Dispensa e video per FAD: stima durata del lavoro complessivo pari a 4 ore.

Verifica con test a risposta multipla in data da definire alla fine della sospensione delle attività didattiche

NUOVA ECDL
MODULO IT SECURITY
Syllabus 2.0

Prof.ssa Agnese Di Donato

Video
MODULO 5 SEZIONE 1_CONCETTI DI SICUREZZA DEI DATI
https://www.youtube.com/watch?v=AKdyLuAqeRo
Durata: 24:25 min

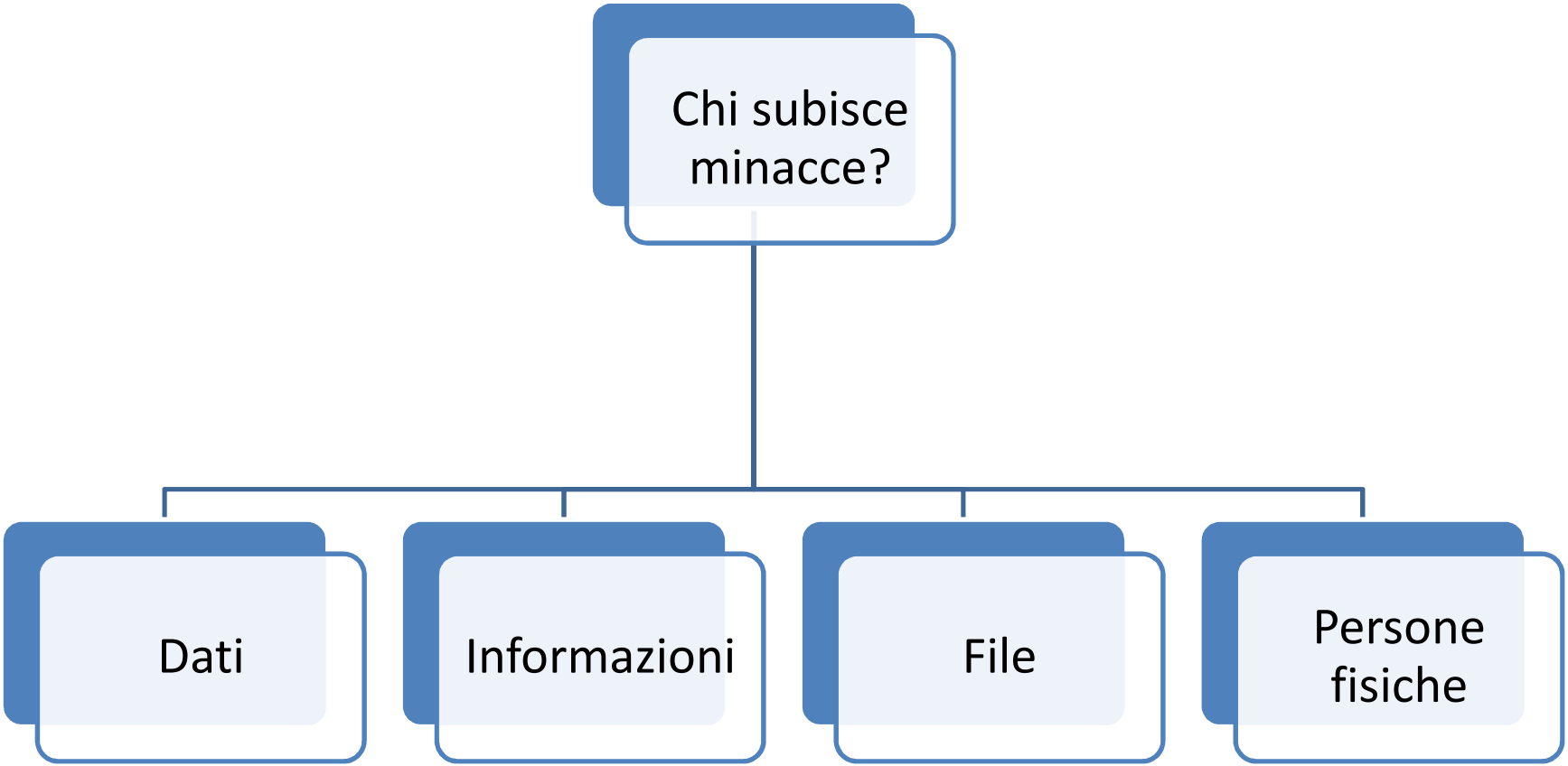
NUOVA ECDL
MODULO IT SECURITY
Syllabus 2.0

NUOVA ECDL
MODULO IT SECURITY
Syllabus 2.0

SEZIONE 1
CONCETTI DI SICUREZZA

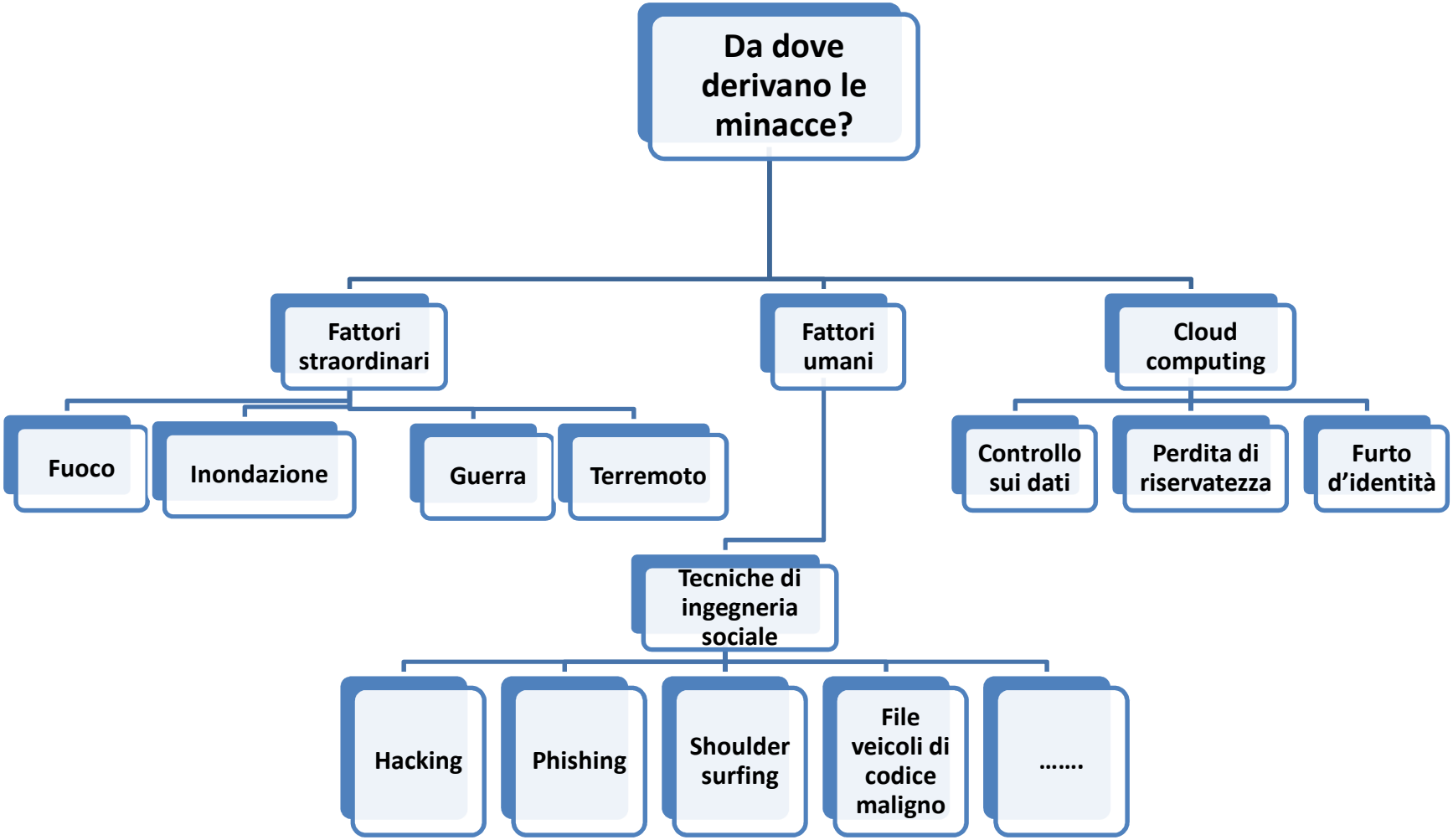
Prof.ssa Agnese Di Donato

SEZIONE 1 – CONCETTI DI SICUREZZA



SEZIONE 1 – CONCETTI DI SICUREZZA

SEZIONE 1 – CONCETTI DI SICUREZZA

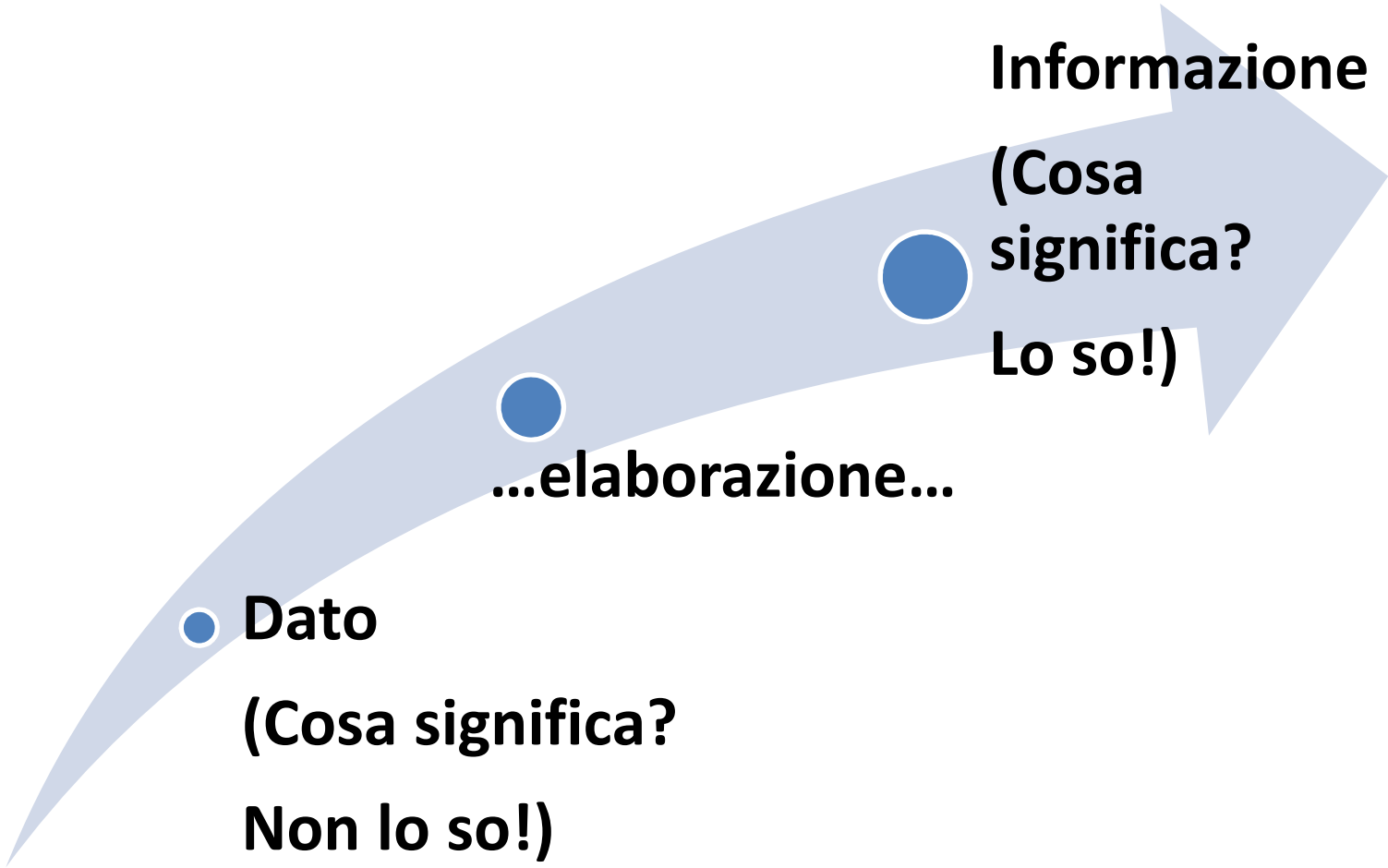


SEZIONE 1 – CONCETTI DI SICUREZZA

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.1 MINACCE AI DATI

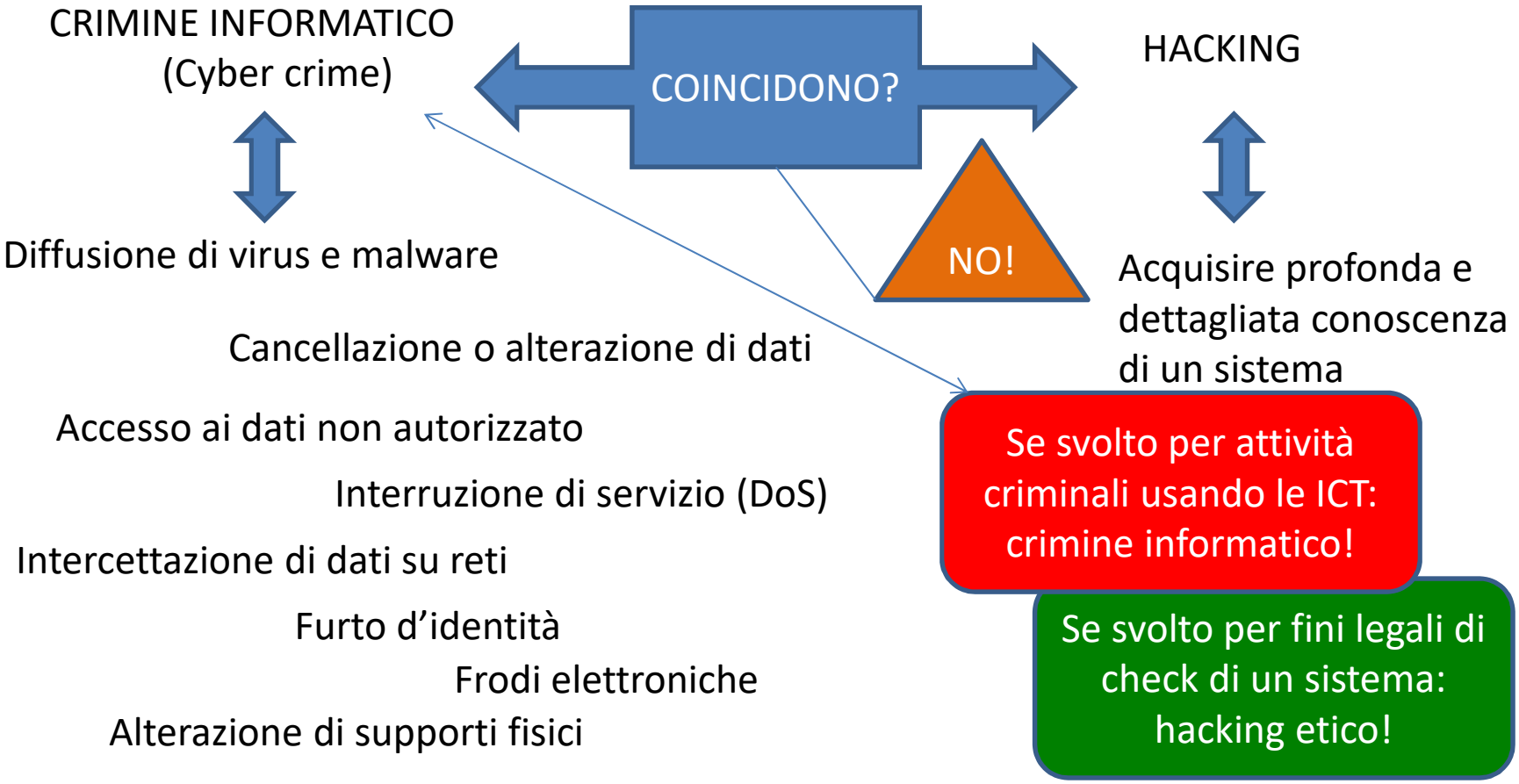
Argomento 1.1.1 Distinguere tra dati ed informazioni



SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.1 MINACCE AI DATI

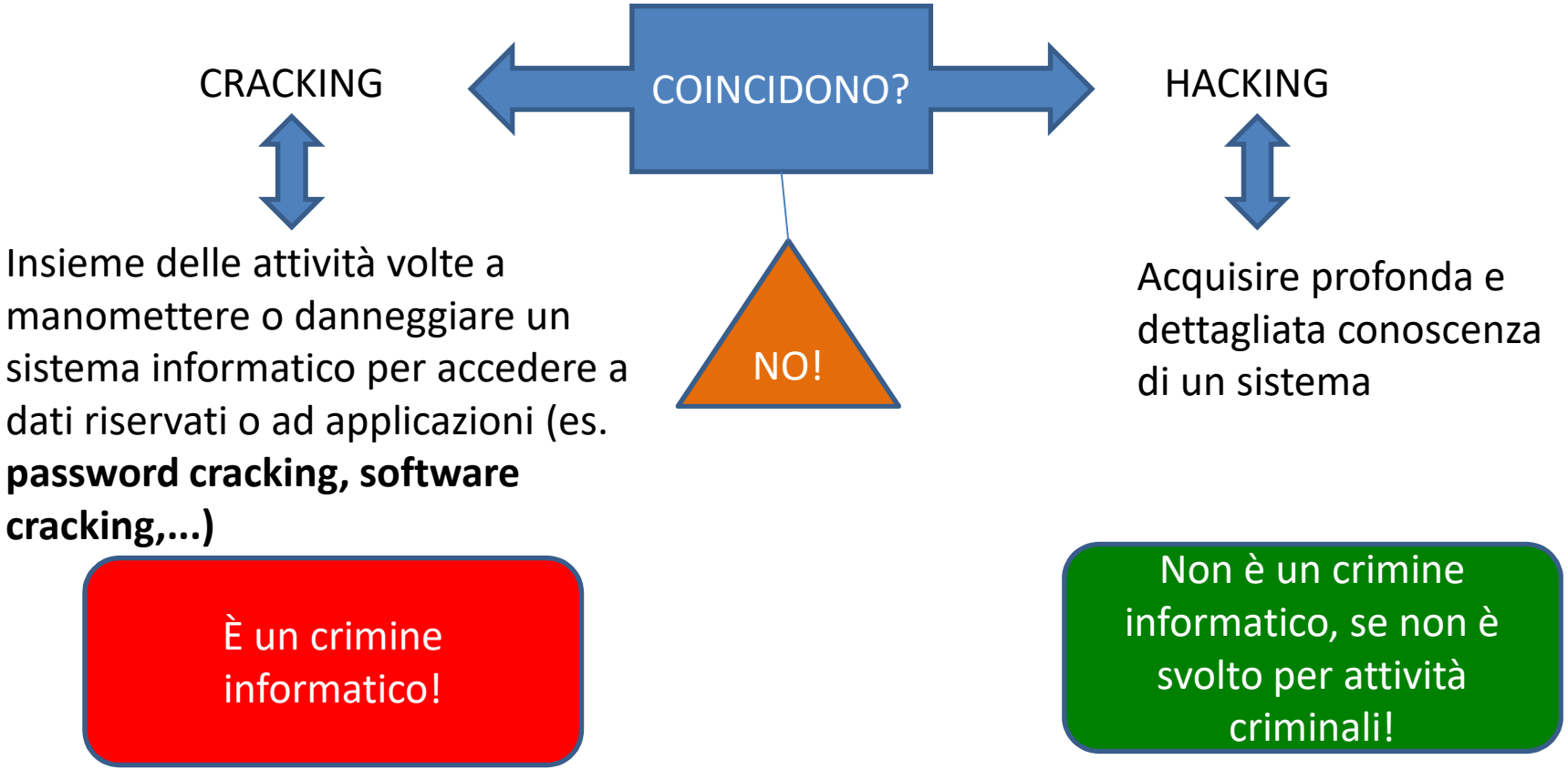
Argomento 1.1.2 Comprendere i termini “crimine informatico” e “hacking”



SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.1 MINACCE AI DATI

Argomento 1.1.2 Comprendere i termini “crimine informatico” e “hacking”



SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.1 MINACCE AI DATI

Argomento 1.1.2 Comprendere i termini “crimine informatico” e “hacking”

CRACKING

Insieme delle attività volte a manomettere o danneggiare un sistema informatico per accedere a dati riservati o ad applicazioni (es. **password cracking, software cracking,...)**

È un crimine informatico!

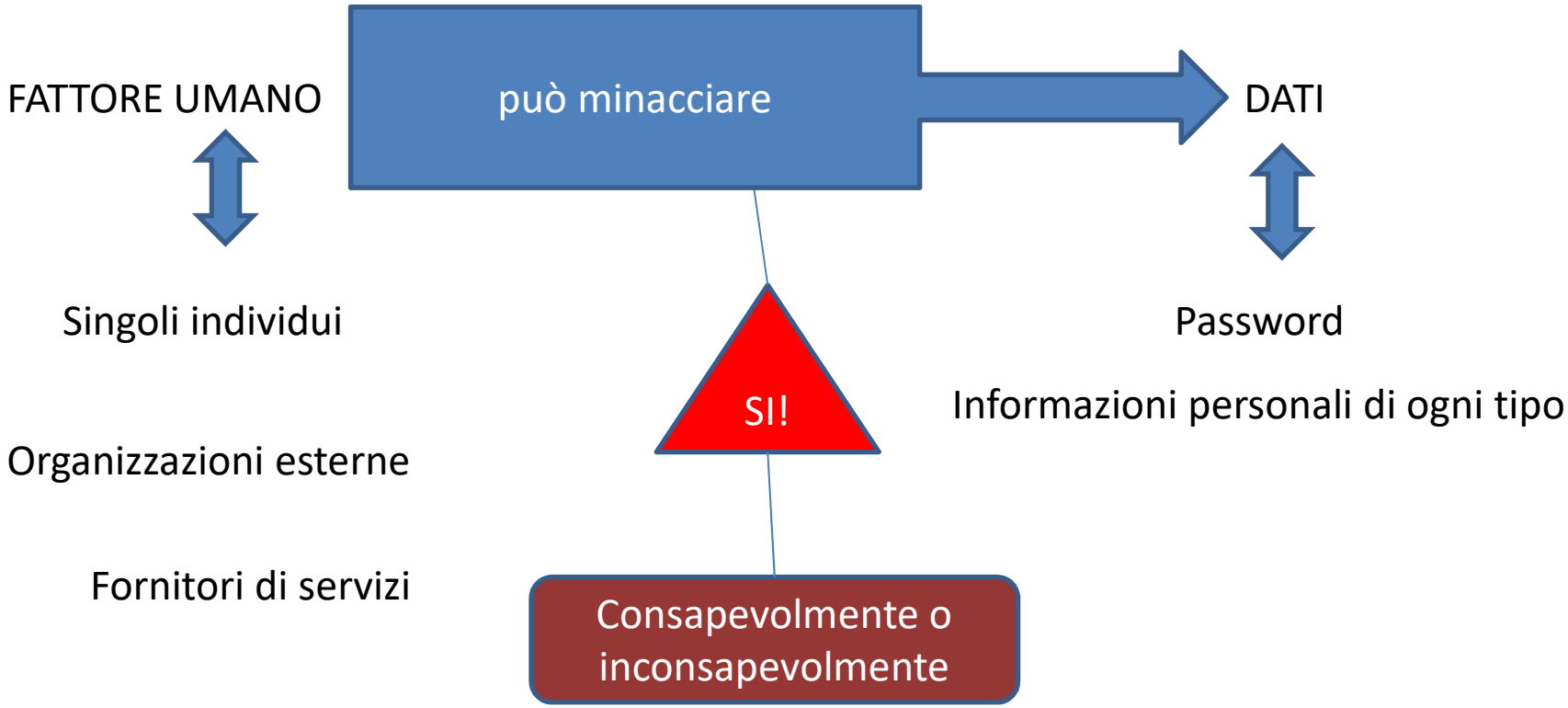
Cracking di password: recupero di password, in modo manuale o con appositi programmi, da dati memorizzati o inviati ad un sistema informatico.

Cracking di software: disattivazione o eliminazione di alcune funzioni del software come la protezione contro la copia, i numeri di serie, le chiavi hardware, i controlli di dati, ecc.

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.1 MINACCE AI DATI

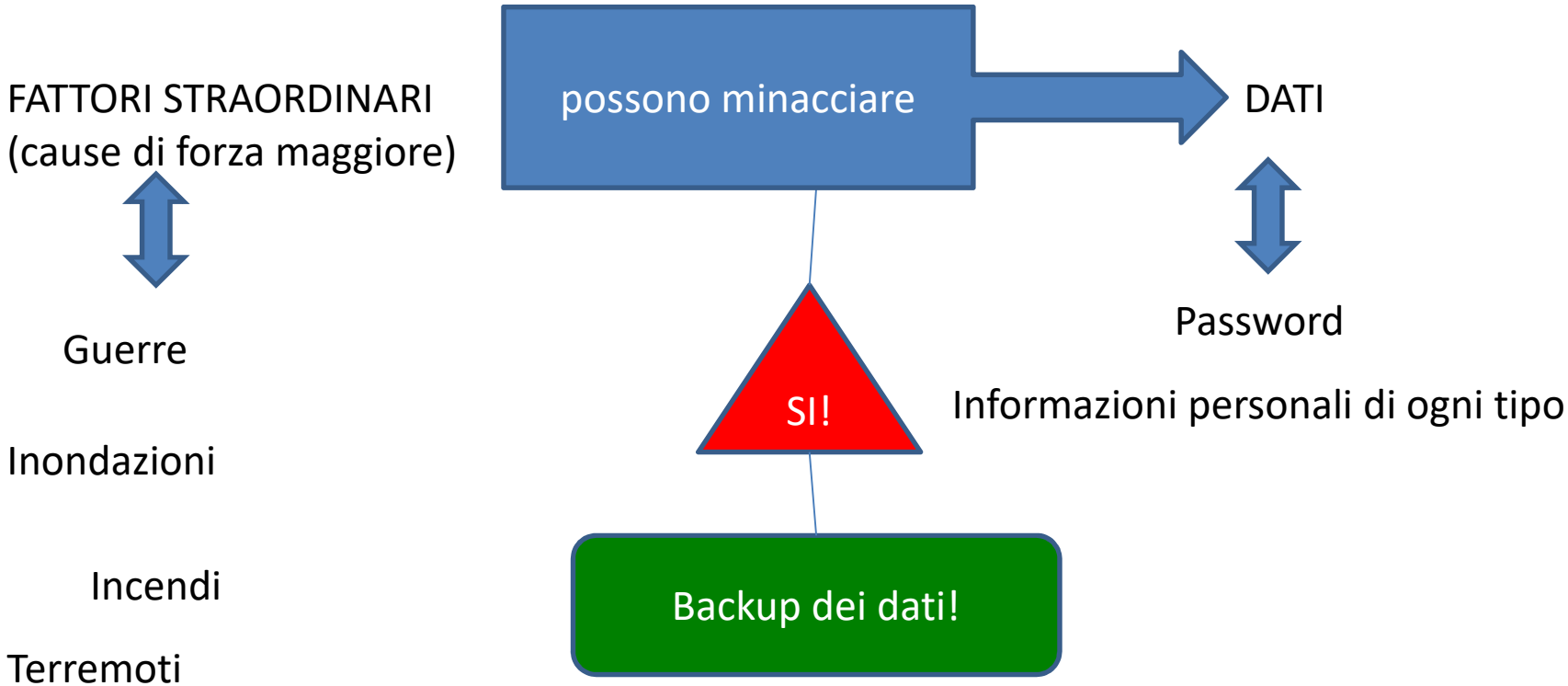
Argomento 1.1.3 Riconoscere le minacce dolose e accidentali ai dati provocate da fattore umano



SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.1 MINACCE AI DATI

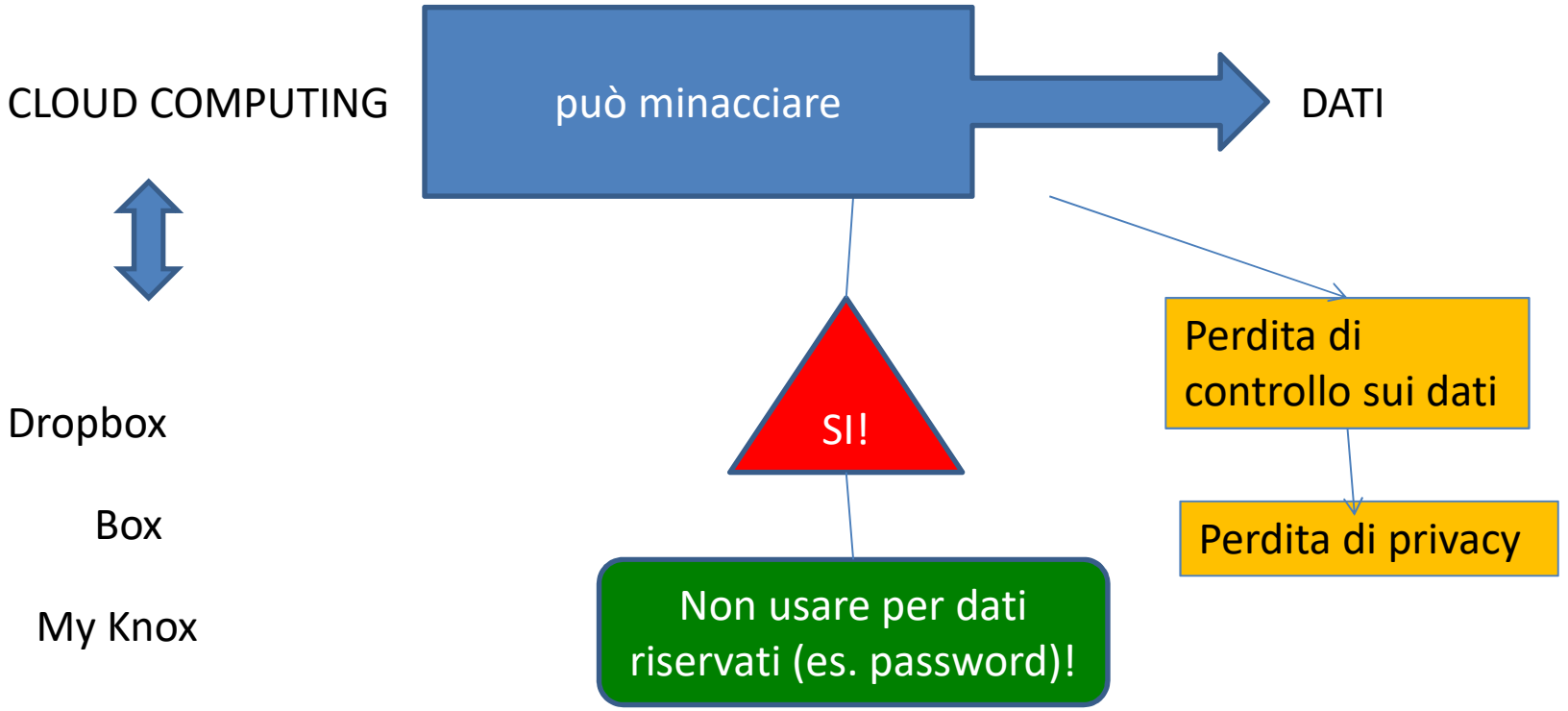
Argomento 1.1.4 Riconoscere le minacce ai dati provocate da circostanze straordinarie



SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.1 MINACCE AI DATI

Argomento 1.1.5 Riconoscere le minacce ai dati provocate da uso di Cloud computing



SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.2 VALORE DELLE INFORMAZIONI

Argomento 1.2.1 Comprendere le caratteristiche fondamentali della sicurezza delle informazioni

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.2 VALORE DELLE INFORMAZIONI

Argomento 1.2.2 Comprendere i motivi per proteggere le informazioni personali

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.2 VALORE DELLE INFORMAZIONI

Argomento 1.2.2 Comprendere i motivi per proteggere le informazioni personali

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.2 VALORE DELLE INFORMAZIONI

Argomento 1.2.2 Comprendere i motivi per proteggere le informazioni personali

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.2 VALORE DELLE INFORMAZIONI

Argomento 1.2.2 Comprendere i motivi per proteggere le informazioni personali

Informazioni personali

(nome, cognome, indirizzo, numero di telefono, abitudini, convinzioni politiche o religiose, stile di vita, stato di salute, relazioni personali, situazione economica, …) → Dati sensibili!

SEZIONE 1 – CONCETTI DI SICUREZZA

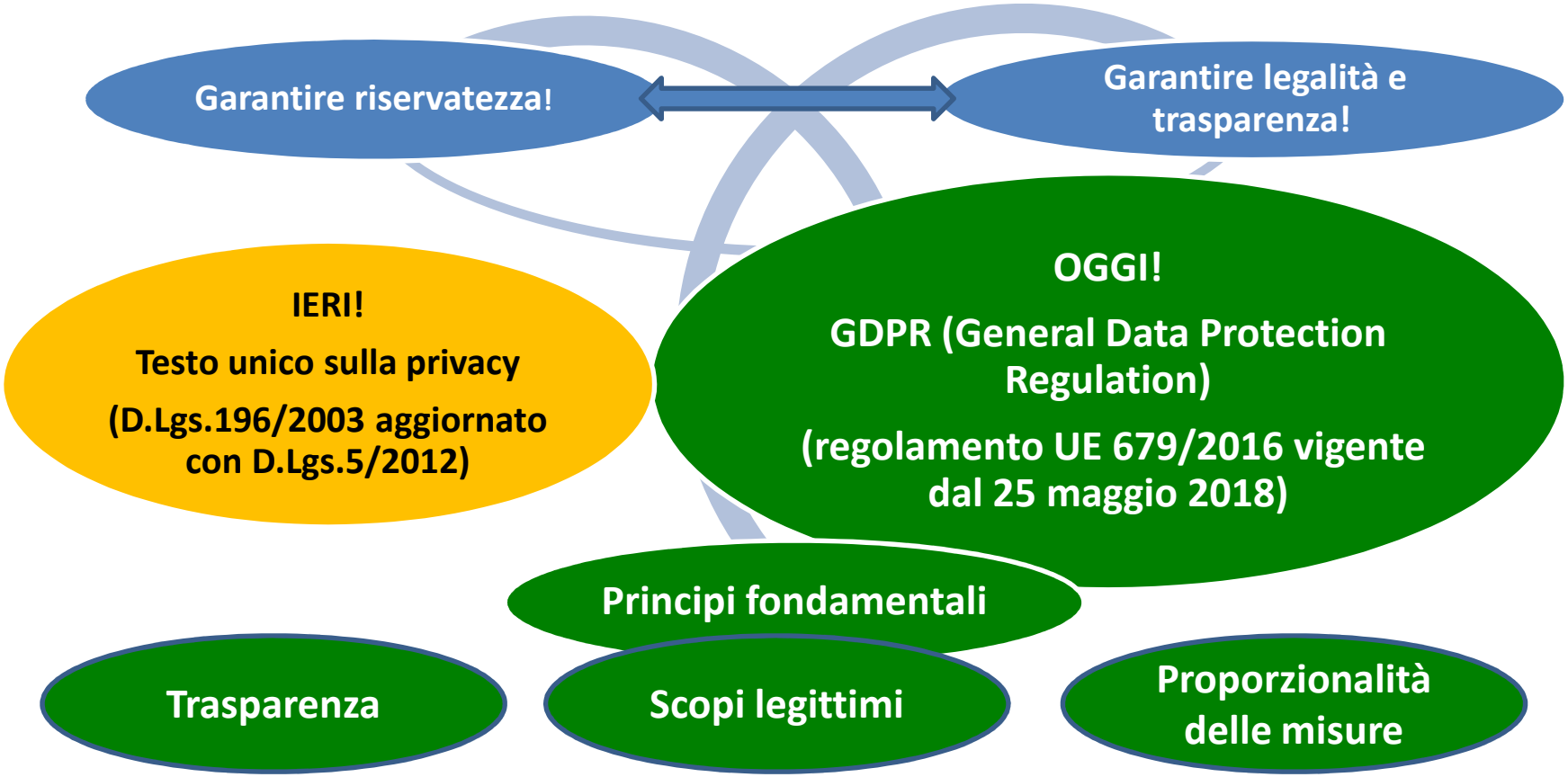
TEMA 1.2 VALORE DELLE INFORMAZIONI

Argomento 1.2.3 Comprendere i motivi per proteggere informazioni di lavoro su computer e dispositivi mobili

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.2 VALORE DELLE INFORMAZIONI

Argomento 1.2.4 Identificare i principi comuni per la protezione, conservazione e controllo dei dati e della riservatezza



SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.2 VALORE DELLE INFORMAZIONI

Argomento 1.2.4 Identificare i principi comuni per la protezione, conservazione e controllo dei dati e della riservatezza

Trasparenza

Modalità mediante la quale i dati vengono raccolti e protetti e deve essere indicata in modo chiaro e privo di qualsiasi ambiguità (devono essere descritti motivi e finalità, comunicate le procedure adottate per il rispetto delle regole e le modalità di contestazione).

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.2 VALORE DELLE INFORMAZIONI

Argomento 1.2.4 Identificare i principi comuni per la protezione, conservazione e controllo dei dati e della riservatezza

Scopi legittimi

Il soggetto che raccoglie e successivamente garantisce la tutela dei dati deve indicare chiaramente quali siano gli scopi e la necessità della raccolta di tali dati, come per esempio l'erogazione di un certo servizio, senza violare i diritti dell'interessato.

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.2 VALORE DELLE INFORMAZIONI

Argomento 1.2.4 Identificare i principi comuni per la protezione, conservazione e controllo dei dati e della riservatezza

Proporzionalità delle misure in rapporto ai danni

Le misure di sicurezza adottate per la protezione dei dati devono essere adeguate alle conseguenze che deriverebbero da una parziale o totale perdita dei dati conservati

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.2 VALORE DELLE INFORMAZIONI

Argomento 1.2.5 Comprendere i termini “soggetti dei dati” e “controllori dei dati” e relativi principi di tutela

SOGGETTI DEI DATI

Persone che forniscono i propri dati

Hanno DIRITTO a conoscere le finalità del trattamento dei propri dati e ad opporsi ad alcune di esse (ad es. fini pubblicitari,…)

CONTROLLORI DEI DATI

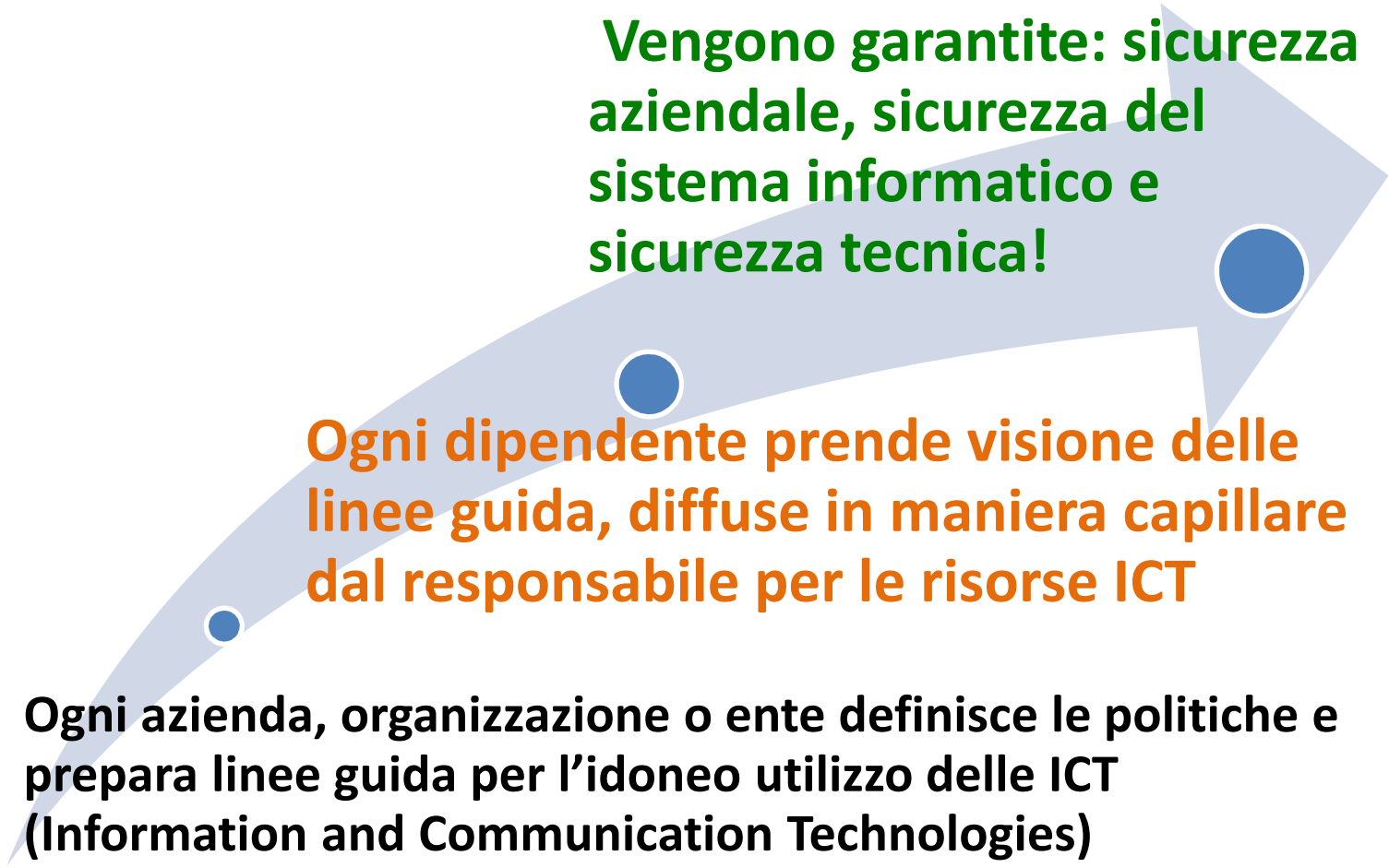
Persone o enti che custodiscono dati

Hanno OBBLIGO di conservarli solo fino ai termini previsti e di proteggerli

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.2 VALORE DELLE INFORMAZIONI

Argomento 1.2.6 Comprendere l'importanza di attenersi alle linee guida e alle politiche per l'uso dell'ICT



Vengono garantite: sicurezza aziendale, sicurezza del sistema informatico e sicurezza tecnica!

Ogni dipendente prende visione delle linee guida, diffuse in maniera capillare dal responsabile per le risorse ICT

Ogni azienda, organizzazione o ente definisce le politiche e prepara linee guida per l'idoneo utilizzo delle ICT (Information and Communication Technologies)

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.3 SICUREZZA PERSONALE

Argomento 1.3.1 Comprendere il termine “ingegneria sociale” e le sue implicazioni

INGEGNERIA SOCIALE (social engineering)

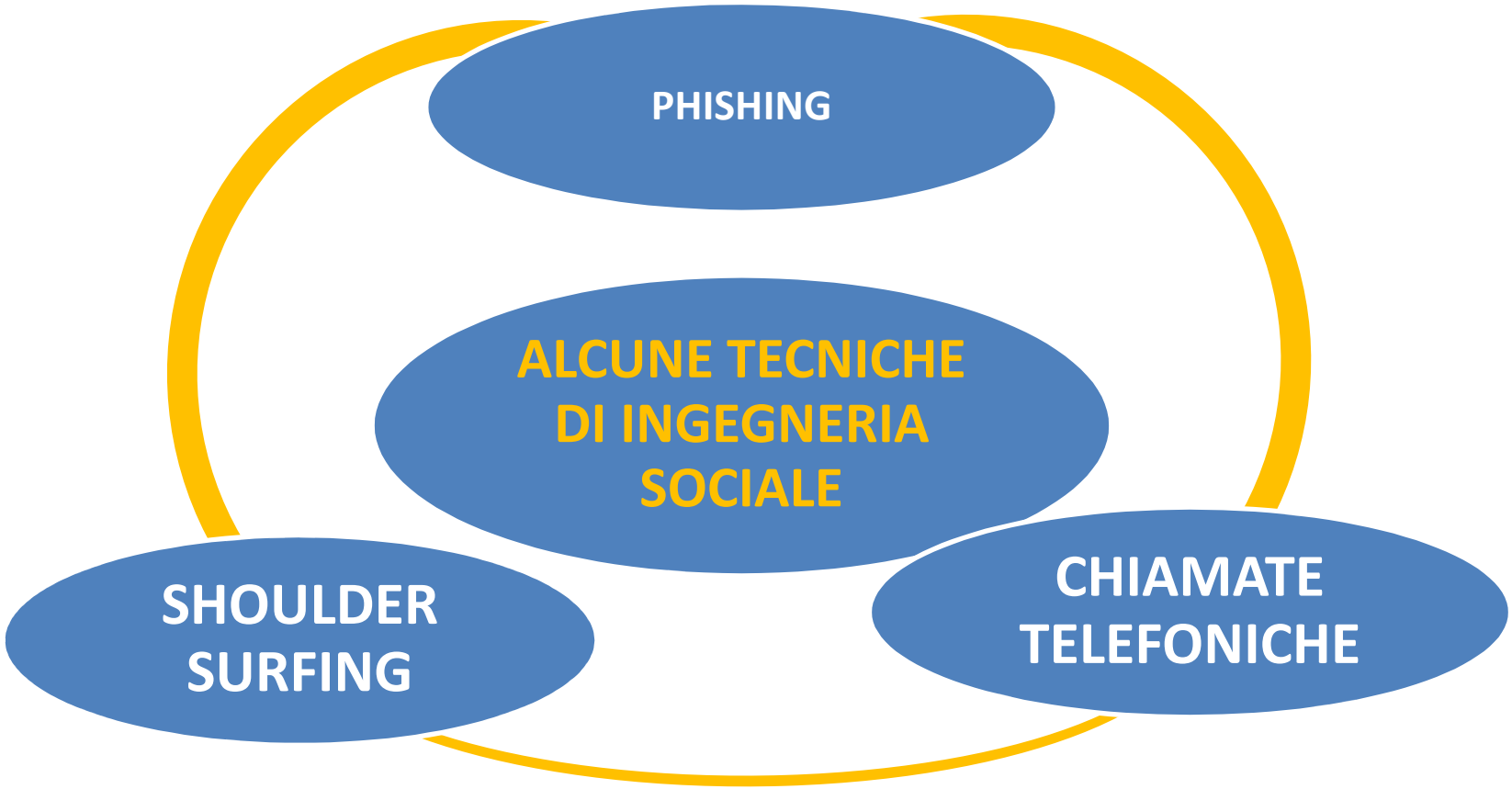
Studio del comportamento del singolo individuo allo scopo di carpirne informazioni riservate.

Non usa solo le moderne ICT, ma anche tecniche più tradizionali, quali contatto diretto, truffe telefoniche, porta a porta, …

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.3 SICUREZZA PERSONALE

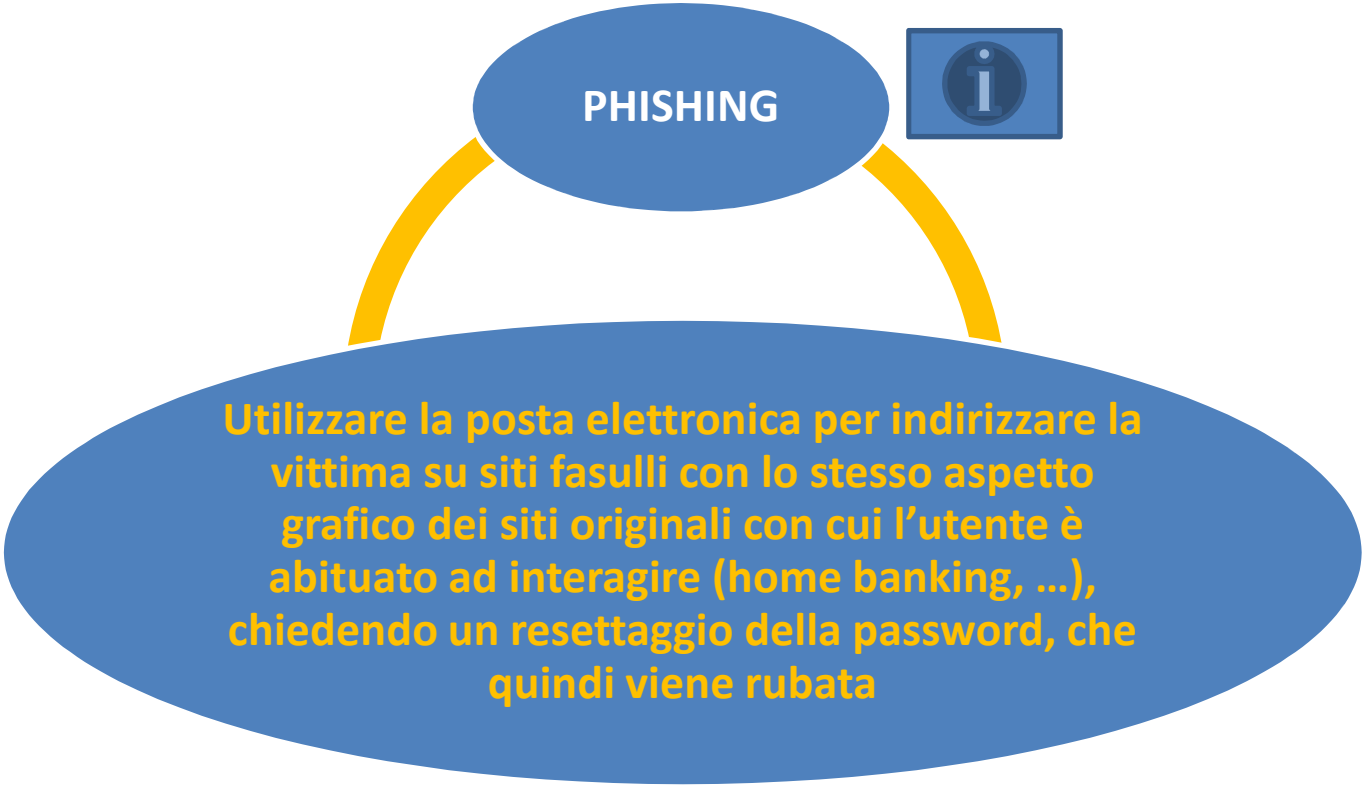
Argomento 1.3.2 Identificare i metodi applicati dall'ingegneria sociale al fine di carpire informazioni personali



SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.3 SICUREZZA PERSONALE

Argomento 1.3.2 Identificare i metodi applicati dall'ingegneria sociale al fine di carpire informazioni personali



SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.3 SICUREZZA PERSONALE

Argomento 1.3.2 Identificare i metodi applicati dall'ingegneria sociale al fine di carpire informazioni personali

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.3 SICUREZZA PERSONALE

Argomento 1.3.2 Identificare i metodi applicati dall'ingegneria sociale al fine di carpire informazioni personali

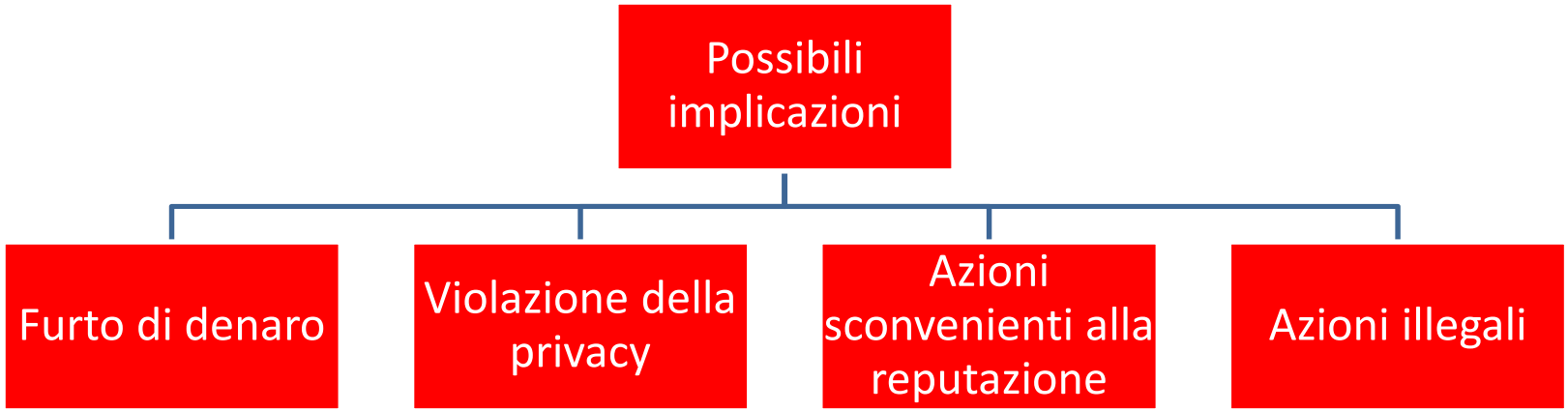
SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.3 SICUREZZA PERSONALE

Argomento 1.3.3 Comprendere il termine “furto d’identità” e le sue implicazioni

FURTO D’IDENTITÀ

Acquisizione dell’identità di un soggetto (tramite appropriazione indebita di credenziali di accesso ad un servizio), compiendo azioni illecite in suo nome



SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.3 SICUREZZA PERSONALE

Argomento 1.3.4 Identificare i metodi applicati per il furto d'identità

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.3 SICUREZZA PERSONALE

Argomento 1.3.4 Identificare i metodi applicati per il furto d'identità

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.3 SICUREZZA PERSONALE

Argomento 1.3.4 Identificare i metodi applicati per il furto d'identità

SKIMMING

Utilizzare particolari dispositivi hardware (skimmer) in grado di leggere la banda magnetica dei badge di carte di credito o bancomat.

Riproduzione skimmer da tavolo. Opportunamente modificato può essere fraudolentemente applicato sulla feritoia degli sportelli bancomat

SEZIONE 1 – CONCETTI DI SICUREZZA

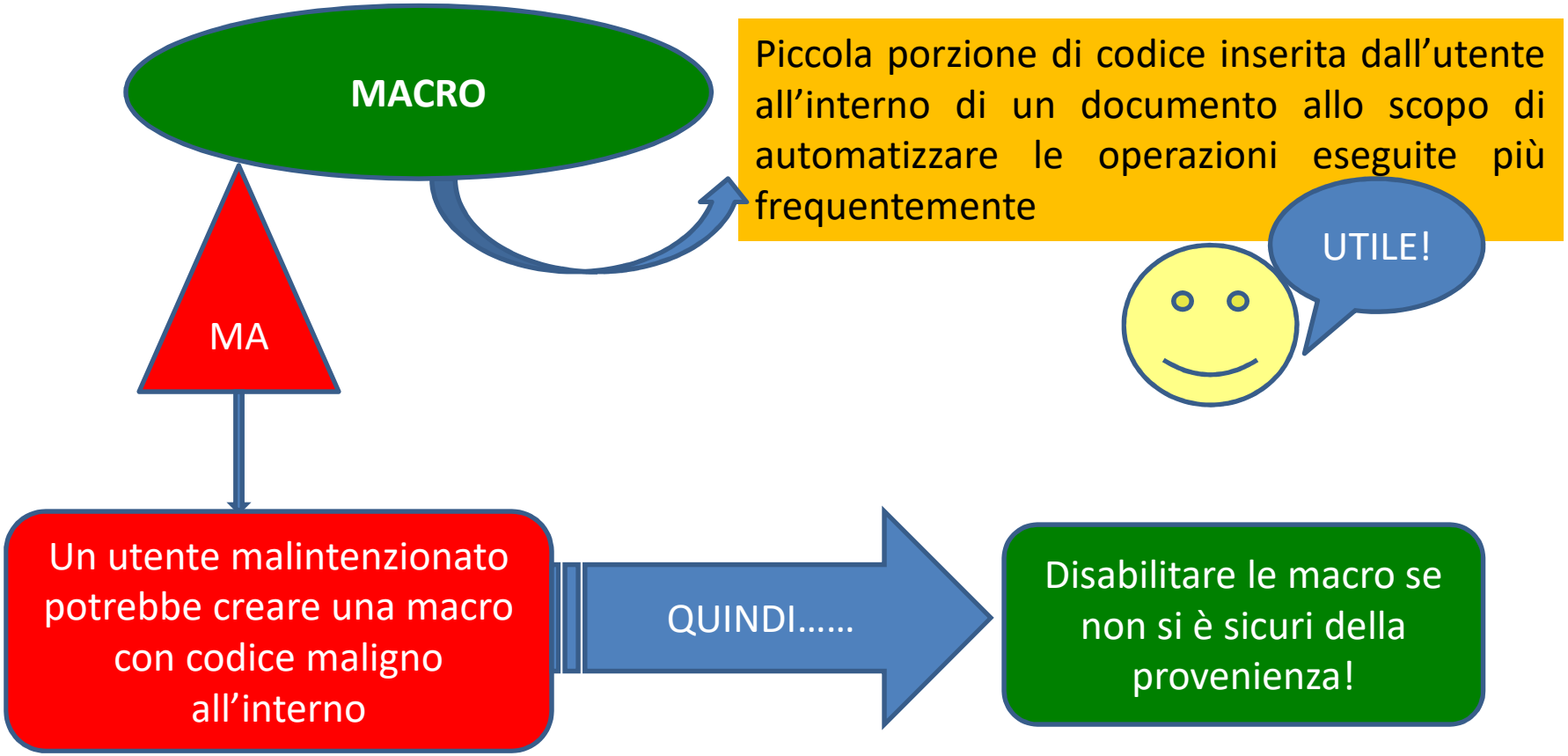
TEMA 1.3 SICUREZZA PERSONALE

Argomento 1.3.4 Identificare i metodi applicati per il furto d'identità

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.4 SICUREZZA DEI FILE

Argomento 1.4.1 Comprendere gli effetti di attivare/disattivare le impostazioni di sicurezza relative alle macro



N.B. ESEMPIO: estensione .xlsm (m sta per macro! In un file di MS Excel)

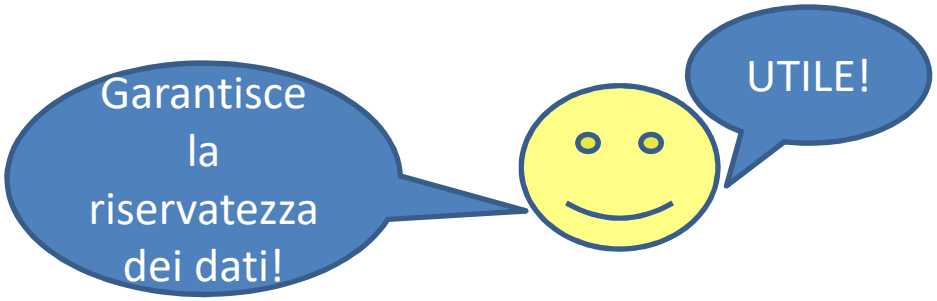
SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.4 SICUREZZA DEI FILE

Argomento 1.4.2 Comprendere significato, vantaggi e limiti della cifratura

CIFRATURA O CRITTOGRAFIA

Procedimento tramite il quale uno o più soggetti possono rendere incomprensibile a terzi il contenuto di un file o di un messaggio o, più in generale, dati e informazioni



ATTENZIONE!

Se si perde la chiave il messaggio non è più decifrabile!

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.4 SICUREZZA DEI FILE

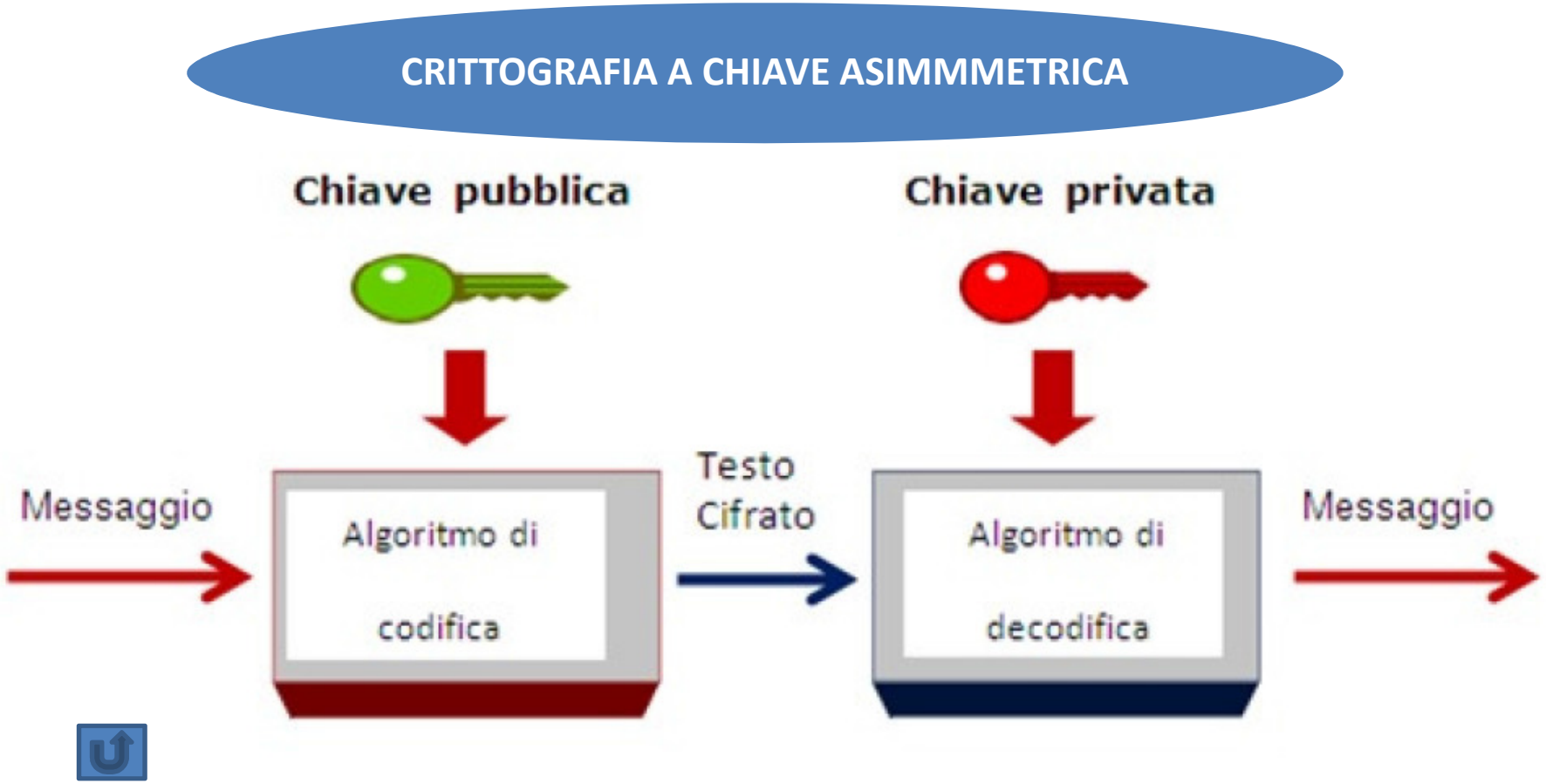
Argomento 1.4.2 Comprendere significato, vantaggi e limiti della cifratura

CRITTOGRAFIA A CHIAVE SIMMMETRICA

SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.4 SICUREZZA DEI FILE

Argomento 1.4.2 Comprendere significato, vantaggi e limiti della cifratura



SEZIONE 1 – CONCETTI DI SICUREZZA

TEMA 1.4 SICUREZZA DEI FILE

Argomento 1.4.2 Comprendere significato, vantaggi e limiti della cifratura

LIMITI

La chiave deve essere casuale, non deducibile da elaborazioni statistiche.

L a chiave deve avere una lunghezza adeguata per contrastare gli attacchi di “forza bruta” (le chiavi moderne vanno da 128 a 512 bit)

La chiave deve essere distribuita in sicurezza. Non intercettabile!