Sicurezza delle Informazioni

Sessione 2024

Agenda

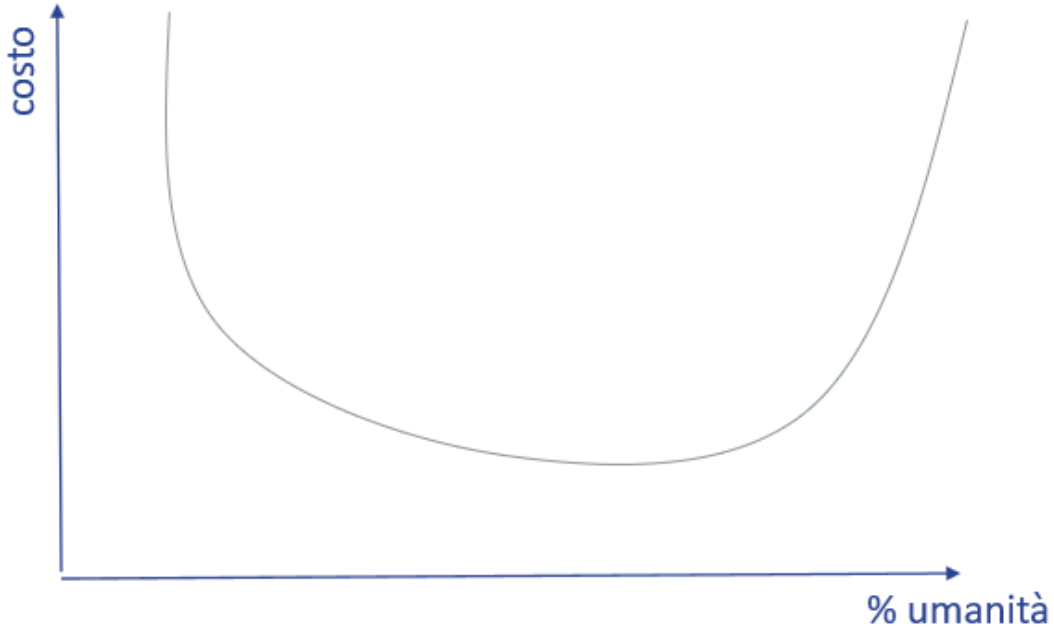
- Principi fondamentali
- La gestione del «rischio»
- Lo scenario attuale
- Standard di riferimento
- ISO 27001 requisiti e controlli
- Domande e risposte

Principi Fondamentali

- La sicurezza è un processo
- La sicurezza di una catena è pari a quella del suo anello più debole
- Non si può gestire ciò che non si può misurare
- Non è necessario essere un obiettivo per diventare una vittima

Il paradosso di Mayfield

- Costa una quantità infinita di denaro sia aprire un sistema a tutti che chiuderlo a tutti



Il Rischio

Bezos: «Amazon fallirà. Il nostro compito è far sì che accada il più tardi possibile»

Il Rischio

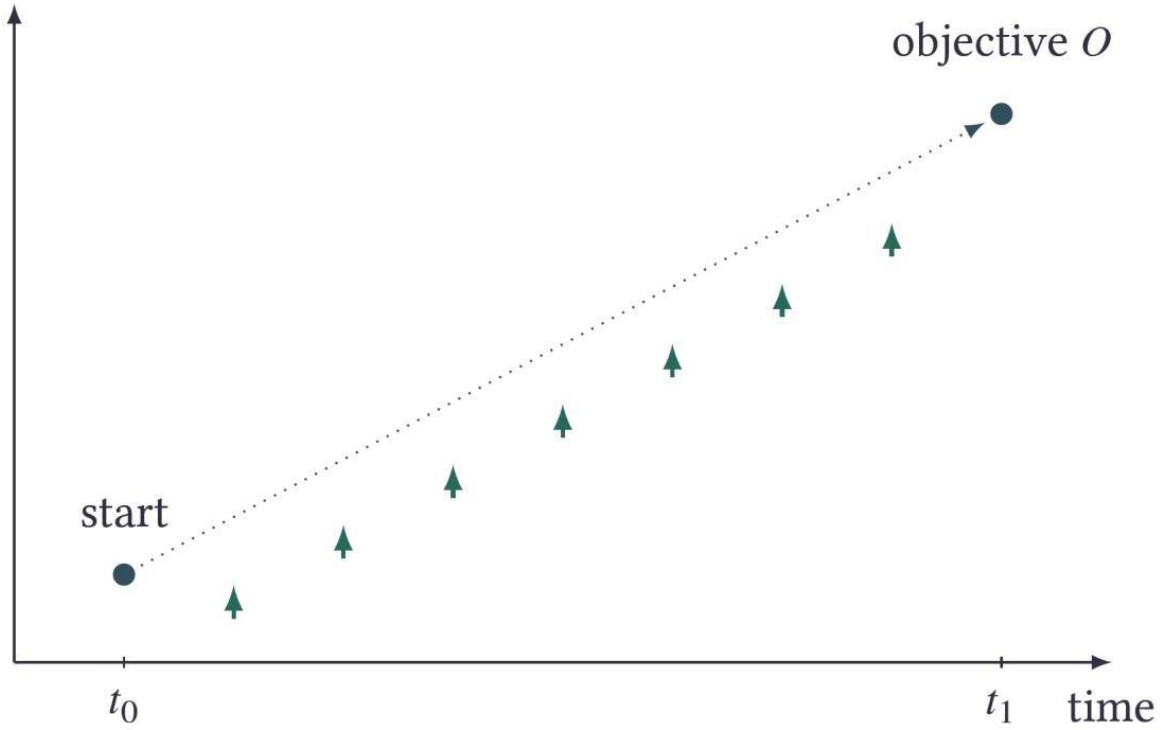
Rischio = l'**effetto** dell'**incertezza** sulla capacità di una organizzazione di raggiungere i suoi **obiettivi**

Effetto una deviazione rispetto a quanto è atteso. Può essere positiva o negativa

Incertezza Mancanza di informazione o conoscenza su un evento, le sue conseguenze o la sua probabilità

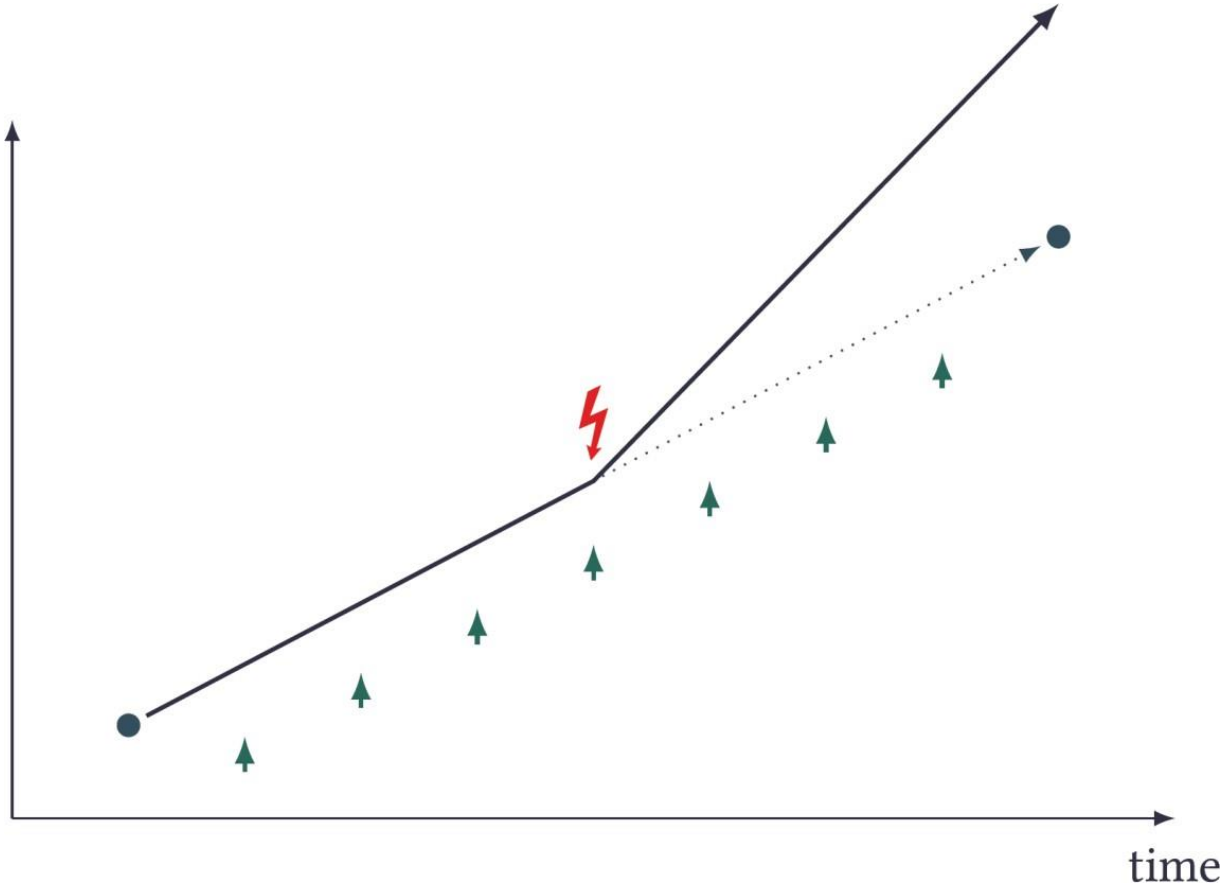
Obiettivi Gli obiettivi devono essere espliciti. Possono essere finanziari, ambientali, politici, sociali, sanitari…

Il Rischio



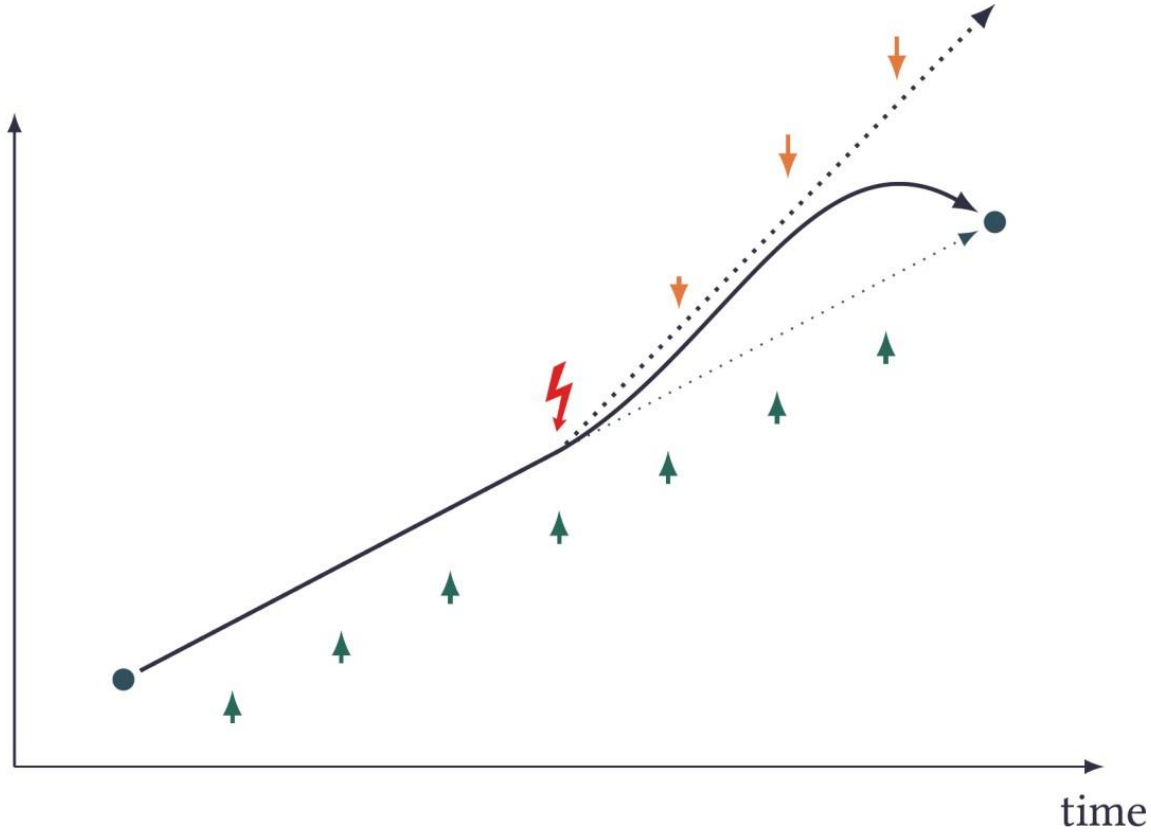
- L'organizzazione stabilisce i suoi obiettivi: al tempo t1 vuole essere nel punto O.
- Per fare questo, stabilisce un Piano d'Azione per spostarsi dalla posizione corrente fino al punto O.

Il Rischio



- La presenza di incertezza significa che delle perturbazioni inattese possono causare deviazioni dal piano definito al tempo t0.
- Se non vengono gestite l'organizzazione non raggiungerà il suo obiettivo.
- Questo è il Rischio, l'effetto dell'incertezza sulla possibilità di raggiungere gli obiettivi.

Il Rischio



Gestire il Rischio significa cercare di anticipare e far attenzione alle deviazioni dal piano e implementare opportune **misure correttive** affinché l'obiettivo sia comunque raggiunto.

Cos’è la Sicurezza?

Lo scopo della Sicurezza e’ quello di Gestire il Rischio!

Gestire il Rischio

Il Risk Management si compone di quattro fasi:

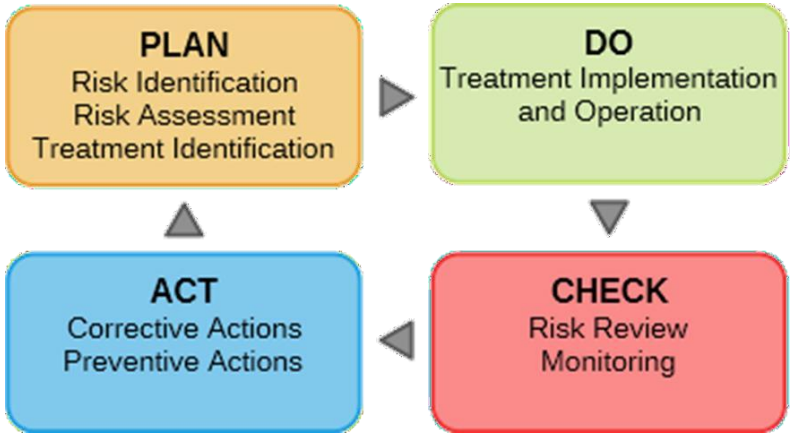
- **Identificazione** in questa fase si cerca di determinare le possibili fonti di Rischio e individuare quegli eventi che potrebbe causare l'insorgere di Pericoli

- **Valutazione qualitativa e quantitativa** consiste nel determinare impatto e probabilità di un Pericolo e nell'assegnare, in modo qualitativo o quantitativo, un ordine di priorità (o, se si preferisce, un indice di pericolosità) dei Rischi

- **Pianificazione** in questa fase si passa a identificare l'insieme delle contromisure applicabili ad un certo rischio. Si fa l'analisi costi/benefici di ognuna di esse e si passa a selezionare quelle da applicare

- **Controllo** anche dopo che sono state poste in essere le contromisure, bisogna continuare a monitorare i rischi per capire se le contromisure stanno effettivamente funzionando e valutare l'insorgere di nuovi rischi

L'output di ognuna delle 4 fasi confluisce nel Piano del Rischio (Risk Plan) complessivo.



Scenario globale

Facebook, nata nel 2006, ha più di 1 miliardo di utenti

Le aziende informatiche riescono (legalmente) a pagare un terzo in meno di tasse rispetto alle aziende non tecnologiche

Ogni minuto su Internet: 60 ore di video caricate su **Youtube**, 800.000 ricerche su **Google**, 15.000 app scaricate dal sito **Apple**, 190 milioni di mail inviate

Il conto economico della criminalità informatica (guadagno + danni) è secondo solo al mercato della droga (guadagno)

Fanno più tendenza i BLOGGER che i giornalisti

Si diventa star tramite i social (youtube, facebook)

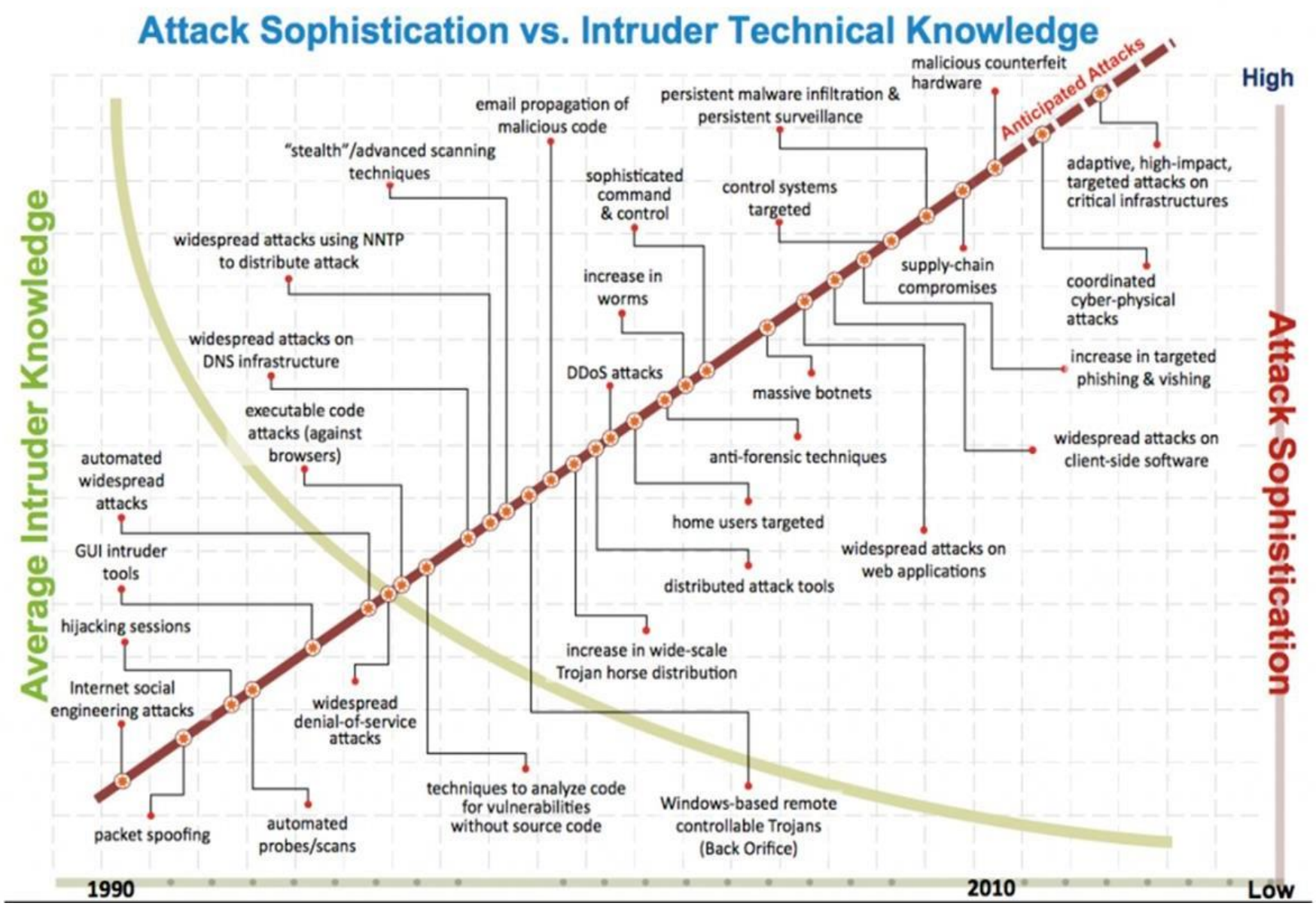
Società dell'Informazione

- Oggi l'informazione è in stragrande maggioranza in "forma digitale"
- Un'informazione in formato digitale è più economica, facile e veloce da:
  - Trasmettere — ma anche da intercettare
  - Copiare — anche se protetta da copyright
  - Modificare — ma anche da alterare
  - Eliminare — ma anche da cancellare prove
- Cambia il concetto di proprietà e di furto del bene digitale
- Si superano le barriere spazio-temporali del mondo fisico
- Cambiano modalità di accesso e fruibilità dell'informazione
- Si stravolgono i modelli economici tradizionali

Nuovi rischi

- Ogni antenna Wi-Fi
- Ogni numero di telefono
- Ogni smartphone
- Ogni computer collegato alla rete
- Ogni casella di posta elettronica
- Ogni sito di commercio elettronico
- Ogni profilo di social network (Facebook, Twitter, Linkedin)
- Ogni servizio di rete dotato di login+password

costituisce un **punto di uscita**, ma anche una **porta di ingresso** verso di noi, le nostre informazioni e la nostra identità digitale



Evoluzione attacchi

Valore dell'informazione

- Un nostro **account** (login+password) ha un valore economico perché consente a un criminale di compiere azioni mascherando la propria identità
- Un nostro **computer** ha un valore economico per:
  - Spazio disco (e occultamento materiale compromettente)
  - Mascheramento dell'origine delle azioni criminali
  - Perdita del controllo (reti di computer zombie botnet)
- Il nostro **profilo** ha un valore economico per:
  - Motivi pubblicitari e commerciali
  - Truffe mirate
  - In alcuni casi, ricatto

Sicurezza Informatica

Con il termine sicurezza informatica si intende quel ramo dell'informatica che si occupa dell'analisi delle vulnerabilità, del rischio, delle minacce o attacchi e della successiva protezione dell'integrità fisica (hardware) e logico-funzionale (software) di un sistema informatico e dei dati in esso contenuti o scambiati in una comunicazione con un utente. Tale protezione è ottenuta attraverso misure di carattere tecnico-organizzativo e funzionali tese ad assicurarne:

- l'accesso fisico e/o logico solo ad utenti autorizzati (autenticazione);
- la fruizione di tutti e soli i servizi previsti per quell'utente nei tempi e nelle modalità previste dal sistema (disponibilità);
- la correttezza dei dati (integrità);
- l'oscuramento dei dati (cifratura);
- la protezione del sistema da attacchi di software malevoli per garantire i precedenti requisiti

Standard di riferimento

ISO 31000: GESTIONE DEL RISCHIO - PRINCIPI E LINEE GUIDA
Standard che fornisce una serie completa di principi e linee guida per aiutare le organizzazioni ad eseguire l'analisi e la valutazione dei rischi.

IRAM 2 (ISF): METODOLOGIA DI SECURITY RISK ASSESSMENT
Metodologia di valutazione dei rischi mediante analisi e valutazione di minacce, vulnerabilità e impatti

ISO 27001: SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI
Standard utilizzato per arricchire il framework di controlli in ambito information security

NIST
Insieme di pubblicazioni utilizzate per arricchire il framework di controlli in ambito information security

MISURE MINIME DI SICUREZZA ICT PER LE PA
Misure per valutare e migliorare il livello di sicurezza informatica della PA, al fine di contrastare le minacce informatiche più frequenti

ISO 27001 Requisiti

Required activities: 4. Context of the organization

4.1 Understanding the organization and its context	The organization determines external and internal issues relevant to its purpose and affecting its ability to achieve the intended outcome(s) of the information security management system (ISMS).
4.2 Understanding the needs and expectations of interested parties	The organization determines interested parties relevant to the ISMS and their requirements relevant to information security.
4.3 Determining the scope of the information security management system	The organization determines the boundaries and applicability of the ISMS to establish its scope.
4.4 Information security management system	The organization establishes, implements, maintains and continually improves the ISMS.

ISO 27001 Requisiti

Required activities: 5. Leadership

5.1 Leadership and commitment	Top management demonstrates leadership and commitment with respect to the ISMS.
5.2 Policy	Top management establishes an information security policy.
5.3 Organizational roles, responsibilities and authorities	Top management ensures that responsibilities and authorities for roles relevant to information security are assigned and communicated throughout the organization.

ISO 27001 Requisiti

Required activities: 6. Planning

6.1 Actions to address risks and opportunities	When planning for the ISMS, the organization determines the risks and opportunities considering issues referred to in 4.1 and requirements referred to in 4.2. The organization defines and applies an information security risk assessment process. The organization defines and applies an information security risk treatment process.
6.2 Information security objectives and planning to achieve them	The organization establishes information security objectives and plans to achieve them at relevant functions and levels.
6.3 Planning of changes	The organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

ISO 27001 Requisiti

Required activities: 7. Support

7.1 Resources	The organization determines and provides the resources for establishing, implementing, maintaining and continually improving the ISMS.
7.2 Competence	The organization determines the competence of persons needed for information security performance, and ensures that the persons are competent.
7.3 Awareness	The persons doing work under the organization's control are made aware of the information security policy, their contribution to the effectiveness of the ISMS, benefits of improved information security performance and implications of not conforming to the requirements of the ISMS.
7.4 Communication	The organization determines the needs for internal and external communications related to the ISMS.
7.5 Documented information	The organization includes documented information in the ISMS as directly required by ISO/IEC 27001, as well as determined by the organization as being necessary for the effectiveness of the ISMS. When creating and updating documented information, the organization ensures its appropriate identification and description, format and media, and review and approval. The organization manages documented information throughout its lifecycle and makes it available where and when needed.

ISO 27001 Requisiti

Required activities: 8. Operation

8.1 Operational planning and control	The organization plans, implements and controls the processes to meet its information security requirements and to achieve its information security objectives. The organization keeps documented information as necessary to have confidence that processes are carried out as planned. The organization controls planned changes and reviews the consequences of unintended changes, and ensures that outsourced processes are identified, defined and controlled.
8.2 Information security risk assessment	The organization performs information security risk assessments and retains documented information on their results.
8.3 Information security risk treatment	The organization implements the information security risk treatment plan and retains documented information on the results of the information security treatment.

ISO 27001 Requisiti

Required activities: 9. Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation	The organization evaluates the information security performance and the effectiveness of the ISMS.
9.2 Internal audit	The organization conducts internal audits to provide information on conformity of the ISMS to the requirements.
9.3 Management review	Top management reviews the ISMS at planned intervals.

ISO 27001 Requisiti

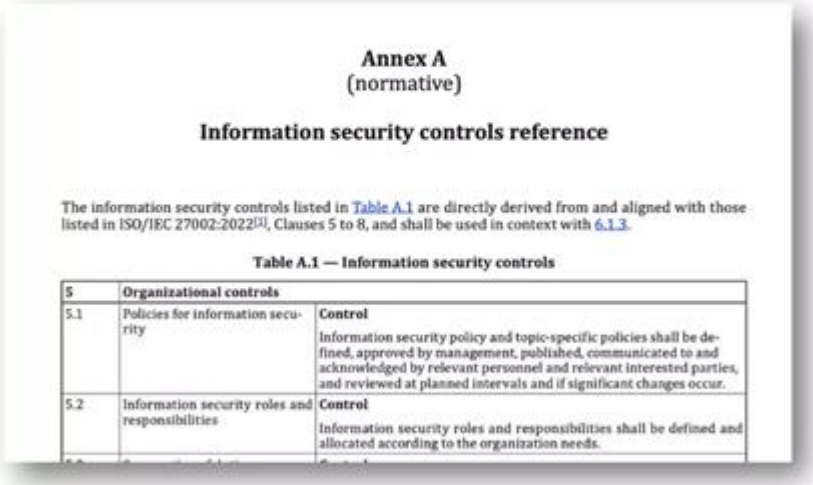
Required activities: 10. Improvement

10.1 Continual improvement	The organization continually improves the suitability, adequacy and effectiveness of the ISMS.
10.2 Nonconformity and corrective action	The organization reacts to nonconformities, evaluates them and takes corrections as well as corrective actions if needed.

ISO 27001 Controlli

Annex A. Information Security Controls

Control: measure that maintains and/or modifies risk



Annex A
(normative)

Information security controls reference

The information security controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2022[1], Clauses 5 to 8, and shall be used in context with 6.1.3.

Table A.1 — Information security controls

5	Organizational controls	
5.1	Policies for information security	**Control** Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.
5.2	Information security roles and responsibilities	**Control** Information security roles and responsibilities shall be defined and allocated according to the organization needs.

Total number of controls – 93, 11 new (2022)

Controls are categorized as:

a) **People**, if they concern individual people
b) **Physical**, if they concern physical objects
c) **Technological**, if they concern technology
d) otherwise they are categorized as **Organizational**

Five attributes only in ISO 27002:2022 (#):

1. Control type (Preventive, Detective, Corrective)
2. Information security properties (CIA)
3. Cybersecurity concepts
   (Identify, Protect, Detect, Respond and Recover)
4. Operational capabilities
5. Security domains

ISO 27001 Controlli

5. Organizational controls	6. People controls	8. Technological controls
5.1. Policies for information security	6.1. Screening	8.1. User endpoint devices
5.2. Information security roles and responsibilities	6.2. Terms and conditions of employment	8.2. Privileged access rights
5.3. Segregation of duties	6.3. Information security awareness, education and training	8.3. Information access restriction
5.4. Management responsibilities	6.4. Disciplinary process	8.4. Access to source code
5.5. Contact with authorities	6.5. Responsibilities after termination or change of employment	8.5. Secure authentication
5.6. Contact with special interest groups	6.6. Confidentiality or non-disclosure agreements	8.6. Capacity management
5.7. Threat intelligence	6.7. Remote working	8.7. Protection against malware
5.8. Information security in project management	6.8. Information security event reporting	8.8. Management of technical vulnerabilities
5.9. Inventory of information and other associated assets		8.9. Configuration management
5.10. Acceptable use of information and other associated assets	**7. Physical controls**	8.10. Information deletion
5.11. Return of assets	7.1. Physical security perimeter	8.11. Data masking
5.12. Classification of information	7.2. Physical entry	8.12. Data leakage prevention
5.13. Labelling of information	7.3. Securing offices, rooms and facilities	8.13. Information backup
5.14. Information transfer	7.4. Physical security monitoring	8.14. Redundancy of information processing facilities
5.15. Access control	7.5. Protecting against physical and environmental threats	8.15. Logging
5.16. Identity management	7.6. Working in secure areas	8.16. Monitoring activities
5.17. Authentication information	7.7. Clear desk and clear screen	8.17. Clock synchronization
5.18. Access rights	7.8. Equipment siting and protection	8.18. Use of privileged utility programs
5.19. Information security in supplier relationships	7.9. Security of assets off-premises	8.19. Installation of software on operational systems
5.20. Addressing information security within supplier agreements	7.10. Storage media	8.20. Network security
5.21. Managing information security in the ICT supply chain	7.11. Supporting utilities	8.21. Security of network services
5.22. Monitoring, review and change management of supplier services	7.12. Cabling security	8.22. Segregation of networks
5.23. Information security for use of cloud services	7.13. Equipment maintenance	8.23. Web filtering
5.24. Information security incident management planning and preparation	7.14. Secure disposal or re-use of equipment	8.24. Use of cryptography
5.25. Assessment and decision on information security events		8.25. Secure development life cycle
5.26. Response to information security incidents		8.26. Application security requirements
5.27. Learning from information security incidents		8.27. Secure system architecture and engineering principles
5.28. Collection of evidence		8.28. Secure coding
5.29. Information security during disruption		8.29. Security testing in development and acceptance
5.30. ICT readiness for business continuity		8.30. Outsourced development
5.31. Legal, statutory, regulatory and contractual requirements		8.31. Separation of development, test and production environments
5.32. Intellectual property rights		8.32. Change management
5.33. Protection of records		8.33. Test information
5.34. Privacy and protection of PII		8.34. Protection of information systems during audit testing
5.35. Independent review of information security		
5.36. Compliance with policies, rules and standards for information security		
5.37. Documented operating procedures		

*New control, 2022


MICE
TECNOLOGY ADVISORY