



# Metodologia di cybersecurity risk management 1/2

## Gli 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

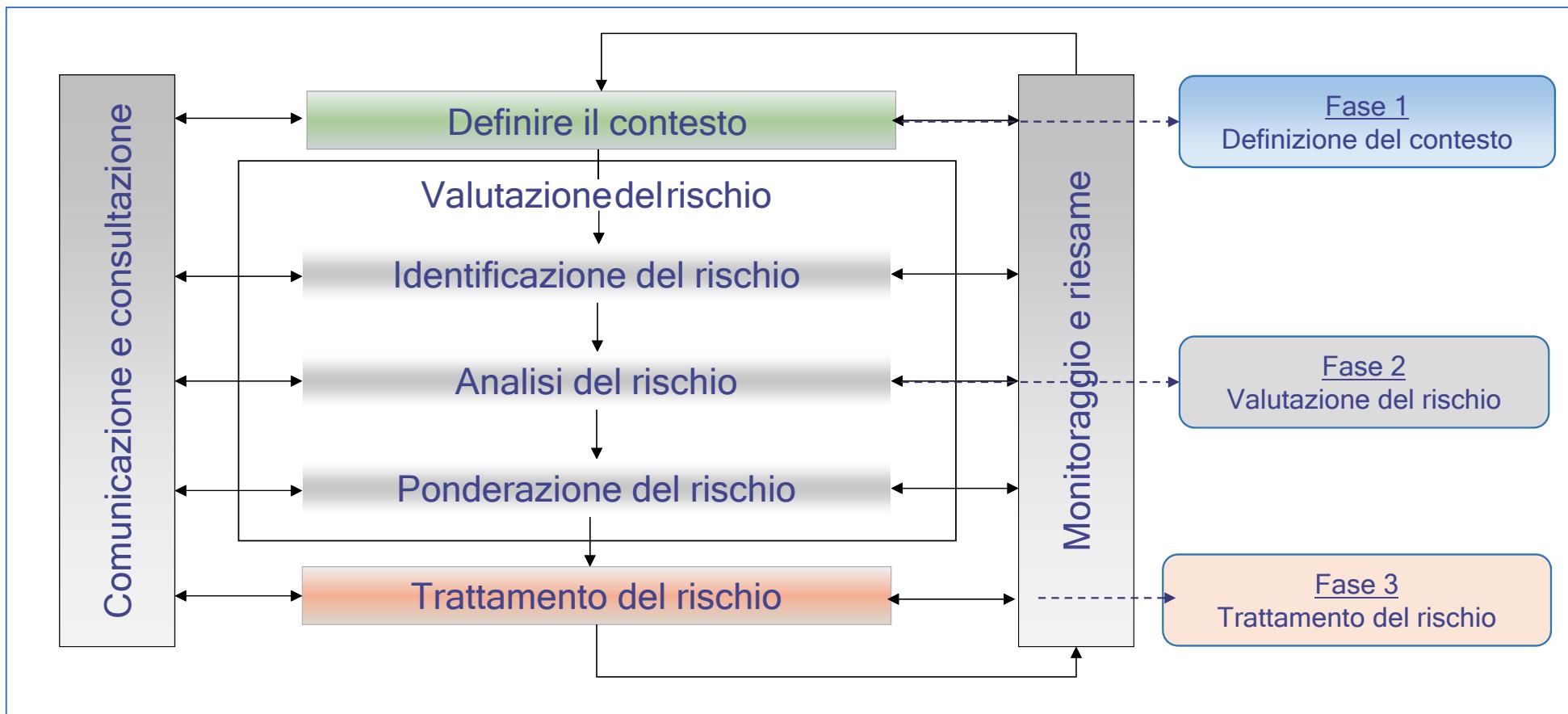


### MISURE MINIME DI SICUREZZA ICT PER LE PA

Misure per valutare e migliorare il livello di sicurezza informatica della PA, al fine di contrastare le minacce informatiche più frequenti



# Metodologia di cybersecurity risk management 2/2





# Metodologia di cybersecurity risk management 2/2

Gentile Cliente,

siamo stati recentemente informati che uno dei nostri fornitori di servizi clienti (subappaltatore) è stato vittima di un attacco informatico nel gennaio 2026, che ha comportato un download non autorizzato di dati personali associati al Suo account cliente.

**Cosa è successo?**

Le nostre indagini, così come quelle del nostro subappaltatore, hanno evidenziato che nel gennaio 2026 è stata effettuata un'estrazione illecita di dati tramite l'account di un agente del nostro subappaltatore.

**Quali dati sono interessati?**

Le informazioni interessate includono: cognome, nome, indirizzo email, numero di telefono ed eventuali scambi con il nostro servizio clienti.

La Sua password non è interessata. I Suoi dati risultano integri e non sono stati modificati.

**Cosa abbiamo fatto?**

Non appena l'incidente è stato individuato, abbiamo adottato immediatamente tutte le misure necessarie per proteggere i Suoi dati.

Le analisi condotte dai nostri team di sicurezza informatica hanno permesso di identificare rapidamente l'account compromesso, che è stato bloccato il giorno stesso della scoperta dell'incidente.

Successivamente, abbiamo revocato tutti gli accessi del nostro subappaltatore ai dati dei nostri clienti. Abbiamo inoltre implementato controlli rafforzati sull'accesso ai dati, sia all'interno della nostra azienda sia presso gli altri nostri subappaltatori.

Abbiamo infine informato la CNIL (Commissione Nazionale Informatica e Libertà francese), l'ANSSI (Agenzia Nazionale per la Sicurezza dei Sistemi Informativi francese) e la piattaforma Cyber Emergency Île-de-France.

**Cosa Le consigliamo di fare?**

I responsabili di questa violazione potrebbero utilizzare alcuni dei dati per tentare azioni



# Metodologia di cybersecurity risk management 2/2

fraudolente nei Suoi confronti o nei confronti di terzi, contattandolo via email o telefono (tentativi di phishing tramite email, SMS o telefonate) oppure impersonandolo (furto d'identità su Internet).

La invitiamo pertanto a prestare la massima attenzione a possibili tentativi di frode e a seguire le seguenti raccomandazioni:

- **Verifichi sempre l'origine delle email ricevute** e accerti l'identità del mittente, controllandone in particolare l'indirizzo email;
- **Non apra email o allegati in caso di dubbio sulla loro origine** e non risponda a messaggi provenienti da mittenti sconosciuti;
- **In caso di incertezza, verifichi l'identità del mittente** tramite un canale alternativo (numero di telefono o indirizzo email diverso);
- **Non comunichi informazioni riservate** senza averne verificato l'origine e non condivida alcun dato (in particolare dati bancari, codici di accesso, password o identificativi) senza aver accertato la sicurezza del messaggio e l'identità del richiedente, indipendentemente dal canale utilizzato (email, telefono, SMS o social media);
- **Non clicchi su link sospetti** presenti nelle email e verifichi l'indirizzo del sito verso cui il link rimanda prima di accedere;
- **Verifichi sempre l'indirizzo del sito** prima di inserire o trasmettere informazioni riservate;
- **Si assicuri che il software antivirus sia attivo e aggiornato** sul Suo computer;
- **Monitori regolarmente i Suoi conti bancari** per verificare l'eventuale presenza di addebiti fraudolenti;
- In caso di operazioni sospette, contatti tempestivamente la Sua banca per contestarle.

Per maggiori dettagli e informazioni, puoi consultare il sito dell'ACN (Agenzia per la



# Metodologia di cybersecurity risk management 2/2

Cybersicurezza Nazionale) su <https://www.acn.gov.it> e la pagina dedicata alla cybersecurity del Garante per la protezione dei dati personali su <https://www.garanteprivacy.it/temi/cybersecurity>, dove troverai i rischi legati al furto di identità e le misure per proteggerli.

## Il nostro impegno

Ci rammarichiamo per questa violazione della riservatezza delle Sue informazioni e stiamo facendo tutto il possibile per porvi rimedio. La sicurezza e la fiducia dei nostri utenti restano la nostra priorità.

A tal proposito, abbiamo attivato una linea telefonica dedicata, disponibile al \_\_\_\_\_ per rispondere a qualsiasi domanda relativa a questo incidente. Il Responsabile della Protezione dei Dati di \_\_\_\_\_ resta inoltre a Sua disposizione per ulteriori informazioni al seguente indirizzo: \_\_\_\_\_



# Macro-modello di calcolo del rischio 1/2

## CARATTERISTICHE SERVIZI

A seconda delle caratteristiche primarie dei servizi erogati, è determinato il livello di criticità intrinseca (Profilo di Criticità). Le caratteristiche primarie e secondarie consentono di selezionare le Misure di Sicurezza da implementare (controlli di tipo amministrativo, sicurezza logica e fisica, etc...) e dunque determinare le Vulnerabilità.

## BENCHMARK

Il benchmark consente di valutare il fattore di Esposizione alla singola minaccia.

## IMPATTO

Consente di valutare gli impatti per ciascun servizio erogato in caso di perdita di Riservatezza (R), Integrità (I) e Disponibilità (D). A partire dagli impatti sui singoli servizi erogati, sarà poi calcolato l'impatto R,I,D sui servizi stessi.





# Macro-modello di calcolo del rischio 2/2





# Gli attacchi informatici

Attività ostili nei confronti di una componente informatica, spesso compiute sfruttando le debolezze della componente umana.



# Panorama delle minacce principali

Malware  
phishing

Web attack  
Vulnerabilità

DDoS  
botnet

**Monetizzare**

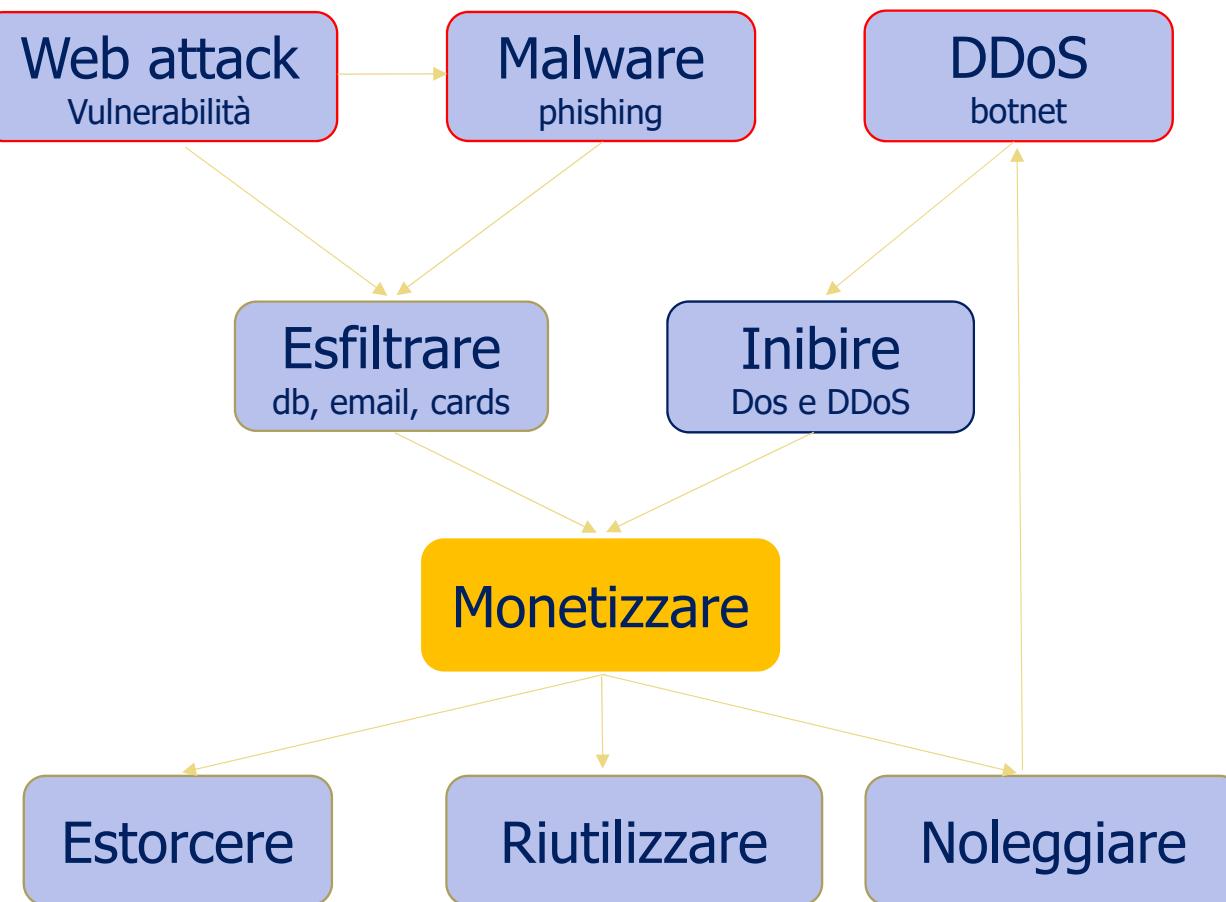
Esfiltrare  
db, credenziali, carte...

Estorcere  
ransomware, ddos, breach...

Botnet



# Flusso della minaccia in dettaglio





# Gli attori

## Le vittime



- Scelte o casuali
- Sistemi informatici **esposti** e **vulnerabili**
- Personale **non** adeguatamente preparato
- Eventi di interesse **nazionale**

## Gli attaccanti



- Criminali di strada, **assoldati** o in **autonomia**, singoli o in gruppo
- Hacktivisti
- Terroristi
- Paesi (ostili?)



# Vittime scelte o casuali?

## Scelte

- Target mirato
- Selezione per brand e per categoria

## Casuali

- Non esiste un target specifico
- Attacchi massivi





# Vittime scelte o casuali?

	Opportunistico	Mirato
Selezione vittima	Casuale	Specifica
Automazione	Alta	Limitata
Preparazione	Minima	Approfondita
Obiettivo	Monetizzazione rapida	Informazione strategica / sabotaggio
Attori tipici	Cybercriminali	APT, stati, gruppi organizzati



# Sistemi esposti e vulnerabili

This screenshot shows a Shodan search results page for the 'Heartbleed' vulnerability. The search bar at the top contains the term 'Heartbleed'. The results are displayed in a grid format. One prominent result is for IP address 102.24.214.81, which is identified as running OpenSSL 1.0.2g-fips 11 Dec 2013. The interface includes a world map showing the locations of discovered hosts and various filters and search options.

Heartbleed

This screenshot shows a Shodan search results page for 'Default password'. The search bar at the top contains the term 'Default password'. The results are displayed in a grid format. One prominent result is for IP address 122.154.98.114, which is identified as running MySQL 5.6.25. The interface includes a world map showing the locations of discovered hosts and various filters and search options.

Default password

This screenshot shows a ZOOME search results page displaying a large list of discovered vulnerabilities across multiple hosts. The results are presented in a table format with columns for host, port, service, and severity. The interface includes a world map showing the locations of discovered hosts and various filters and search options.



# Sistemi esposti e vulnerabili

Heartbleed	Default password
Vulnerabilità di codice	Vulnerabilità di configurazione
Complessa da scoprire	Banale
Richiede patch	Richiede policy
Dipende dallo sviluppatore	Dipende dall'utente/amministratore



# Eventi nazionali

**Al fine di consentire una migliore e piu' efficace canalizzazione delle richieste di servizio,  
il sito è temporaneamente non disponibile.**

**Si assicura che tutti gli aventi diritto potranno utilmente presentare  
la domanda per l'ottenimento delle prestazioni.**

Il servizio di presentazione della domanda di Indennità COVID-19 prevista dal Decreto-legge n 17 marzo 2020, sarà disponibile a breve.

Le indennità previste riguarderanno le seguenti categorie:

- Professionisti con partita IVA e lavoratori con rapporto di collaborazione coordinativa;
- Lavoratori autonomi iscritti alla Gestione speciali dell'AGO;
- Lavoratori del turismo e degli stabilimenti termali;
- Lavoratori agricoli operai a tempo determinato;
- Istruttori della carriera iscritti ai ruoli ordinari del funzionario dello Stato;

**INPS**

La pagina richiesta non è al momento disponibile , si prega di riprovare più tardi.  
Per tornare al sito cliccare qui [www.inps.it](http://www.inps.it)

**Impossibile raggiungere il**

La pagina web all'indirizzo  
<https://www.inps.it/nuovoportaleinps/default.aspx> potrebbe essere temporaneamente non disponibile oppure è stata permanentemente spostata a un nuovo indirizzo.

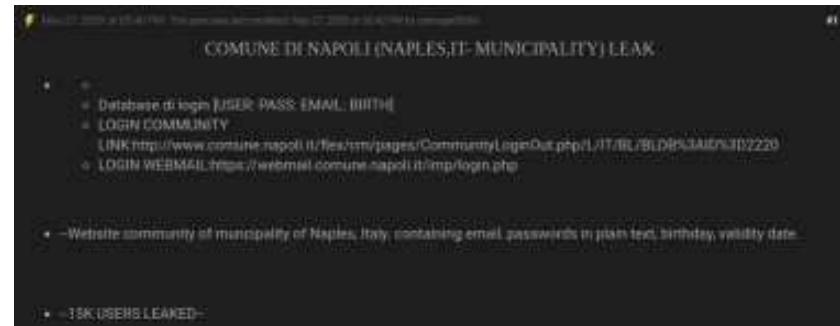


# Data leak

- Sono sempre esistiti ma oggi è diventata una moda
- È nato un mercato di nicchia in forte crescita
- I blackmarket sono migrati dal darkweb al deepweb
- Prezzi sempre più accessibili

## Quali dati in vendita?

- Dati anagrafici
- Email
- Credenziali
- Carte di credito





# Data leak

- Sono sempre esistiti ma oggi è diventata una moda
- È nato un mercato di nicchia in forte crescita
- I blackmarket sono migrati dal darkweb al deepweb
- Prezzi sempre più accessibili

## Quali dati in vendita?

- Dati anagrafici
- Email
- Credenziali
- Carte di credito



# Leak con pubblica minaccia di estorsione

Fondazione Arena di Verona - Full dump (100%)  
<https://www.arena.it/>

 Cybersecurity

**Total Info**

- Phone: +39 02 00000000
- Fax: +39 02 00000000
- Email: [comunicazioni@arena.it](mailto:comunicazioni@arena.it)
- Address: Via Mario Andretti 60, 35122 Verona

**Proofs**

- Facebook.zip
- Twitter.zip
- Discord#2448#7890#1122#123456 [K] 07/01/19 00:20:24 04/25/20 07/28/29 00:00:34 2014  
00:00:37/01:26:43:01:42:43:44:45

Erci Group [www.erci.com]

Search for:  Advanced search

THE SECRET AND THE PUBLIC

THIS PAGE IS FOR INTERNAL USE ONLY. PLEASE DO NOT DISTRIBUTE IT TO ANYONE ELSE.

In 7 days we will publish the part one and two, and so on until the forthcoming weeks that will be published.

**ALTRI**

- ALQUILER
- BANCA
- BASTARDO
- BORGARD
- BULOGNA
- VOLCANO
- IRMIND
- CENTRO
- COAL-BRASIL
- COAL-NIGERIA
- COAL-URUGUA
- COAL-URUGUAY
- COAL-TORNE NORI
- CORTI
- DOMINÓ-OCULOS
- EMILIA-TOSCANA, IT
- EN\_70\_MILIT
- FUSION
- GEM-46
- GEM-BRASILE
- HYDRO-MG\_GOLCARA
- HYDRO-MG\_GOLCARA

**IT**

- Erci Web Up 120-CPO
- Chile
- Colombia
- O
- DODGE
- DODGE INSPIRE09
- EIE
- FRANCE
- GREECE
- ITALY
- JAPAN
- Magnesite\_Bardon
- Magnesite\_Ferrante
- MIRAZZONE\_SPADOLI
- Magnesite\_Drapols
- Magnesite\_Ferranti
- OEM\_LH\_JAPAN
- ROMASPA
- Z

**Energy-Market**

**Finance-Group**

**Industrial**

**Marketing-PR**

**Project-Management**

**Real-Estate**

**R&D**

**Regulatory-Insider**

**Sales-Channel**

**Supply**



UNIVERSITÀ DEGLI STUDI DI ENNA "KORE"

## CORPORATE LEAKS

[HOME](#) | [ACTIVE](#) | [FINISHED](#) | [ABOUT](#) | [CONTACT](#)

### Luxottica. Part 3, 4, 5, other 1.

0

Posted on November 7, 2020 by leaker\_10000

LUXOTICA\_Human\_Resources\_part\_3.xlsx  
LUXOTICA\_ranking\_part\_4.xlsx  
LUXOTICA\_e\_com\_part\_5.xlsx  
LUXOTICA\_other\_part\_1.xlsx  
LUXOTICA\_human\_Resources\_part\_3.xls  
LUXOTICA\_ranking\_part\_4.xls  
LUXOTICA\_e\_com\_part\_5.xls  
LUXOTICA\_other\_part\_1.xls

Luxottica Group S.p.A. is an Italian eyewear conglomerate and the world's largest company in the eyewear industry. It is based in Milan, Italy.

As a vertically integrated company, Luxottica designs, manufactures, distributes and retails its eyewear brands, including LuxCrafters, Sunglass Hut, Apex by Sunglass Hut, Pearle Vision, Target Optical, Eyemed vision care plan, and Glasses.com. Its best known brands are Ray-Ban, Persol, and Oakley.

Luxottica also makes sunglasses and prescription frames for designer brands such as Chanel, Prada, Giorgio Armani, Burberry, Versace, Dolce and Gabbana, Mu Mu and Tory Burch.

In January 2017, Luxottica announced a merger with Essilor. The combined entity would