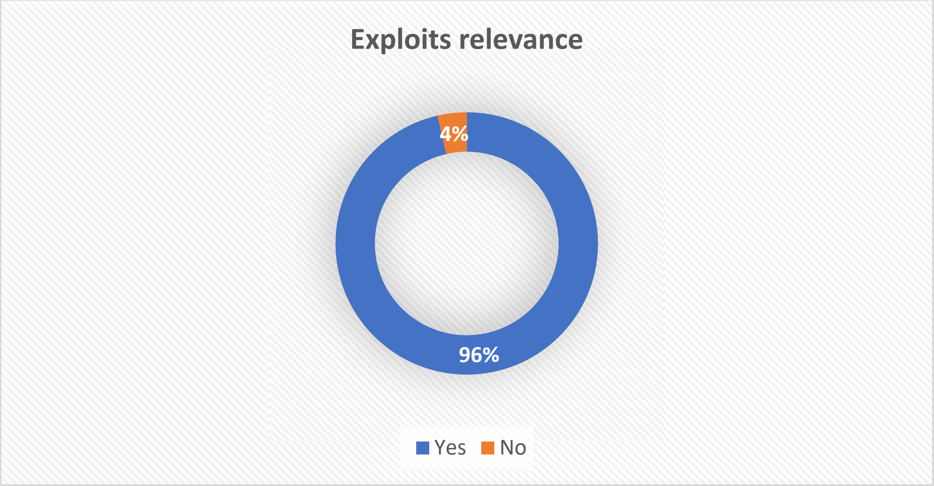
20.- Does your organization use impact metrics for Information Availability, Integrity and Confidentiality?



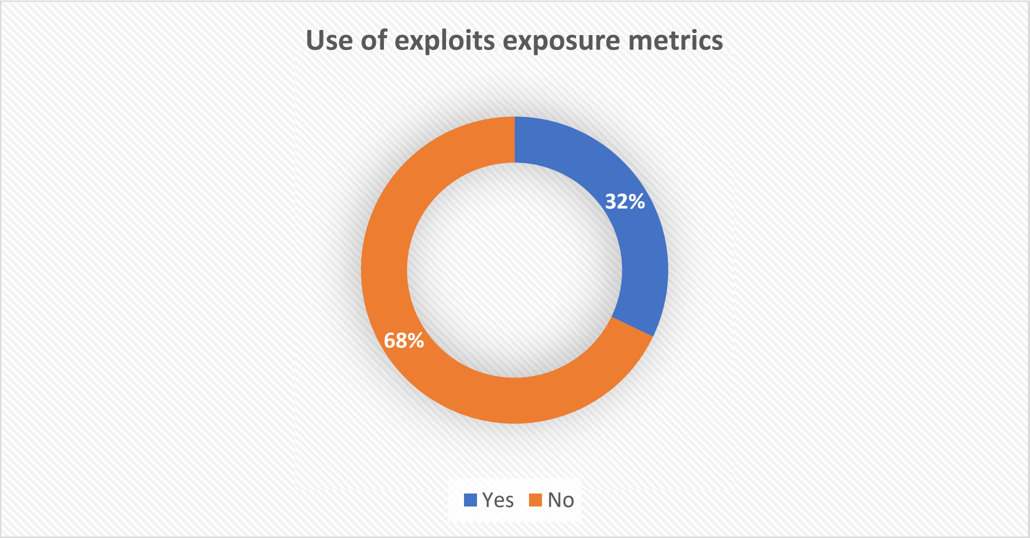
21.- NIST has a vulnerability assessment tool (URL: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator) Do you consider the method of identification and evaluation of vulnerabilities proposed by NIST to be appropriate?



22.- Do you consider it important to identify exposure to possible "exploits" when calculating vulnerabilities?



23.- Does your organization use impact metrics for Information Availability, Integrity and Confidentiality?

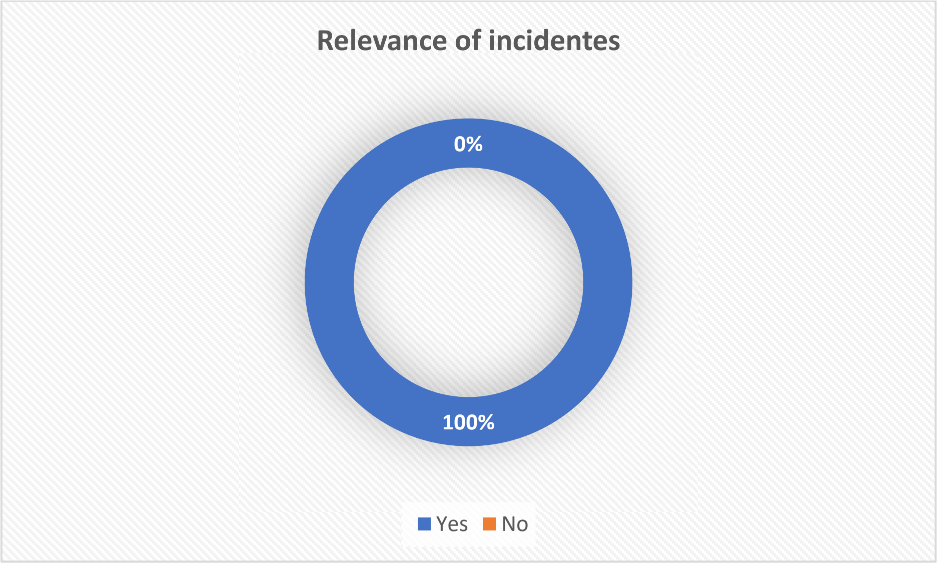


24.- What method do you use to identify and/or quantify exploits and potential vulnerabilities?

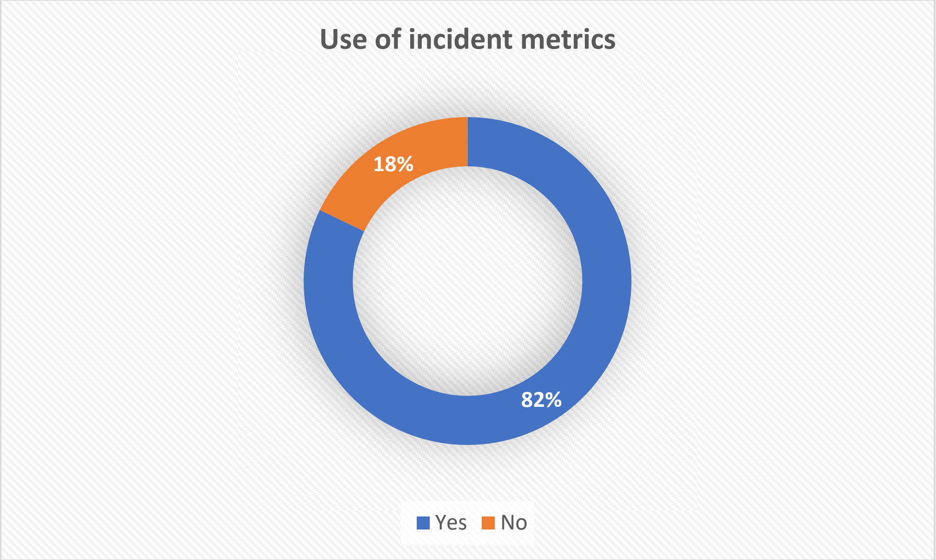
Open answer

Threat identification

25.- Do you consider it important to know the number of incidents that have been reported related to an information asset?

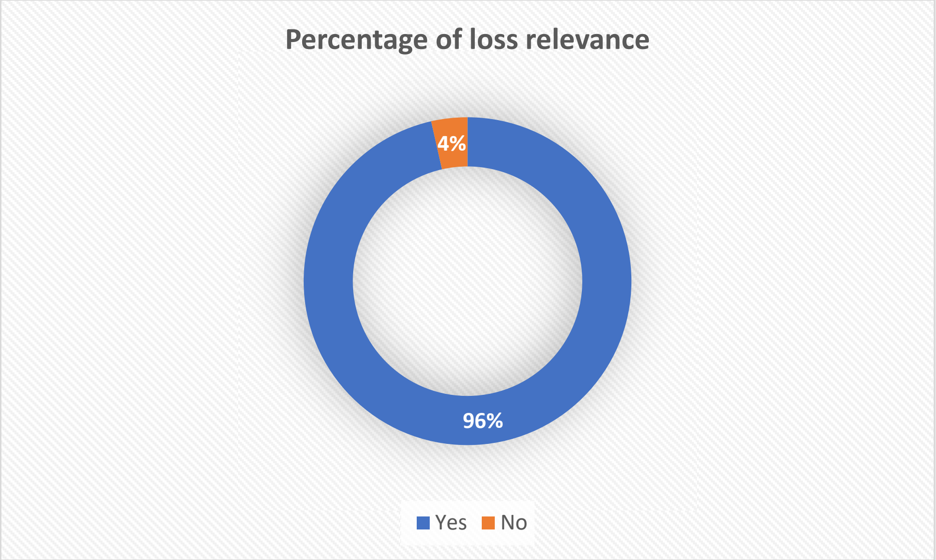


26.- Does your organization use metrics related to the number of reported incidents related to an asset?

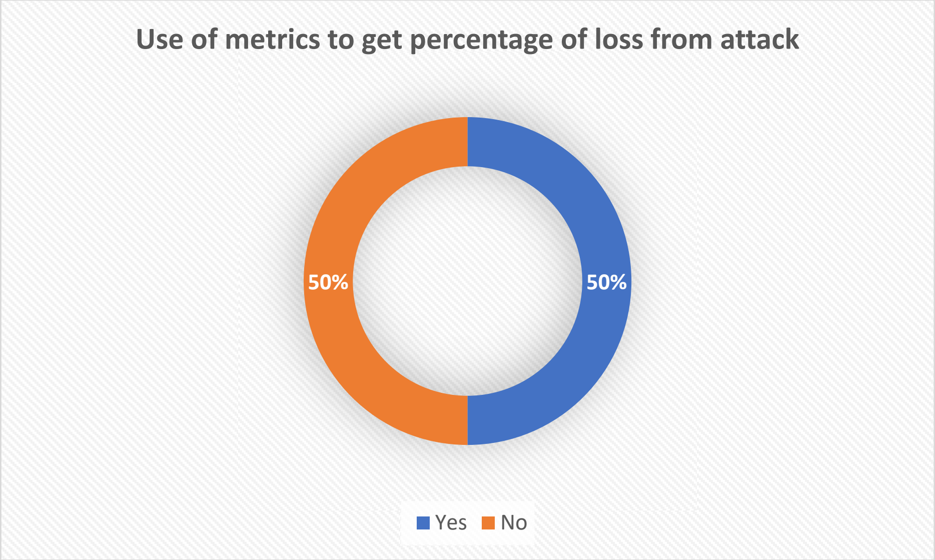


Impact

27.- Do you consider relevant the identification of percentages of loss of an asset in the event of an attack?



28.- Does your organization use any metrics to quantify the percentage of loss from a possible attack on an asset?

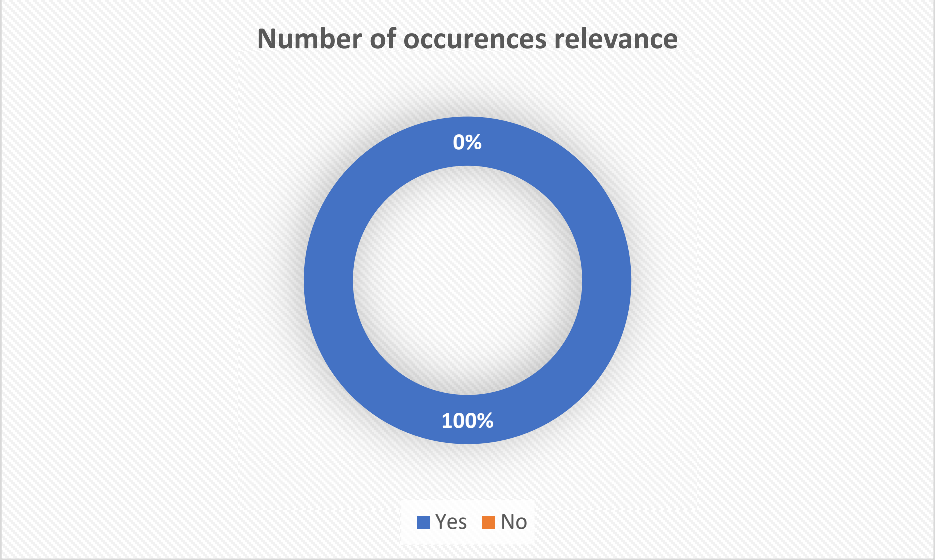


29.- What model do you use to calculate the impact of an attack?

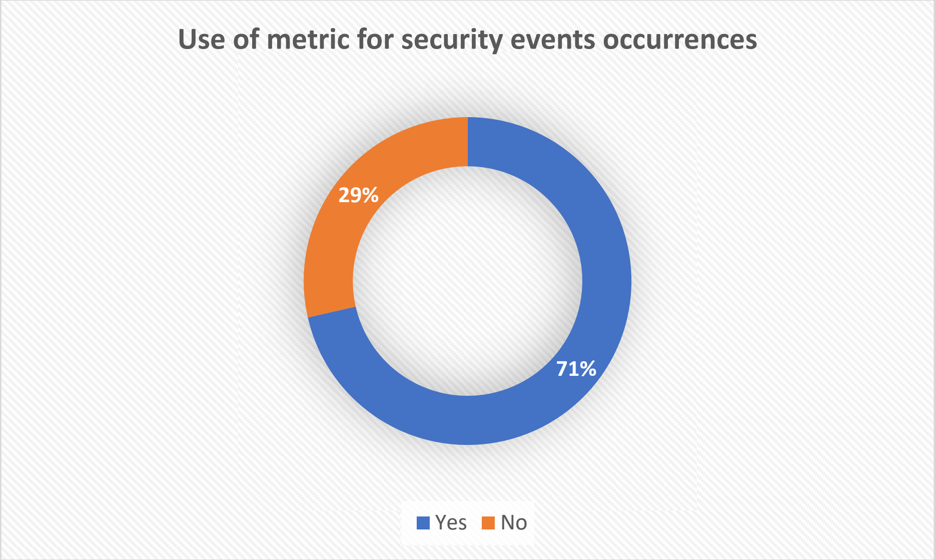
Open answer

Likelihood

30.- Do you consider it important to identify the number of occurrences of security events?



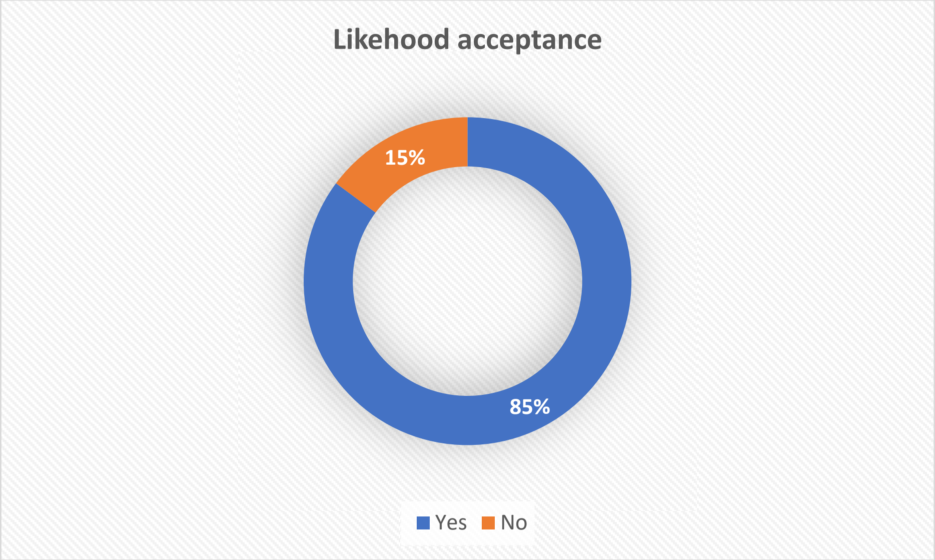
31.- Does your organization use any metrics to measure the number of occurrences of security incidents?



32.- What method do you use to calculate the risk probability?

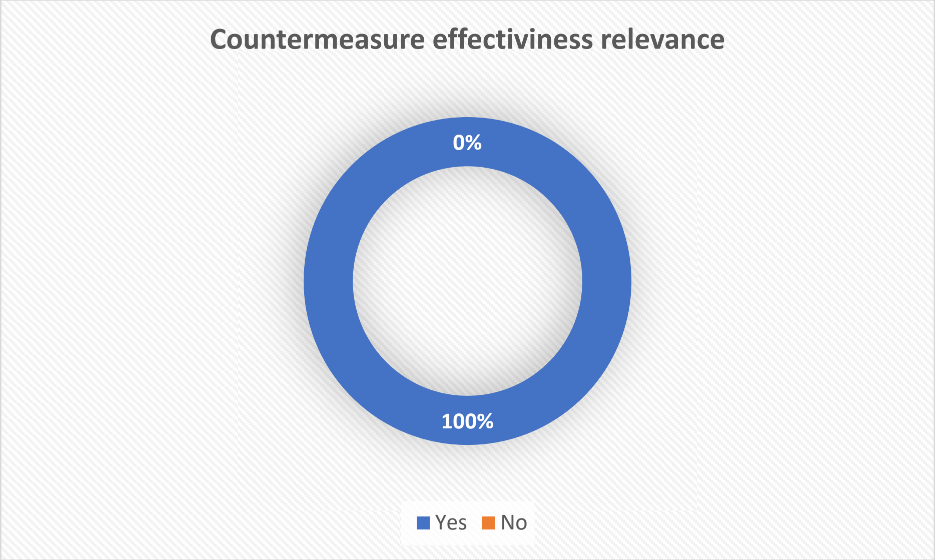
Open answer

33.- Do you consider the relationship (Number of occurrences/years recorded) adequate to measure the probability of an event?

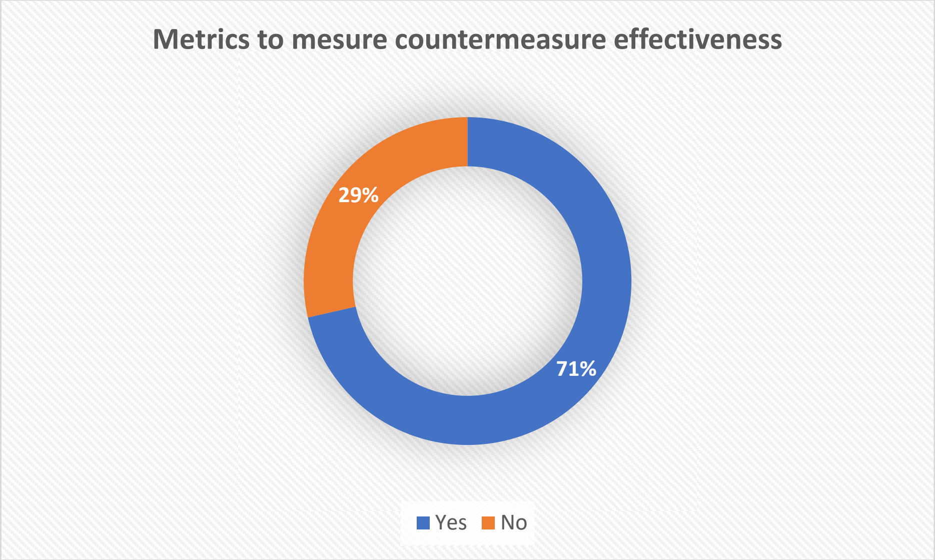


Risk reduction

34.- Do you consider it important to identify the effectiveness of a control/countermeasure?



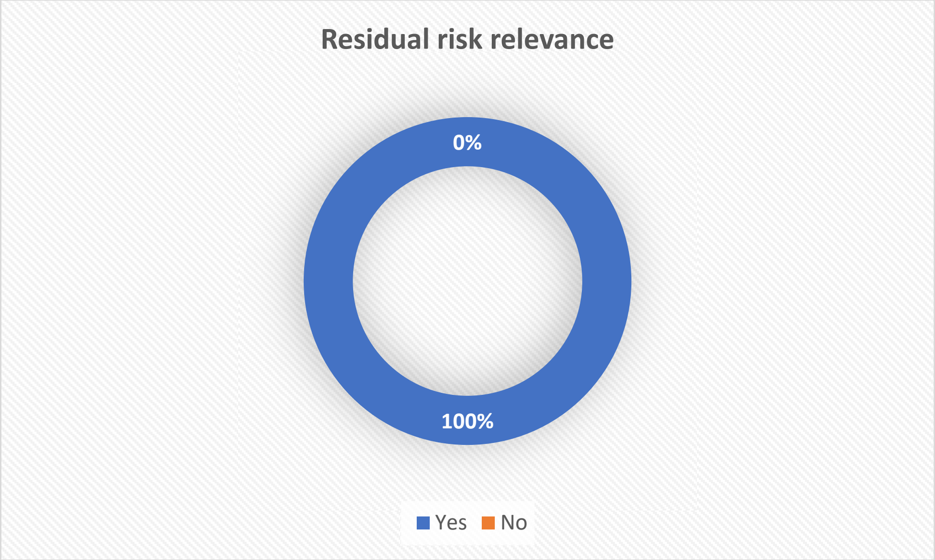
35.- Does your organization use metrics to measure the effectiveness of a control/countermeasure?



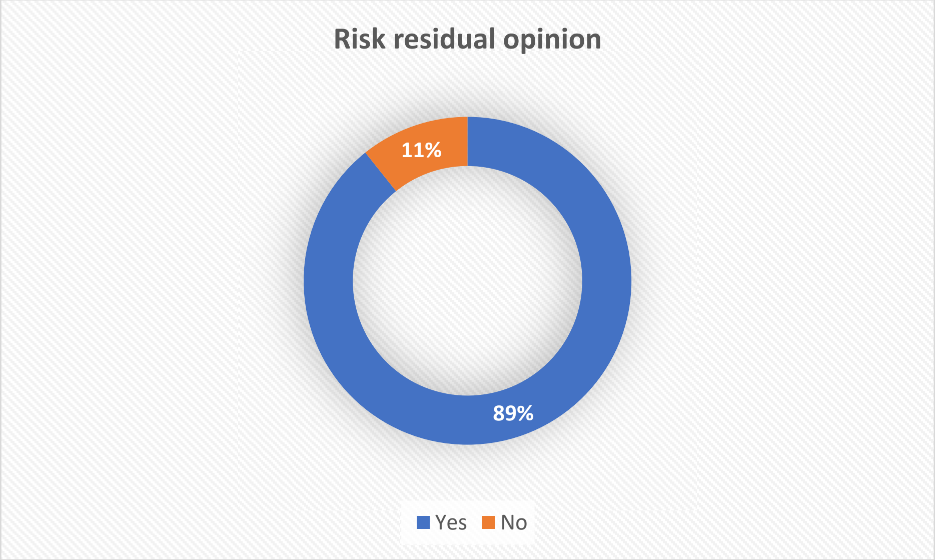
36.- What metrics do you use to measure the effectiveness of a control/countermeasure?

Open answer

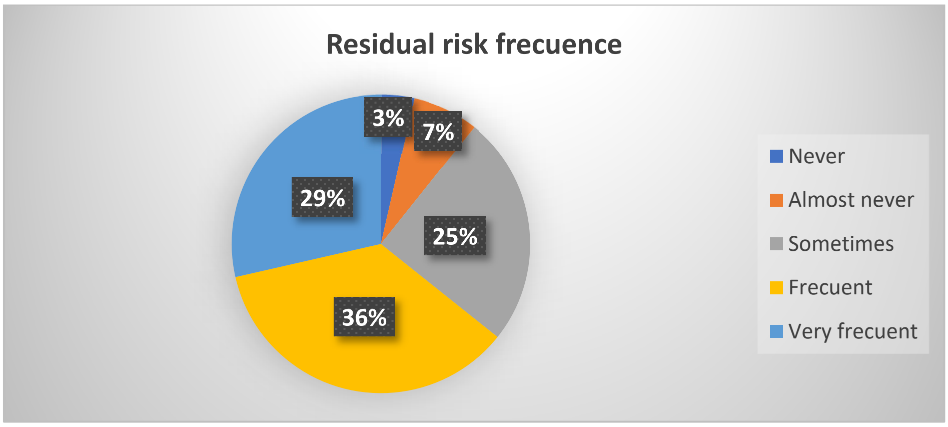
37.- Do you consider it important to calculate the residual risk after applying a control/countermeasure?



38.- Do you consider the ratio of the difference in impact before and after applying the control/countermeasure adequate to measure the effectiveness of a countermeasure?



39.- How often does your organization measure residual risk?



Section IV Evaluation of the model proposal

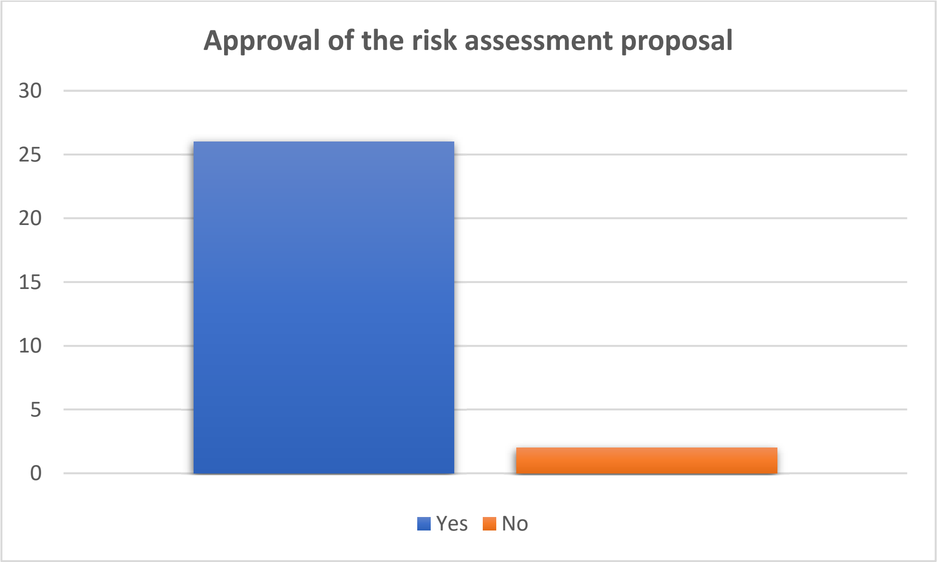
This section will ask questions about the proposed risk assessment model.

40.- Do you consider the relationships proposed for the qualitative and quantitative models adequate?

Table IV.- 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	$\mathrm{EVA} = (\mathrm{MVA} + \mathrm{VICA}\,) * \mathrm{RA}\ddot{}\mathrm{P}$
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	$RR = (R_t - R_{t-1})$



41.- If the answer is "No", indicate possible contributions

Open answer

42.- Add an open opinion of the proposal and possible recommendations

Survey link (Spanish): https://lnkd.in/diMzzZAx

Survey link (English): https://lnkd.in/dMHC3hkB