UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CORSO DI PERFEZIONAMENTO IN
«SECURITY MANAGER»
CORSO DI FORMAZIONE IN
«PROFESSIONISTA DELLA SECURITY»

Luisa Franchina

Enterprise risk management

1

Indice

- Evoluzione normative
- Infrastrutture critiche
- Architettura Nazionale Cyber
- Direttiva NIS
- Perimetro di sicurezza nazionale cibernetica
- Il golden power e il 5G
- Direttiva NIS 2 e CER
- Regolamento UE 2019/452 - cybersecurity act
- Certificazioniù
- Framework Nazionale

2

2

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Il trucco

$$R = f (M ; V ; I)$$

La valutazione del rischio si basa su due dimensioni

PROBABILITA' DI ACCADIMENTO

IMPATTO

$$P = f (M ; V)$$

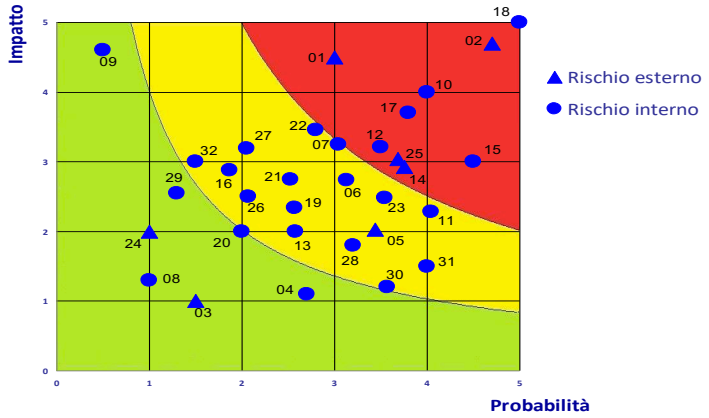
3

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

La valutazione del rischio «classica»

Esempio

Livello di rischio	Score
ALTO	$\beta \leq$ score $\leq \gamma$
MEDIO	$\alpha \leq$ score $< \beta$
BASSO	score $< \alpha$



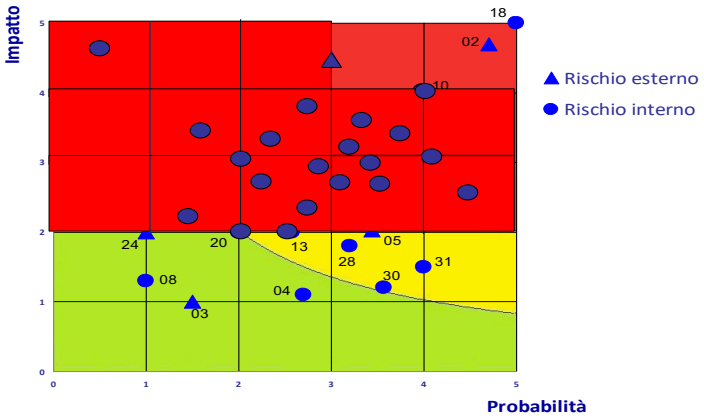
4

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

La valutazione dell'impatto

Esempio

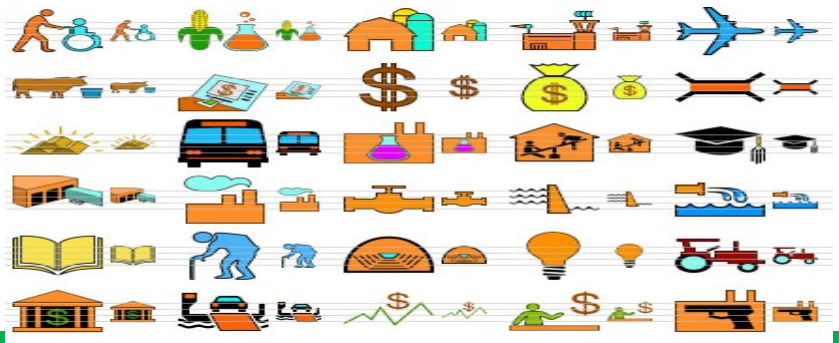
Livello di rischio	Score
ALTO	β ≤ score ≤ γ
MEDIO	α ≤ score < β
BASSO	score < α



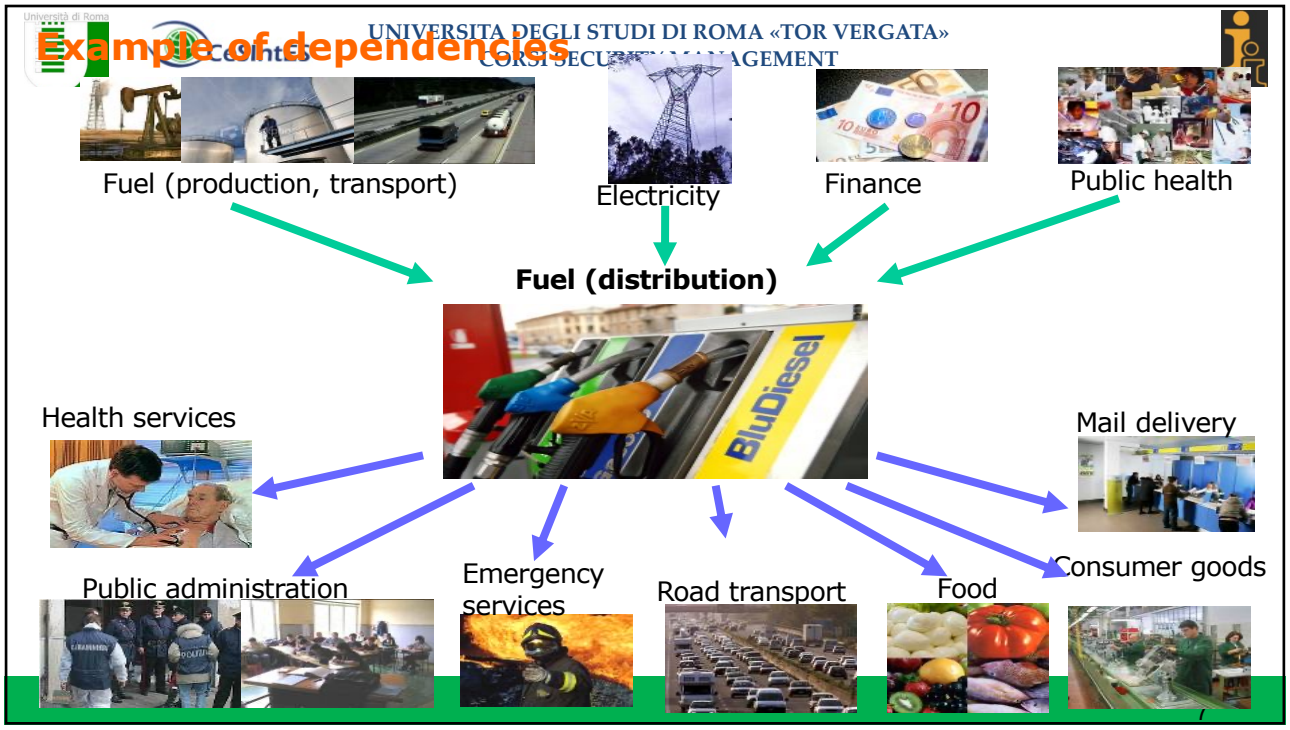
5

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

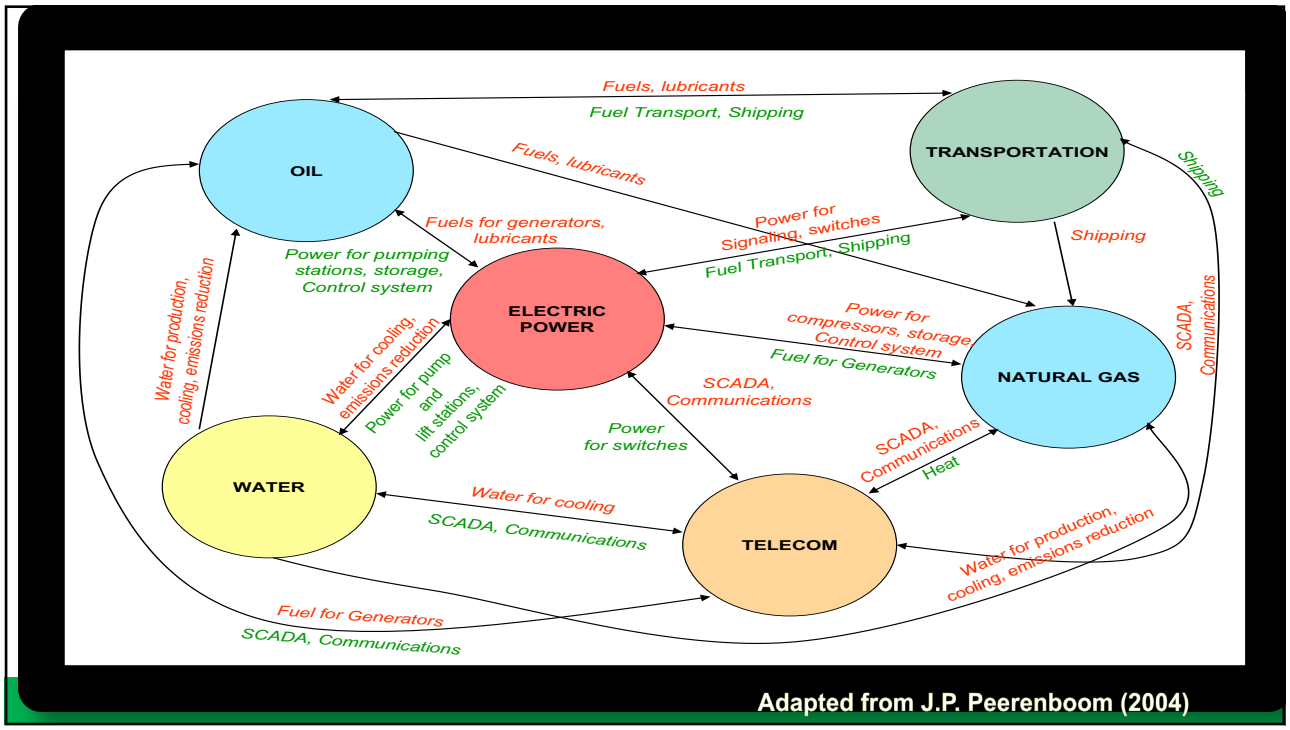
Le interdipendenze nelle IC



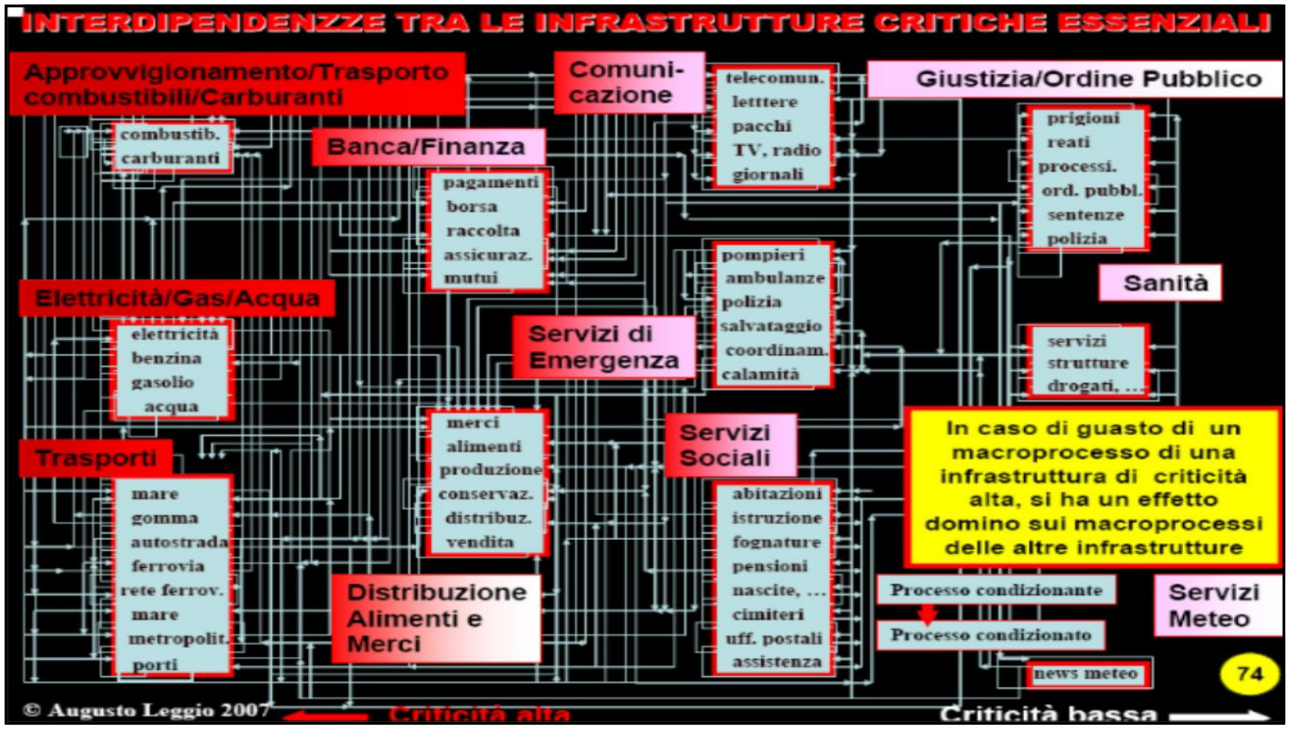
6


Example of dependencies
UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
Fuel (production, transport)
Electricity
Finance
Public health
Fuel (distribution)
BluDiesel
Health services
Mail delivery
Public administration
Emergency services
Road transport
Food
Consumer goods

7


OIL
TRANSPORTATION
ELECTRIC POWER
NATURAL GAS
WATER
TELECOM
Fuels, lubricants
Fuel Transport, Shipping
Fuels, lubricants
Fuels for generators, lubricants
Power for pumping stations, storage, Control system
Power for Signaling, switches
Fuel Transport, Shipping
Shipping
Shipping
Water for production, cooling, emissions reduction
Water for cooling, emissions reduction
Power for pump and lift stations, control system
Power for compressors, storage, Control system
Fuel for Generators
SCADA, Communications
SCADA, Communications
Power for switches
SCADA, Communications
Heat
Water for cooling
SCADA, Communications
Water for production, cooling, emissions reduction
Fuel for Generators
SCADA, Communications
Adapted from J.P. Peerenboom (2004)

8



9

Metriche dell'impatto

- Vittime
- Impatti economici
- Sicurezza economica
- Sofferenza fisica
- Perturbazione della vita quotidiana
- Fiducia nelle istituzioni
- Salute pubblica
- Sicurezza pubblica
- Impatti psicologici
- Sicurezza dello Stato
- Difesa della Nazione
- Violazione del territorio
- Panico
- Perturbazione della democrazia
- Impatto sull'ordine sociale
- Impatto geopolitico
- Impatto ambientale
- Impatto sociopolitico
- Effetti negativi sui marchi e aziende nazionali
- NGH…

Soglie di Tolleranza

10

Metriche dell'impatto

ERM COSO

Danni economici (lucro cessante danno emergente)
Reputazionale
Vantaggio competitivo
Mercato

Soglie di Propensione e Tolleranza

11

12

	EU	G8	USA	RUS	UK	NL	FR	GER	SWE	JP	AUS	CAN	TRK	IN	CH
ICT and MEDIA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
WATER, DAMS, SURFACE WATER MNGT	✓		✓	✓	✓	✓	✓			✓	✓	✓	✓		✓
ENERGY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
NUCLEAR (radiological hazard), HAZARDOUS MATERIALS	✓		✓			✓	✓	✓		✓		✓			
FOOD	✓		✓		✓	✓					✓	✓			✓
AGRICULTURE			✓	✓							✓	✓			
HEALTH, MEDICAL SERVICES	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓			✓
FINANCE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
TRANSPORT, POSTAL, PIPELINES and LOGISTIC	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
CHEMICHAL INDUSTRY and BIOTECH	✓		✓			✓	✓					✓	✓		✓
SPACE	✓													✓	
MONUMENTS ICONS			✓								✓	✓			✓
GOVERNMENT ADM		✓	✓	✓	✓	✓		✓		✓		✓			✓
DEFENSE INDUSTRY BASE, DEFENSE			✓	✓							✓	✓	✓	✓	✓
COMMERCIAL FACILITIES			✓												
EMERGENCY SERVICES		✓	✓		✓						✓	✓			✓
CRITICAL MANUFACTURING			✓										✓		
VERY LARGE INFORMATION SYS				✓											
UTILITY INCLUDING WARMING SYSTEMS				✓											
INDUSTRY				✓											
MUNICIPAL SERVICES				✓					✓						
CIVIL DEFENSE				✓											✓
LEGAL ORDER, PUBLIC SAFETY						✓	✓							✓	
PROTECTION & SAFETY									✓			✓			✓
SERVICES, OTHER								✓							
RETAIL, PROVISIONS									✓						

13

14

Le infrastrutture critiche 1/3

Il **D. Lgs. 11 aprile 2011 n. 61** (recepimento della **Direttiva 2008/114/CE**) definisce :

Infrastruttura: un elemento, un sistema o parte di questo, che contribuisce al mantenimento delle funzioni della società, della salute, della sicurezza e del benessere economico e sociale della popolazione;

Infrastruttura Critica (IC): Infrastruttura, ubicata in uno Stato membro dell'Unione europea, che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale della popolazione ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in quello Stato, a causa dell'impossibilità di mantenere tali funzioni.

Infrastruttura Critica Europea (ICE): Infrastruttura critica ubicata negli Stati membri dell'UE la cui perturbazione o distruzione avrebbe un significativo impatto su almeno **due Stati membri dell'UE**. La rilevanza dell'impatto è valutata in termini intersettoriali. Sono compresi gli effetti derivanti da dipendenze intersettoriali in relazione ad altri tipi di infrastrutture.

https://www.gazzettaufficiale.it/eli/id/2011/05/04/011G0101/sg

15

15

Leggi in vigore e istituzioni attive nella PA - 2

Direttiva 114/08CE e DECRETO LEGISLATIVO 11 aprile 2011 , n. 61 Attuazione della Direttiva 2008/114/CE recante **l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione**. (GU n. 102 del 4-5-2011)

*Il Decreto legislativo istituisce **presso la PCM la struttura responsabile** che effettua le istruttorie tecnico-scientifiche per la individuazione delle possibili ICE e attribuisce al **NISP** (Nucleo Interministeriale di situazione e pianificazione, istituito con DPCM 5 maggio 2010, GU* n. 139 del 17 giugno 2010*) la facoltà di designarle su impulso della struttura responsabile.*

Attualmente la struttura responsabile è nell'Ufficio del Consigliere Militare del PCM.
*I settori previsti dalla direttiva e dal DLgsv sono **energia e trasporti**.*
Gli obblighi previsti per gli eventuali operatori di ICE sono: identificazione di un responsabile e redazione di un piano operativo di sicurezza.
Non ci sono ICE designate in Italia ad oggi.

16

Fare clic per modificare lo stile del titolo

"Infrastruttura Critica Europea": infrastruttura critica ubicata negli Stati membri dell'UE la cui perturbazione o distruzione avrebbe un significativo impatto su almeno **due Stati membri dell'UE**. La rilevanza dell'impatto è valutata in termini intersettoriali. Sono compresi gli effetti derivanti da dipendenze intersettoriali in relazione ad altri tipi di infrastrutture.

I four

Brussels, 28.8.2013
SWD(2013) 318 final

EUROCONTROL is designated as the EU Air Traffic Management (ATM) Network Manager, managing the flow of approximately 30 000 flights per day. The objective, tasks and functions of the Network Manager are regulated by the Commission Regulation (EU) No 677/2011 of 7 July 2011 laying down detailed rules for the implementation of ATM network functions.

GALILEO is the European programme for a global satellite navigation system, which is partly owned by the EU and will provide services of vital importance for our citizens and economy.

The **Electricity Transmission Grid** and the **European Gas Transmission Network** are networks without national boundaries, which mean that a failure of one portion of the network

17

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Le infrastrutture critiche nazionali

Il D.L. n. 34 del 19 maggio 2020 convertito con **Legge n. 77 del 17 luglio 2020** fa rientrare nelle IC :

1. le società che gestiscono **infrastrutture individuate con i decreti emanati dai Ministeri di riferimento**;
2. le **società individuate in funzione dell'emergenza sanitaria**;
3. gli **OSE** e i **Fornitori di Servizi Digitali** (NIS);
4. le società e gli enti che gestiscono od ospitano i **sistemi spaziali per la difesa dell'Unione europea e nazionale**;
5. ogni altra società che gestisce **infrastrutture o beni che sono dichiarati critici con DPCM**.

https://www.gazzettaufficiale.it/eli/id/2020/05/19/20G00052/sg

18

19

Leggi in vigore e istituzioni attive nella PA - 1

- LEGGE 18 marzo **2008, n. 48** Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalita' informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno. (GU n. 80 del 4-4-2008 - Suppl. Ordinario n. 79)

  Definisce i crimini informatici. Nessuna istituzione in particolare

- D.L. 27-7-2005 n. 144 Misure urgenti per il contrasto del terrorismo internazionale. Pubblicato nella Gazz. Uff. 27 luglio 2005, n. 173 e convertito in legge, con modificazioni, dall'art. 1, L. 31 luglio 2005, n. 155 (Gazz. Uff. 1° agosto 2005, n. 177).

- Decreto 9 gennaio 2008 del Ministero dell'interno "**Individuazione delle infrastrutture critiche informatiche di interesse nazionale**", G.U. 30 aprile 2008, n. 101

  *Istituisce il **CNAIPIC** (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche) all'interno della Polizia delle Comunicazioni. **Si occupa solo di prevenzione e repressione del crimine informatico.***

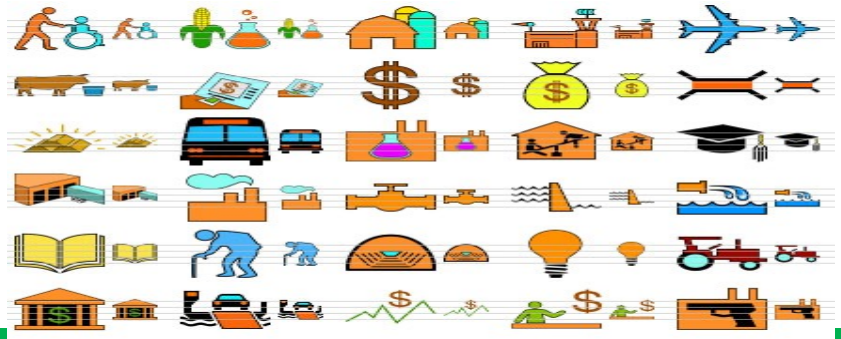
  Il DM identifica alcune infrastrutture critiche informatizzate **Non ci sono obblighi per tali operatori***

* Ministeri, agenzie ed enti da essi vigilati; operanti nei settori dei rapporti internazionali, della sicurezza, della giustizia, della difesa, della finanza, delle comunicazioni, dei trasporti, dell'energia, dell'ambiente, della salute;
Banca d'Italia ed autorità indipendenti;
Società partecipate dallo Stato, dalle regioni e dai comuni interessanti aree metropolitane non inferiori a 500.000 abitanti, operanti nei settori delle comunicazioni, dei trasporti, dell'energia, della salute e delle acque;
Ogni altra istituzione, amministrazione, ente, persona giuridica pubblica o privata la cui attività, per ragioni di tutela dell'ordine e della sicurezza pubblica, sia riconosciuta di interesse nazionale dal Ministro dell'interno, anche su proposta dei prefetti - autorità provinciali di pubblica sicurezza.

20

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

La reazione istituzionale



21

HB

Architettura Nazionale Cyber

22

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Architettura Nazionale

DPCM 24 gennaio 2013
Ruolo del CISR
Quadro strategico nazionale (dic. 2013) e Piano nazionale per la protezione cibernetica (dic. 2013).

DPCM 27 febbraio 2017
L'NSC (Nucleo per la sicurezza cibernetica), precedentemente sotto il controllo dell'Ufficio del Consigliere militare di Palazzo Chigi, viene incluso nel DIS
Secondo piano nazionale per la protezione cibernetica (marzo 2017)

https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-17-febbraio-2017.html

23

24

NIS: Directive on Network and Information Security 2016/1148

- Definizione misure necessarie per ottenere un **elevato livello di sicurezza delle reti**
- Designazione **CSIRT nazionali**
- Adozione **misure di sicurezza, gestione dei rischi**
- **Notifica degli incidenti** da parte degli Operatori dei Servizi Essenziali

Recepimento:

DLGS 18 Maggio 2018 n.65

L'operatore di servizi essenziale (OSE) è un soggetto pubblico o privato:
- Un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali
- La fornitura di tale servizio dipende dalla rete e dai sistemi informativi
- Un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

SCHEMA FLUSSO INFORMATIVO NIS

25

L'applicazione del panorama completo…

Si ottiene dal combinato disposto tra NIS e direttiva 2009/140/CE

26

Operatori dei Servizi Essenziali (OSE)

I **settori** in cui operano gli **Operatori dei Servizi Essenziali** (**OSE**) sono definiti dalla Direttiva NIS e ripresi dal D.Lgs. 18 maggio 2018, n. 65:

Settore **Energetico** e sottosettori:
- energia elettrica;
- gas;
- petrolio

Settore **Trasporti** e sottosettori:
- trasporto aereo;
- trasporto ferroviario;
- trasporto per vie d'acqua;
- trasporto su strada

Settore **Bancario**

Settore **Infrastrutture dei mercati finanziari**

Settore **Sanitario**

Settore **Forniture e distribuzione di acqua potabile**

27

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Fornitori di Servizi Digitali (FSD)

I **Fornitori di Servizi Essenziali (FSD)** sono persone giuridiche che forniscono servizi di:

E-COMMERCE

MOTORI DI RICERCA

CLOUD COMPUTING

28

Direttiva NIS: Autorità nazionali competenti

Sono stati identificati cinque Ministeri quali "**Autorità competenti NIS**":

Autorità competenti NIS	Ambito di competenza
Ministero dello sviluppo economico	Settore dell'energia – Sottosettori energia elettrica, gas e petrolio
	Settore delle infrastrutture digitali
	Servizi digitali
Ministero delle infrastrutture e dei trasporti	Settore dei trasporti – Sottosettori trasporto aereo, trasporto ferroviario, trasporto per vie d'acqua e trasporto su strada
Ministero dell'economia e delle finanze in collaborazione con Banca d'Italia e Consob	Settore bancario
	Settore delle infrastrutture dei mercati finanziari
Ministero della salute, Regioni e Province autonome di Trento e di Bolzano (direttamente o per il tramite delle Autorità sanitarie territorialmente competenti)	Settore sanitario
Ministero dell'ambiente e della tutela del territorio e del mare, Regioni e Province autonome di Trento e di Bolzano (direttamente o per il tramite delle Autorità territorialmente competenti)	Settore della fornitura e distribuzione di acqua potabile

PUNTO DI CONTATTO UNICO NIS

Il **Dipartimento delle informazioni per la sicurezza (DIS)** è designato quale **Punto di Contatto Unico** verso l'Unione europea e di coordinamento con le autorità competenti in materia di cybersecurity negli altri Stati membri

https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/06/La-NIS-in-pillole.pdf

29

Perimetro di Sicurezza Nazionale Cibernetica

30

Il Perimetro di Sicurezza Nazionale Cibernetica

- È composto da attori pubblici e privati che esercitano funzioni essenziali per gli interessi dello Stato
- L'esercizio di tale funzione o del servizio dipende da reti, sistemi informativi e servizi informatici.

Legge 18 Novembre 2019 n.133 che ha convertito il decreto-legge n. 105 del 2019

CVCN

Viene istituito il **Centro di Valutazione e Certificazione Nazionale (CVCN)** con il compito di elaborare e adottare schemi di certificazione cibernetica tenendo conto di standard europei e internazionali e compiere verifiche preliminari di sicurezza e nelle fasi di procurement ICT.

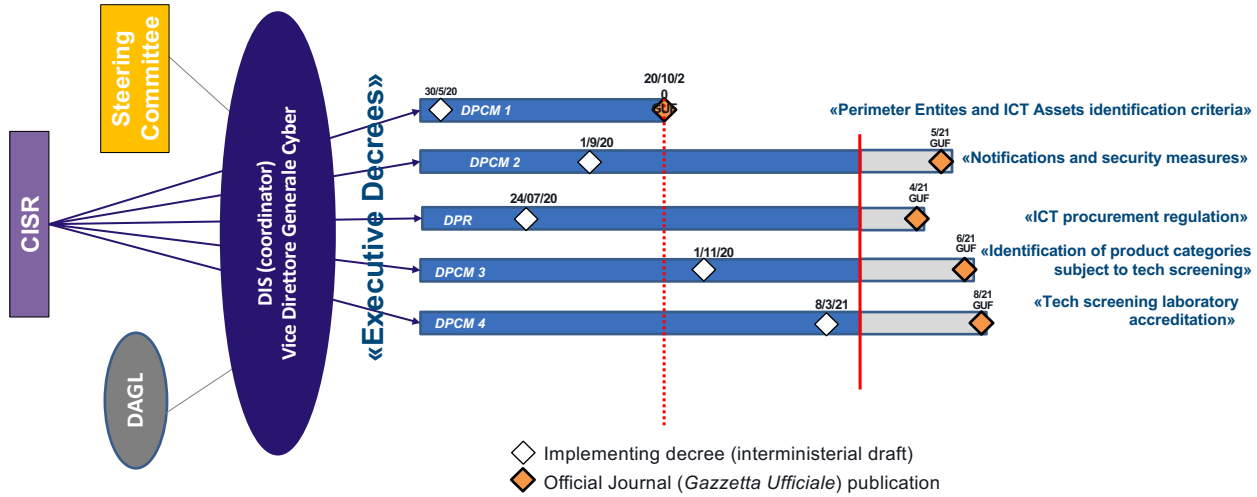
I soggetti afferenti al Perimetro:
- Trasmettono elenchi dei propri beni ICT
- Segnalano gli attacchi in tempo reale

il DL 105/2019 convertito con legge del 18 novembre 2019 n.133
relazione sulla politica dell'informazione per la sicurezza 2019

31

31

PSNC: Implementation status



32

DPCM del 30 Luglio 2020 n.131

DPCM del 30 Luglio 2020 n.131
attuativo Legge 18 Novembre 2019 n.133

- Estrinseca il concetto di sicurezza nazionale:
  - Disponibilità, integrità e confidenzialità dei dati
  - **Continuità dei servizi** identificati
- Definisce le **modalità e i criteri** di individuazione dei soggetti, pubblici e privati, inclusi nel perimetro di sicurezza nazionale cibernetica
- Definisce i criteri con cui tali soggetti predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza.
- Definisce le modalità di trasmissione degli elenchi.

33

DPCM 30 luglio 2020 n. 131 2/2

Sono inclusi nel Perimetro:

- i **soggetti che operano nel settore governativo con riferimento alle attività delle amministrazioni CISR**;
- ulteriori **soggetti**, pubblici e privati, **coinvolti nei seguenti settori**:
  - interno;
  - difesa;
  - spazio e aerospazio;
  - energia;
  - telecomunicazioni;
  - economia e finanza;
  - trasporti;
  - servizi digitali;
  - tecnologie critiche;
  - enti previdenziali/lavoro.

34

Schema DPR Attuazione Art. 1, C. 6, D.L. 105/2019

Il 29 Gennaio 2021, dopo il parere del Consiglio di Stato, il consiglio dei ministri, ha approvato, in esame definitivo, il **regolamento, da adottarsi mediante decreto del Presidente della Repubblica**, di attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n.105, convertito con modificazioni dalla legge 18 novembre 2019, n. 133.

Il **regolamento** definisce le **procedure, le modalità e i termini** con cui il Centro di valutazione e certificazione nazionale istituito presso il Ministero dello sviluppo economico (**CVCN**) e gli altri centri di valutazione individuati dalla normativa **svolgono** i procedimenti di **verifica** e **valutazione dei beni**, **sistemi** e **servizi** di Information and Communication Technologies (ICT) che i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica intendono acquisire, nel caso in cui da questi ultimi dipenda la fornitura di servizi essenziali ovvero l'esercizio di una funzione essenziale dello Stato.

Inoltre, si **stabiliscono i criteri di natura tecnica** per l'individuazione delle **categorie**, ovvero **l'elenco di beni**, **sistemi** e **servizi ICT** a cui si applica la procedura di valutazione. Infine, si definiscono le **procedure**, le **modalità** e i termini con cui le autorità competenti effettuano le **attività** di **verifica** e ispezione ai fini dell'accertamento del rispetto degli obblighi stabiliti nel decreto-legge e nei decreti attuativi.

SCHEMA DPR: https://d110erj175o600.cloudfront.net/wp-content/uploads/2021/01/28112827/dpr.pdf
COMUNICATO http://www.governo.it/it/articolo/comunicato-stampa-del-consiglio-dei-ministri-n-95/16129

35

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Atto del Governo 240: Schema DPCM in materia di notifiche

Schema di decreto del Presidente del Consiglio dei ministri recante regolamento in **materia di notifiche degli incidenti aventi impatto su reti**, sistemi informativi e servizi informatici

Disciplina **modi e tempi delle notifiche degli incidenti** aventi impatto su reti, sistemi informativi e servizi informatici.

Nello schema sono inseriti due allegati

Allegato A- TASSONOMIE DEGLI INCIDENTI

Allegato B- MISURE DI SICUREZZA

https://www.camera.it/leg18/682?atto=240&tipoAtto=Atto&idLegislatura=18&tab=1

TESTOhttp://documenti.camera.it/apps/nuovosito/attigoverno/Schedalavori/getTesto.ashx?file=0240.pdf&leg=XVIII#pagemode=none

36

Decreti attuativi del Perimetro

PSNC

DPCM 131/2020	Criteri di individuazione soggetti inclusi nel perimetro e predisposizione elenchi ICT
DPR 54/2021	CVCN
DPCM 81/2021	Notifica degli incidenti e misure di sicurezza
DPCM 15 giugno 2021	Categorie di beni, sistemi e servizi ICT soggetti a valutazione CVCN
NON PUBBLICATO	Regolamentazione laboratori accreditati per screening tecnologici

37

37

DPCM n. 131 30 luglio 2020 1/2

Sicurezza nazionale cibernetica:
disponibilità, integrità e confidenzialità dei dati
continuità dei servizi identificati

Soggetti inclusi nel perimetro:
modalità e criteri di individuazione dei soggetti, pubblici e privati, inclusi nel perimetro di sicurezza nazionale cibernetica

Elenco reti, sistemi informativi e servizi informatici:
criteri per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici

Modalità trasmissione elenchi:
comprensivi della descrizione dell'architettura, della componentistica e dell'analisi del rischio effettuata

https://www.gazzettaufficiale.it/eli/id/2020/10/21/20G00150/sg

38

38

DPCM n. 131 30 luglio 2020 2/2

Sono inclusi nel Perimetro:

- i **soggetti che operano nel settore governativo con riferimento alle attività delle amministrazioni CISR**;
- ulteriori **soggetti**, pubblici e privati, **coinvolti nei seguenti settori**:

• interno; • difesa; • spazio e aerospazio; • energia; • telecomunicazioni;	• economia e finanza; • trasporti; • servizi digitali; • tecnologie critiche; • enti previdenziali/lavoro.

https://www.gazzettaufficiale.it/eli/id/2020/10/21/20G00150/sg

39

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DPR n. 54 del 5 febbraio 2021

CVCN:

procedure, modalità e termini con cui il CVCN verifica e valuta beni, sistemi e servizi ICT che i soggetti inclusi nel perimetro intendono acquisire

Categorie beni, sistemi e servizi ICT:

criteri di individuazione delle categorie soggette alla validazione del CVCN

Ispezioni e verifiche:

procedure, modalità e termini con cui le autorità competenti effettuano le attività di ispezione e verifica del rispetto degli obblighi

https://www.gazzettaufficiale.it/eli/id/2021/04/23/21G00060/sg

40

DPCM n. 81 del 14 aprile 2021

Classificazione incidenti:

L'allegato A riporta le categorie di incidenti aventi impatto su beni ICT suddivisi per gravità

Notifica incidenti:

Procedura di notifica incidenti su beni ICT

Misure di sicurezza:

L'allegato B riporta le misure di sicurezza da adottare per ciascun bene ICT successivamente alla trasmissione degli elenchi.

L'allegato C riporta le misure di sicurezza minime da applicare entro 60 giorni dall'entrata in vigore del regolamento.

https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg

41

41

Allegato A – TASSONOMIE DEGLI INCIDENTI

Nelle **tabelle 1 e 2 dell'Allegato A** viene proposta una classificazione di incidenti di natura cyber che possono avere un **impatto su "beni ICT".** Le due tabelle si differenziano in base al livello di gravità individuato per ciascun incidente: **un livello meno grave e un livello più grave**.

In generale, il concetto di tassonomia rappresenta uno **strumento di riduzione della complessità** particolarmente utile e diffuso nell'ambito dell'analisi e della gestione del rischio.

La tassonomia individuata **è basata sul concetto di impatto**, ovvero sulle implicazioni di un evento di sicurezza a danno dei beni ICT e, conseguentemente, dei servizi essenziali collegati agli stessi.

Tab.	Identificativo (incidente con impatto-ICP)	Categoria
1	ICP-A-1	Infezione (Initial exploitation)
	ICP-A-2	Guasto (Fault)
	ICP-A-3	
	ICP-A-4	
	ICP-A-5	
	ICP-A-6	
	ICP-A-7	
	ICP-A-8	
	ICP-A-9	
	ICP-A-10	
	ICP-A-11	Installazione (Establish persistence)
	ICP-A-12	
	ICP-A-13	
	ICP-A-14	
	ICP-A-15	Movimenti laterali (Lateral Movement)
	ICP-A-16	
	ICP-A-17	
	ICP-A-18	Azioni sugli obiettivi (Actions on objectives)
	ICP-A-19	
2	ICP-B-1	Azioni sugli obiettivi (Actions on objectives)
	ICP-B-2	
	ICP-B-3	
	ICP-B-4	Disservizio (Failure)
	ICP-B-5	
	ICP-B-6	

https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg

42

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Allegato B – MISURE DI SICUREZZA

Le misure di sicurezza previste dall'Allegato B, basate su quanto previsto dal Framework Nazionale per la Cybersecurity e la Data Protection, dovranno essere adottate sui beni ICT da parte di ciascun soggetto incluso nel Perimetro, che dovrà comunicarne l'adozione e le relative modalità al DIS.

Di seguito è riportato un esempio di misure di sicurezza che dovranno essere implementate.

IDENTIFICAZIONE (IDENTIFY)	**Gestione degli asset (Asset Management) (ID.AM)**	I dati, il personale, i dispositivi e i sistemi e le facility necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.
	Governance (ID.GV)	Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.
	Valutazione del rischio (Risk Assessment) (ID.RA)	L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.
	Strategia della gestione del rischio (ID.RM)	Le priorità e i requisiti dell'organizzazione e la tolleranza al rischio sono definiti e utilizzati per supportare le decisioni sul rischio operazionale.
	Gestione del rischio relativo alla catena di approvvigionamento (ID.SC)	Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.

https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg

43

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

DPCM 15 giugno 2021

Categorie di beni, sistemi e servizi ICT soggetti a valutazione CVCN

Componenti hardware e software che svolgono funzionalità e servizi di rete di telecomunicazione (accesso, trasporto, commutazione)

Componenti hardware e software che svolgono funzionalità per la sicurezza di reti di telecomunicazione e dei dati da esse trattati

Componenti hardware e software per acquisizione dati, monitoraggio, supervisione controllo, attuazione e automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali

Applicativi software per l'implementazione di meccanismi di sicurezza

https://www.gazzettaufficiale.it/eli/id/2021/08/19/21A05087/sg

44

Categorie di beni 1/2

Categoria	Bene, Sistema, Servizio
Componenti hardware e software che svolgono funzionalità e servizi di rete di telecomunicazione (accesso, trasporto, commutazione)	• Router • Switch • Repeater • Bilanciatori di carico • Traffic shaper • Proxy • Ponte radio • Access Network per reti radiomobili 2G, 3G, 4G, 5G • Gateway Wifi • Network Function Virtualization (NFV): vSwitch, vRouter, Application Function (5G) • Optical transmission board • Multiservice Provisioning Platform (MSPP) • Automotive ECU switch (Ethernet, CAN, LIN) • IoT Edge Gateway
Componenti hardware e software che svolgono funzionalità per la sicurezza di reti di telecomunicazione e dei dati da esse trattati	• Firewall • Security Gateway • Hardware Security Module (HSM) • Intrusion Detection System (IDS) • Intrusion Prevention System (IPS) • Network Function Virtualization (NFV): Authentication Server Function (5G), Whitelisting dei processi • Virtual Private Network (VPN) • Trusted Platform Module

https://www.gazzettaufficiale.it/eli/id/2021/08/19/21A05087/sg

45

45

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Categorie di beni 2/2

Categoria	Bene, Sistema, Servizio
Componenti hardware e software per acquisizione dati, monitoraggio, supervisione controllo, attuazione e automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali	• Sistemi SCADA (Supervisory Control And Data Acquisition) • Manufacturing Execution Systems (MES) • Software Defined Network (SDN) Controller • Sistemi Artificial Intelligence (AI) e Machine Learning (ML) per gestione reti/sistemi • 5G Mobile Edge Computing (MEC) • Network Function Virtualization (NFV): Network Slice Selection Function (5G), Application Function (5G), Policy Control Function (5G), Unified Data Management (5G), Session Management Function (5G) • Management and Orchestration (MANO) • IoT orchestrator
Applicativi software per l'implementazione di meccanismi di sicurezza	• Applicazioni informatiche per la sicurezza: Public Key Infrastructure (PKI), Single Sign-On (SSO), Controllo Accessi • Moduli software che implementano Web Service mediante API, per protocolli di comunicazione

https://www.gazzettaufficiale.it/eli/id/2021/08/19/21A05087/sg

46

46

47

D.L. 22 del 22 marzo 2019

I servizi di comunicazione basati sulla tecnologia **5G** risultano **attività di rilevanza strategica** per il sistema di difesa e sicurezza nazionale.

Devono essere **notificate** alla Presidenza del Consiglio dei Ministri:

contratti o accordi relativi all'acquisto di beni o servizi relativi alla:

- **progettazione**
- **realizzazione**
- **manutenzione**
- **gestione**

delle reti dei servizi basati sulla tecnologia 5G.

Quando posti in essere con soggetti esterni all'Unione Europea.

48

Regolamento UE 2019/452 - Cybersecurity Act

49

Il Cybersecurity Act

Creare un quadro europeo per la certificazione della sicurezza informatica di prodotti ICT e servizi digitali, uniformando i sistemi di certificazione dei paesi dell'Unione. Il Regolamento agisce in due direzioni:

Quadro europeo di certificazione

L'istituzione di **regole europee per la certificazione di prodotti e servizi ICT**, al fine di facilitare il mutuo riconoscimento di certificati tra Paesi dell'Unione

Stakeholder Cybersecurity Certification Group

Rafforza il ruolo di ENISA

ENISA:
- dovrà redigere uno **schema di certificazione europea**
- assume un **mandato permanente per le attività di supporto** in caso di incidenti informatici subiti dagli Stati membri.

enisa THE EU CYBERSECURITY AGENCY

https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32019R0881&from=EN

50

Direttiva NIS 2 e CER

51

Proposta Direttiva NIS 2 e CER 1/2

Due proposte per affrontare il tema della sicurezza di entità critiche:

DIRETTIVA NIS 2

Aggiornamento disposizioni della Direttiva 2016/1148 (NIS)

DIRETTIVA CER

Amplia l'ambito della Direttiva 2008/114 sulle infrastrutture critiche europee.

Le due direttive mirano ad affrontare i rischi attuali e futuri, derivanti dagli attacchi informatici, dalle attività criminali o dai disastri naturali

52

Direttiva NIS 2

Una revisione della Direttiva NIS si è resa necessaria alla luce dell'accelerazione del processo di digitalizzazione di aziende ed enti pubblici connessa all'attuale pandemia e all'aumento delle minacce cibernetiche.

La valutazione sul funzionamento della Direttiva NIS 2016/1148 ha individuato le tematiche su cui si è ritenuto di intervenire:

1. Il basso livello di cyber resilienza delle imprese operanti nell'UE
2. L'incoerenza del livello di resilienza tra gli Stati membri e i settori
3. Il basso livello comune di consapevolezza della situazione e la mancanza di una risposta comune alle crisi

https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union

NIS 2: categorie essenziali e importanti

Allegato 1: Le entità essenziali		Allegato 2: Le entità importanti
Energia	Acqua potabile	Servizi postali
Trasporti	Acque reflue	Smaltimento rifiuti, manifattura, produzione e distribuzione di prodotti chimici
Banche	Infrastrutture digitali	Produzione, elaborazione e distribuzione di alimenti
Infrastrutture Mercati Finanziari	Pubblica Amministrazione	Manifattura
Sanità	Spazio	Provider di servizi digitali

https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union

NIS 2: Soggetti coinvolti

Non sarà più **competenza** dei singoli Stati membri individuare i soggetti interessati dalla Direttiva.

Tutte le medie e grandi imprese, come definite dalla **raccomandazione della Commissione Europea 2003/361/CE**, rientrano nel campo di applicazione della NIS 2.

Micro e piccole imprese sono **esenti**, a meno di specificità.

Si impone una strategia nazionale di cyber security a tutti gli Stati Membri.

Fonte https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade

55

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

NIS 2: Gestione dei rischi e segnalazione incidenti informatici 1/2

La proposta mira a rafforzare gli **obblighi di sicurezza** per i soggetti coperti dalla normativa, imponendo un approccio di gestione del rischio con un elenco minimo di misure di sicurezza da applicare.

Si amplia l'elenco delle misure da adottare nel processo di gestione dei rischi, come i controlli sulla sicurezza informatica dei propri fornitori o l'uso della **crittografia.**

Gli operatori interessati dovranno adottare **misure tecniche e organizzative adeguate e proporzionate** per gestire le minacce poste alla sicurezza delle reti e dei sistemi informativi e per minimizzare l'impatto di eventuali incidenti informatici.

Per dimostrare la conformità a tali requisiti, gli Stati membri possono richiedere agli operatori interessati di certificare alcuni prodotti, servizi e processi ICT nell'ambito di specifici schemi europei di **certificazione** sulla sicurezza informatica.

fonte: Art. 18 par. 2 della proposta di direttiva

56

NIS 2: Gestione dei rischi e segnalazione incidenti informatici

Sono introdotte disposizioni più dettagliate sulla procedura di segnalazione degli incidenti.

DEFINIZIONE INCIDENTE

Un incidente è considerato significativo se:

- ha un impatto sulla continuità e sulla fornitura dei servizi
- causa perdite finanziarie o danni sulle attività operative
- colpisce persone fisiche o giuridiche determinando considerevoli danni materiali o non materiali.

L'operatore viene a conoscenza dell'avvenuto **incidente**.

La notifica deve essere effettuata **entro 24 ore** alle autorità competenti o al ***Computer Security Incident Response Team (CSIRT).***

A distanza di un mese, dovrà essere rilasciato un **report finale** comprendente una descrizione dettagliata dell'incidente, della sua gravità e del suo impatto, il tipo di minaccia o la causa che lo ha probabilmente provocato e le misure di mitigazione previste.

La proposta di direttiva incoraggia i soggetti che non rientrano nel suo ambito di applicazione a segnalare volontariamente incidenti o minacce alla sicurezza delle reti e delle informazioni, escludendo l'imposizione di obblighi (negativi) al soggetto che effettua la segnalazione.

Fonte: Art. 20, par. 3 della proposta di direttiva; Art. 20, par. 4 della proposta di direttiva

57

NIS 2: Cooperazione tra Stati Membri

La Commissione mira a promuovere la **condivisione** delle informazioni e la **cooperazione** tra gli Stati membri, rafforzando il ruolo del **Cooperation Group**.

All'European Cyber Crises Liaison Organisation Network (EU – CyCLONe) spetta il coordinamento della gestione degli incidenti su larga scala

Il **CSIRT** assume il ruolo di coordinatore, agendo come intermediario di fiducia tra i soggetti segnalanti e i fornitori di prodotti o di servizi ICT.

Fonte: Art. 6 della proposta di direttiva

58

Direttiva sulla Resilienza delle Entità Critiche

La Commissione vuole **creare una panoramica dei rischi transfrontalieri e intersettoriali a livello dell'Unione** per sviluppare pratiche, metodologie, esercitazioni e attività di formazione **per garantire e testare la resilienza delle entità critiche**.

LA STRATEGIA NAZIONALE:

Gli Stati membri adotteranno una strategia nazionale per:

- **garantire la resilienza delle entità critiche;**
- **eseguire valutazioni periodiche del rischio.**

https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

59

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Resilienza delle Entità Critiche

Secondo la direttiva CER le entità critiche devono essere definite sulla base di **criteri comuni** riferiti alla valutazione del rischio che tenga conto sia dei rischi naturali che dei rischi antropici.

Gli Stati membri (entro 3 anni dall'entrata in vigore) devono individuare le entità critiche tenendo conto dei risultati della **valutazione del rischio** e applicando i seguenti criteri:

a) l'entità fornisce uno o più **servizi essenziali**;

b) la **fornitura di tale servizio dipende dall'infrastruttura situata nello Stato membro**;

c) un **incidente avrebbe effetti destabilizzanti** sulla fornitura del servizio o di altri servizi essenziali nei settori che dipendono dallo stesso.

60

Resilienza delle Entità Critiche

Nel determinare la rilevanza di un effetto destabilizzante, gli Stati membri tengono conto dei seguenti **criteri**:

- **numero di utenti**;
- **dipendenza di altri settori dai servizi (di cui all'allegato)**;
- **impatti** che gli incidenti potrebbero avere sulle attività economiche e sociali, **sull'ambiente e sulla sicurezza pubblica**;
- **quota di mercato** dell'entità nel mercato di tali servizi;
- **l'area geografica interessata da un incidente, compresi impatti transfrontalieri**;
- **l'importanza dell'entità nel mantenere un livello sufficiente del servizio**

https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/15122020_proposal_directive_resilience_critical_entities_annex-1_com-2020-829-1_en.pdf

61

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CER: settori

Energia	Acqua potabile
Trasporti	Acque reflue
Banche	Infrastrutture digitali
Infrastrutture Mercati Finanziari	Pubblica Amministrazione
Sanità	Spazio

62


I DI ROMA «TOR VERGATA»
Y MANAGEMENT
Dr. Ing. Luisa Franchina, PhD
l.franchina@hermesbay.com
HB

63