

# The NIST Cyber Security Framework

Il Cyber Security Framework è un **framework sviluppato per facilitare le organizzazioni nel gestire le attività di gestione del rischio**. In particolare, il framework è nato da una direttiva del presidente Obama nel 2013, che riconosceva l'importanza, per garantire la sicurezza nazionale degli USA, di avere delle infrastrutture critiche sicure. La direttiva del presidente, quindi, impartiva al NIST (**National Institute of Standards and Technology**) di realizzare un insieme di attività, che potessero garantire la sicurezza delle infrastrutture critiche all'interno del Paese. Il NIST ha pubblicato la prima versione del framework nel febbraio del 2014, mentre la versione attuale (ovvero la **versione 1.1**) è stata rilasciata nell'aprile del 2018.

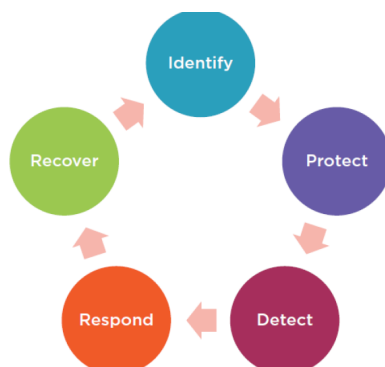
Il Cyber Security Framework è composto da **tre parti** fondamentali:

1. **Core** → insieme di attività e strategie, che un'organizzazione può adottare per gestire i rischi;
2. **Tiers** → sono i diversi livelli, con cui un'organizzazione può implementare le attività descritte nel framework. I Tiers, di fatto, rappresentano il livello di maturità con cui un'organizzazione gestisce gli attacchi cyber;
3. **Profile** → rappresentano quali sono le attività (del framework) che vengono implementate dall'organizzazione, personalizzate per il contesto specifico dell'organizzazione. Pensiamo, quindi, ai profili come una versione personalizzata delle attività del framework, per una specifica organizzazione.

A questo punto, analizziamo in maniera approfondita queste tre parti e quindi iniziamo con il **Core** → esso è organizzato in **cinque funzioni**, le quali rappresentano delle strategie che un'organizzazione può implementare per gestire i rischi cyber. Queste cinque funzioni, a loro volta, sono articolate in attività (che vengono chiamate **categorie**) e **sotto-categorie**, le quali dettagliano ulteriormente le attività svolte (dall'organizzazione) all'interno delle categorie. In totale, il framework è costituito da:

- 5 funzioni;
- 23 categorie;
- 108 sotto-categorie.

A questo punto, analizziamo in maniera più approfondita ogni singola componente del framework. Iniziamo con le cinque funzioni, le quali possono essere osservate meglio attraverso il seguente schema:



Vediamo che abbiamo:

- la funzione **Identify** → essa corrisponde a tutte le attività, che consentono ad un'organizzazione di capire quali sono gli assets (ovvero le risorse critiche) da proteggere e il processo (che deve essere adottato dall'organizzazione) per gestire i rischi;
- la funzione **Protect** → comprende tutte quelle misure di protezione, che l'organizzazione deve adottare per prevenire gli attacchi agli assets dell'organizzazione stessa. Quindi, questa funzione comprende le misure di protezione preventive degli attacchi, che l'organizzazione deve adottare;
- la funzione **Detect** → comprende tutte quelle misure di protezione, che consentono all'organizzazione di identificare che vi è un attacco in corso, verso uno o più dei propri assets;
- la funzione **Respond** → comprende tutte quelle attività e misure di protezione, che l'organizzazione deve implementare per contenere l'impatto che l'attacco ha sugli assets;
- la funzione **Recover** → comprende tutte quelle azioni, che l'organizzazione (nell'ipotesi in cui l'attacco abbia avuto successo e di conseguenza ha causato degli impatti negativi su uno o più assets) deve adottare al fine di ripristinare gli assets compromessi e l'operatività dell'organizzazione.

Ciascuna di queste funzioni specifica le macro-categorie, ovverosia le categorie ad alto livello di attività che l'organizzazione deve implementare e poi le sotto-categorie, le quali dettagliano maggiormente le attività che devono essere implementate. All'interno del Core (oltre quindi alle funzioni, alle categorie e alle sotto-categorie) vi

sono i **referimenti normativi** → il framework, per ciascuna sotto-categoria, specifica dei riferimenti ad altri standard di sicurezza, in modo tale da dare delle linee guida su come implementare una specifica attività all'interno dell'organizzazione.

Ora analizziamo meglio ciascuna funzione:

- funzione di **Identify** → comprende sei categorie:
  - **Asset Management** → comprende l'inventario di tutte le risorse, che l'organizzazione ritiene critiche per il perseguimento dei propri obiettivi di business. In questa attività, quindi, la prima cosa da fare è capire quali sono le risorse critiche per l'organizzazione (le risorse critiche possono essere, ad esempio, le informazioni personali dei propri clienti o dei propri dipendenti, oppure dispositivi HW, Server).
  - **Business Environment** → una volta eseguita l'attività di Asset Management, bisogna capire l'ambiente in cui opera l'organizzazione. Quindi, capire quali sono gli obiettivi strategici dell'organizzazione ed eventuali vincoli derivanti da legislazioni a cui l'organizzazione è sottoposta. Questo ci fa capire quali sono i vincoli, a cui l'organizzazione è sottoposta, per selezionare determinate misure di protezione degli assets;
  - **Governance** → questa attività comprende tutti i processi e le politiche, che governano l'attività dell'organizzazione e che le consentono di raggiungere gli obiettivi strategici. In questa fase, vengono creati dei processi ad hoc per gestire i rischi derivanti dagli attacchi cyber, in maniera tale che la gestione di tali rischi venga gestita come parte dell'intera organizzazione;
  - **Risk Assessment** → attività per identificare i rischi agli assets aziendali e quindi consiste nell'andare a determinare quali sono i possibili attacchi agli assets aziendali e qual è il livello di rischio associati a questi attacchi.
  - **Risk Management Strategy** → il processo di Risk Assessment deve essere fatto nell'ambito di un processo continuo, in modo tale da aggiornare ed individuare continuamente nuove misure di protezione, che l'organizzazione deve implementare per difendersi dagli attacchi;
  - **Supply Chain Risk Management** → visto che è molto importante avere un processo per gestire separatamente tutti i rischi, che possono derivare da attacchi che vanno a colpire organizzazioni che forniscono servizi all'organizzazione stessa (quindi attacchi che vanno a colpire organizzazioni, che forniscono software, dispositivi o servizi online alla nostra organizzazione). È importante avere un processo che identifica tali rischi,

perchè sempre di più abbiamo attacchi che vanno a colpire la Supply Chain di un'organizzazione (ovvero le organizzazioni di terze parti, sfruttando ad esempio, delle vulnerabilità presenti nell'organizzazione di erogazione di servizi), invece di colpire l'organizzazione stessa. Il processo, oltre che ad identificare i rischi, deve stabilire un contratto, che obbliga i fornitori a implementare misure di protezione adeguate, in modo tale da mitigare i rischi a cui l'organizzazione può essere esposta.

- la funzione **Protect** → comprende sei categorie:
  - **Identify Management, Authentication, Access Control** → una delle attività fondamentali di questa funzione, è l'attività di gestione:
    - delle **identità digitali**;
    - e dei **permessi** che hanno gli utenti e ogni dispositivo connesso alla rete aziendale

Quindi, avere una funzionalità di questo tipo, consente all'organizzazione di verificare l'identità sia degli utenti connessi alla rete aziendale, sia di tutti i sistemi (quali ad esempio: dispositivi e Server) connessi alla rete aziendale.

Inoltre, nella definizione dei permessi associati agli utenti e ai dispositivi, è importante che venga implementata la proprietà del Least Privilege, ovvero che ad ogni utente e dispositivo vengano associati solamente i permessi necessari alla loro attività;

- **Awareness and Training** → dato che non basta verificare l'identità dei dispositivi e degli utenti e limitarne i permessi (a solamente quelli che ne hanno bisogno), ma bisogna agire anche sulla conoscenza dei dipendenti, nel senso che: una delle componenti fondamentali dell'azienda è rappresentata dai propri dipendenti, i quali devono essere educati ad utilizzare i servizi e le informazioni processate dall'azienda. In questa sotto-categoria abbiamo diverse tipologie di Training:
  - training mirato ai dipendenti dell'azienda, per insegnarli i rischi a cui è soggetta l'azienda e le azioni che nel loro piccolo possono compiere per limitare tali rischi (esempio: password sicura oppure l'autenticazione a due fattori);
  - training per il personale con privilegi elevati (come per esempio gli amministratori), per educarli sulle varie tipologie di attacco che l'azienda può subire.

- **Data Security** → comprende una serie di attività legate a garantire la protezione dei dati, quando essi sono condivisi su una rete non sicura, oppure quando sono memorizzati su una macchina o su un Server. Oltre a garantire la protezione dei dati, comprende una serie di attività legate alla protezione dei software, che vengono eseguiti sulle macchine dell'organizzazione. Quindi, questa sotto-categoria comprende una serie di meccanismi atti a garantire:
  - l'integrità del codice eseguito sulle macchine;
  - la disponibilità dei dati e dei servizi offerti dall'organizzazione.
- **Information Protection Processes and Procedures** → va a definire le attività, che devono definire le politiche su come i processi e i servizi (che vanno a processare i dati dell'organizzazione) devono essere implementati, in maniera tale che si evitino situazioni in cui le vulnerabilità dei processi stessi, vengano utilizzate dagli attaccanti;
- **Maintenance** → attività che si focalizzano sulla protezione e sulla disponibilità degli assets aziendali;
- **Protective Technology** → comprende una serie di misure di protezione tecniche (come per esempio, la cifratura), che garantiscono la confidenzialità, la disponibilità e l'integrità dei sistemi e delle informazioni aziendali.
- la funzione **Detect** → essa comprende tre categorie:
  - **Anomalies and Events** → serie di attività che si focalizzano sull'analisi di dati, che sono associati alle attività di rete condotte dagli utenti, utilizzando i dispositivi e i servizi aziendali. L'obiettivo di queste attività è di analizzare i dati e rilevare eventuali situazioni, che potrebbero corrispondere ad attacchi informatici (per esempio, controllare se vi è un accesso alla rete aziendale da un indirizzo IP particolare, oppure che da uno stesso indirizzo IP si rilevino molteplici accessi);
  - **Security Continuous Monitoring** → serie di attività che prescrivono cosa deve essere monitorato per rilevare eventuali attacchi in corso. In particolare, deve essere monitorato:
    - tutta l'attività di rete;
    - le attività degli utenti;

- qualsiasi connessione comunemente non utilizzati all'interno dell'azienda;
  - tutte le situazioni, in cui un utente potrebbe abusare dei propri privilegi, per accedere ad informazioni e/o servizi a cui normalmente non accede.
- **Detection Processes** → serie di attività che riguardano il processo di identificazione degli attacchi. In particolare, si comprendono le attività che prescrivono:
- **cosa** si deve fare nel momento in cui si rileva un attacco;
  - **quali** informazioni devono essere fornite, in riferimento all'attacco che è stato rilevato (indirizzo IP, pacchetti di rete, pacchetti utilizzati);
  - **chi** sono i responsabili ad intervenire, nel caso in cui l'attacco venga rilevato.
- la funzione **Respond** → essa comprende cinque categorie:
- **Response Planning** → serie di attività che mirano a definire, per ogni tipologia di attacco, quali sono le azioni che l'organizzazione deve adottare per limitare gli effetti dell'attacco (per esempio, nel caso di un attacco malware, disconnettere immediatamente la macchina per evitare la propagazione del malware). Oltre alle attività, bisogna definire i **ruoli**, ovvero si deve definire chi è responsabile ad implementare tali attività, in maniera tale da limitare l'impatto dell'attacco;
  - **Communications** → nel momento in cui si rileva un attacco, vi è una serie di soggetti a cui condividere le informazioni relative all'attacco. Certamente, tali informazioni sono da comunicare:
    - ai soggetti responsabili del piano di risposta all'attacco;
    - alle altre organizzazioni e agli utenti, che possono essere impattati dall'attacco;
    - agli enti governativi (come ad esempio, il garante della privacy).
  - **Analysis** → serie di attività che consistono nell'andare ad analizzare le **cause**, che hanno portato all'attacco, e le **tecniche** utilizzate dagli attaccanti. In base a queste analisi, si devono poi implementare determinate misure per limitare gli effetti dell'attacco;
  - **Mitigation** → queste misure per limitare gli effetti dell'attacco vengono implementate nella fase di Mitigazione;

- **Improvements** → serie di attività che sono focalizzate sull'aggiornamento e il miglioramento del piano di risposta (definito dall'organizzazione) agli attacchi.
- la funzione **Recover** → essa è composta da tre sotto-categorie:
  - **Recovery Planning** → come nella fase di Detection, la prima cosa da fare è definire un piano per ripristinare gli assets aziendali compromessi dall'attacco e identificare i soggetti in grado di implementare tale piano di ripristino;
  - **Improvements** → si identificano delle azioni migliorative rispetto al piano di ripristino, in modo tale da limitare gli effetti negativi di possibili futuri attacchi;
  - **Communications** → si gestiscono le comunicazioni con il pubblico e con gli investitori dell'organizzazione, in modo tale da limitare gli impatti all'immagine aziendale, fornendo informazioni su come è avvenuto l'attacco e su quali misure sono state adottate per ripristinare l'operatività dell'azienda.

---

Una volta analizzato in maniera approfondita il Core, passiamo ad analizzare la seconda componente fondamentale del Cyber Security Framework, ovvero i **Tiers** → essi rappresentano il livello di implementazione delle attività presenti nel Core. Possiamo, quindi, definire qual è la maturità con cui l'organizzazione ha implementato le attività presenti nel Cyber Security Framework. In particolare, vi sono quattro livelli di implementazione definiti dal Cyber Security Framework, ovvero:

1. livello **Parziale** → rappresenta il livello più basso;
2. livello di **Risk informed**;
3. livello **Ripetibile**.
4. livello **Adattivo** → rappresenta il livello più maturo di implementazione.

In base alle seguenti tre caratteristiche, vengono definiti i quattro livelli definiti dal Cyber Security Framework:

1. se l'azienda ha un programma di gestione dei rischi;
2. se i rischi, relativi agli attacchi cyber, sono gestiti nell'ambito degli altri rischi che ha l'azienda (come per esempio: rischi finanziari, rischi relativi all'operatività) → quindi se i rischi, relativi agli attacchi cyber, non vengono considerati come una

categoria a parte, bensì vengono considerati come una categoria di rischio che può compromettere il raggiungimento degli obiettivi strategici dell'azienda;

3. se vengono utilizzate informazioni (riguardanti rischi, vulnerabilità e attacchi correnti) provenienti da enti esterni (come per esempio: agenzie governative nazionali) o dalle organizzazioni con cui l'azienda stessa interagisce.

A questo punto, analizziamo meglio i singoli livelli:

- livello **Parziale** → rappresenta il livello più basso del Cyber Security Framework e in questo caso, l'organizzazione non ha definito un processo di Risk Management. L'organizzazione, quindi, adotta un approccio alla gestione dei rischi che è “**reattivo**”, nel senso che: Quando l'azienda è soggetta ad un attacco informatico, allora si decide quali misure di protezione adottare per ripristinare l'operativa oppure per limitare gli effetti dell'attacco. In questo caso, quindi, l'azienda:
  - non è consapevole delle tipologie di attacco informatici a cui è soggetta;
  - non ha un piano di gestione dei rischi;
  - ignora qualsiasi informazione provenienti da enti esterni o dalle altre organizzazioni;
  - non ha un piano per gestire i rischi legati ai fornitori di servizi terzi.
- livello **Risk Informed** → assume che l'organizzazione:
  - faccia almeno una volta un processo di Risk Assessment e quindi, sappia quali sono i rischi a cui è soggetta;
  - non ha un processo formale di Risk Management (a livello organizzativo) e di conseguenza, i rischi relativi agli attacchi cyber, sono gestiti nell'ambito degli altri rischi che ha l'azienda;
  - ha una relazione con i fornitori di servizi ed è consapevole, che ci possono essere dei rischi derivanti dai fornitori di servizi, ma **non** ha un processo per gestirli;
  - attinge dalle informazioni sugli attacchi recenti, per condurre il processo di Risk Assessment.
- livello **Ripetibile** → rappresenta il livello a cui tutte le organizzazioni ambiscono di raggiungere, in quanto in questo caso, abbiamo che l'organizzazione:
  - ha definito, in maniera formale e rigorosa, un processo di gestione dei rischi;

- ha una gestione dei rischi cyber, per cui sono stati definiti processi e politiche;
- ha un processo di gestione dei rischi derivanti dai fornitori di servizi.
- livello **Adattivo** → in questo caso, abbiamo che:
  - il processo di gestione dei rischi riesce ad essere facilmente aggiornato all'organizzazione, in funzione di come cambiano gli obiettivi strategici dell'azienda o anche su come cambia lo scenario di attacco → questo è possibile, perchè il processo di gestione dei rischi è ben strutturato.

---

Analizziamo, infine, l'ultima parte del Cyber Security Framework, ovverosia i **Profili** → essi definiscono lo stato corrente della strategia di gestione dei rischi implementata da un'organizzazione. In particolare, un'organizzazione dovrebbe ambire a creare due profili:

1. profilo **Target** → consiste nell'andare a prendere le attività, che compongono le cinque funzioni del Core, e selezionarle per soddisfare gli obiettivi strategici dell'azienda, ridurre i rischi identificati durante il processo di Risk Management e soddisfare eventuali vincoli, che potrebbero derivare dal contesto in cui opera l'organizzazione;
2. profilo della **Situazione corrente** → l'organizzazione deve capire le attività presenti nel Cyber Security Framework, che sono attualmente implementate dall'organizzazione.

Sorge a questo punto la domanda: **“Come si applica il framework all'interno di un processo di Risk Management?”** La fase iniziale (comune a tutti i processi di Risk Management) consiste nell'andare a capire quali sono gli assets aziendali. Dopo di ch  si deve andare a prioritizzare gli assets, in base a quali sono gli obiettivi strategici, che l'organizzazione vuole raggiungere. Successivamente dobbiamo fare Risk Assessment, ovverosia identificare quali sono gli attacchi e le vulnerabilit  presenti negli assets aziendali e come questi possono essere compromessi dagli attacchi. Alla fine del processo di Risk Assessment, dobbiamo definire qual   il profilo corrente dell'organizzazione, ovverosia quali sono le attivit , del Cyber Security Framework, attualmente implementate dall'organizzazione. Successivamente dobbiamo fare la valutazione dei rischi e quindi, per tutti gli scenari di attacco, dobbiamo capire l'impatto negativo e la probabilit  con cui si verifichi. Una volta fatto ci , sapr  per ciascun rischio, il suo livello corrispondente (alto, medio, basso). Dopo di ch , dobbiamo definire il profilo Target dell'organizzazione. Una volta che abbiamo il profilo corrente e il profilo Target, dobbiamo effettuare la **gap analysis**, ovvero

dobbiamo identificare le attività presenti nel profilo Target, che non sono attualmente implementate dall'organizzazione. Infine, dobbiamo implementare un piano di implementazione e di conseguenza, per ciascuna delle attività non presenti nel profilo corrente dell'organizzazione, dobbiamo definire un piano di implementazione e dobbiamo definire tutte le persone che saranno coinvolte nell'implementare ciascuna attività.

Riassumendo tutto, possiamo dire che: Il Cyber Security Framework è costituito da standard, linee guida e pratiche per ridurre il rischio informatico delle infrastrutture critiche. Esso è composto da:

- il **Core**, che fornisce un insieme di attività e risultati desiderati in materia di cybersecurity;
  - i **Tiers**, che guidano le organizzazioni a considerare il livello di rigore appropriato per il loro programma di cybersecurity;
  - i **Profili**, che sono utilizzati principalmente per identificare e dare priorità alle opportunità di miglioramento della cybersecurity in un'organizzazione.
- 

## An Introduction to Privacy

Una prima definizione di privacy è la seguente: **“La privacy è un concetto, che ha una quantità infinita di significati.”** → ovvero, la privacy è un concetto difficile da definire, perchè per un soggetto potrebbe avere un significato, mentre per altri potrebbe avere un altro significato. Vediamo alcune definizioni di privacy:

- una delle prime definizioni di privacy risale al 1890 ed è: il diritto di essere lasciati da soli → questa definizione è stata realizzata da due avvocati, in risposta a due grandi innovazioni tecnologiche di quel periodo, ovvero:
  - la fotografia;
  - i giornali scandalistici.

queste due innovazioni, quindi, venivano visti dai due avvocati come un'invasione della privacy degli individui;

- un'altra definizione risale al 1970 ed è: il diritto dell'individuo di decidere quali informazioni su di sé debbano essere comunicate ad altri e in quali circostanze → questa definizione, corrisponde all'idea di privacy in cui l'utente deve essere in controllo dei propri dati personali;

- un'altra definizione risale al 2001 ed è: la libertà di esprimersi e di costruire la propria identità → questa definizione è molto legata ai sistemi e agli Stati, in cui la popolazione non ha diritto di esprimersi;
- la definizione più recente, è del GDPR e risale al 2018 ed è: soddisfacimento di quattro principi cardine, ovvero:
  - la **trasparenza** → tutte le volte, che l'organizzazione raccoglie dei dati personali relativi ad un individuo, dovrebbe informare l'individuo su come i dati vengono trattati e con chi verranno condivisi;
  - lo **scopo** → ovverosia, i dati devono essere raccolti per uno scopo preciso;
  - la **proporzionalità** → i dati che vengono forniti dagli utenti, devono essere solamente quelli necessari per raggiungere lo scopo preciso prefissato;
  - la **responsabilità** → l'organizzazione che raccoglie i nostri dati personali, deve dimostrare che tratta i dati in maniera conforme a questi principi appena elencati. Se non lo fa, la privacy viene violata.

Quando parliamo di rispettare la privacy (così come per rispettare la sicurezza) abbiamo un insieme di proprietà, che vogliamo che vengano garantite da un sistema. In particolare, le proprietà le possiamo raggruppare in due categorie:

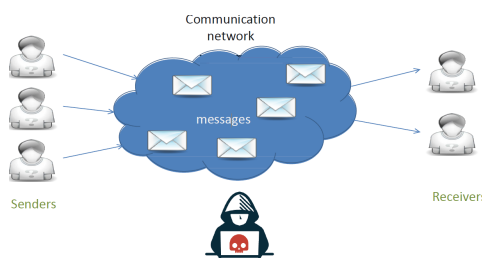
1. **Hard Privacy** → parte dall'assunzione, che le organizzazioni con cui un utente condivide i propri dati personali, non possono essere fidate e non gli si possono dare il ruolo di proteggere i nostri dati personali. Questo significa, che l'utente (nel momento in cui interagisce con il fornitore di servizi e/o l'organizzazione) deve fornire all'organizzazione la minor quantità di informazioni possibile e inoltre l'utente è responsabile di implementare misure di protezione, per garantire la privacy dei propri dati;
2. **Soft Privacy** → parte dall'assunzione, che dal momento in cui l'utente decide di condividere i propri dati personali con un'organizzazione, l'utente ha perso il controllo di quei dati e quindi, l'utente non può implementare alcuna misura di protezione per garantire la privacy. L'unica cosa che può fare l'utente, quindi, è fidarsi dell'organizzazione a cui ha condiviso i propri dati personali e delegarli il ruolo di proteggere tali dati.

Le due categorie di privacy, ovverosia la Hard privacy e la Soft privacy, richiedono di soddisfare proprietà diverse. In particolare:

- parliamo di Hard Privacy, quando il sistema soddisfa una o più delle seguenti proprietà:

- Anonimità;
- Unlinkability;
- Anonymity & Pseudonymity;
- Plausible deniability.
- parliamo, invece, di Soft Privacy, quando il sistema soddisfa almeno le seguenti proprietà:
  - Compliance;
  - User awareness;
  - Confidenzialità.

Queste proprietà sono state definite da due studiosi e quando le hanno definite, avevamo in mente un modello di comunicazione molto semplice, ovvero:



vi è un sistema, in cui gli utenti si scambiano delle informazioni (come per esempio: messaggi o delle email) e quindi abbiamo due categorie di utenti:

1. i **senders** → ovvero gli utenti che inviano i messaggi;
2. i **receivers** → ovvero gli utenti che ricevono i messaggi.

Abbiamo poi un **attaccante**, il quale osserva le comunicazioni che avvengono tramite questo sistema e il suo obiettivo è ricavare delle informazioni da queste comunicazioni. Tali informazioni di interesse per l'attaccante prendono il nome di **items of interest** e possono essere, ad esempio:

- sapere chi è il mittente oppure il destinatario di un messaggio;
- sapere con quale frequenza un dato mittente e un dato destinatario comunicano;
- sapere se o più messaggi appartengono alla stessa conversazione.



Queste informazioni sono di interesse all'attaccante, perchè da esse l'attaccante è in grado di ricavare ulteriori informazioni sensibili degli utenti e/o dei destinatari.

A questo punto, analizziamo meglio le proprietà elencate precedentemente:

- **Anonimità** → viene definita come l'incapacità dell'attaccante di identificare il mittente oppure il destinatario di un messaggio. Solitamente, l'anonymità viene definita rispetto ad un insieme di utenti, perchè chiaramente non si ha anonimato, se il sistema è costituito da un unico utente. L'anonymità, quindi, mira a spezzare il legame che c'è tra un messaggio (e quindi un'informazione) e l'utente a cui tale messaggio (e quindi tale informazione) si riferisce → l'anonymità del mittente, quindi, viene garantita se l'attaccante non riesce a distinguere il mittente del messaggio, da tutti gli altri utenti, che possono inviare messaggi all'interno del sistema. Allo stesso modo, garantiamo l'anonymità del destinatario del messaggio, se l'attaccante non è in grado di distinguere il destinatario del messaggio, da tutti gli altri utenti che possono ricevere messaggi all'interno del sistema;

Adesso, immaginiamoci di essere un impiegato di un'azienda e di dover fare delle statistiche (come per esempio: il salario medio) sui dipendenti di sesso femminile. All'interno dell'azienda, però, vi è un solo dipendente donna e quindi, capiamo immediatamente che l'anonymità non è garantita e che siamo immediatamente in grado di capire chi è e quanto guadagna. Spesso, quindi, il concetto di anonimato viene associato all'utilizzo di uno **Pseudonimo** → ovvero, invece di utilizzare l'identità reale di un utente per autenticarsi nel sistema, gli si associa uno pseudonimo, che solitamente è una **stringa casuale di caratteri**. Il problema di questa soluzione è: Se ogni volta che accediamo al sistema, utilizziamo sempre lo stesso pseudonimo, non potremmo mai raggiungere l'anonymità.

- Un'altra proprietà da analizzare è l'**Unlinkability** → in questo caso, quello che vogliamo nascondere all'attaccante è che **esiste una relazione tra due items of interest** (per esempio, vogliamo che l'attaccante non sia in grado di determinare che due messaggi sono legati alla stessa conversazione tra due utenti). Se l'attaccante riesce a scoprire questa relazione, potrebbe inferire nuove informazioni sensibili sull'utente a cui queste informazioni sono associate, oppure l'attaccante potrebbe addirittura risalire all'identità dell'utente;
- Un'altra proprietà da analizzare è l'**Undetectability** → in questo caso, vogliamo nascondere all'attaccante, il fatto che addirittura esista un certo item of interest

legato ad un utente del sistema. Vogliamo, quindi, effettivamente nascondere l'esistenza di un certo dato/informazione relativo ad un utente del sistema (per esempio, immaginiamoci che il dipendente di una clinica vuole accedere al fascicolo di una persona famosa, ma non ha i permessi per farlo. Il dipendente, però, ha potuto dedurre che il personaggio famoso si trova all'interno della clinica e con l'**Undetectability** questo non può più essere possibile);

- Un'altra proprietà è la **Plausible Deniability** → questa proprietà, fa sì che un utente possa negare di aver compiuto una determinata azione all'interno del sistema → questa proprietà, quindi, è esattamente l'opposto della proprietà di Non Repudiation;
- Un'altra proprietà è la **Confidenzialità** → vogliamo garantire, che i dati personali degli utenti siano accessibili solamente agli utenti del sistema autorizzati e che non vengano divulgati;
- Un'altra proprietà è la **Compliance** → si riferisce alla legislazione sulla protezione dei dati. Il regolamento generale sulla protezione dei dati (ovverossia il GDPR) specifica i principi per il trattamento dei dati personali all'interno dell'UE (per esempio, che le organizzazioni devono cancellare i dati personali degli utenti, una volta che non gli servono più);
- Un'altra proprietà è l'**Awareness** (= consapevolezza) → gli utenti devono essere informati delle conseguenze della condivisione delle informazioni e quindi devono essere consapevoli di **con chi** i propri dati vengono condivisi e devono poter esercitare il controllo **su chi** ha accesso ai propri dati (quindi, evitare ad esempio di condividere la foto della propria carta di credito sui social network, dato che in questo modo tutti gli amici, possono conoscere il numero della carta). Soluzione suggerita è di adottare strumenti di feedback e di sensibilizzazione.