



«I sabati di AICIM»

La Cybersecurity nel processo di digitalizzazione di una PMI

18 marzo 2023
h. 10-12

10.00: Apertura lavori

Gianmarco Biagi, Presidente AICIM-AISOM e Holding 7p9

10.10: consapevolezza e sviluppo della sicurezza informatica nelle PMI

Michele Vanzi, Coordinatore Team Innovazione & ITC,
Founder Michele Vanzi&Partners

10.20: studio ed attuazione di un progetto di sicurezza informatica

Giulio Valeri, Founder Software Solutions S.r.l.

10.35: implementazione di sistemi per la protezione dei dati: aspetti legali ed operativi

Maria Clara Piatti, Innovaton Manager / **William Di Cicco**, Avvocato

10.55: Le insidie informatiche di oggi e di domani: come difendersi

Giorgio Sbaraglia, Information & Cyber Security Advisor | DPO
| Docente 24 Ore Business School | Comitato Direttivo CLUSIT

11:55: Q&A - conclusione

William Di Cicco

Avvocato

Consulente d'impresa – DPO - Auditor



Implementazione di sistemi per la protezione dei dati: aspetti legali ed operativi

QUALI DATI PROTEGGERE

- ➔ «**DATI PERSONALI**»: informazioni riguardanti una persona fisica identificata o identificabile («interessato»),
p.es. nome, codice fiscale, email, stato di salute, situazione familiare, provvedimenti giudiziari, ecc.
- ➔ «**INFORMAZIONI AZIENDALI RISERVATE**»: rappresentano il valore distintivo e originale dell'organizzazione e le chiavi strategiche per raggiungere i propri obiettivi
p.es. processi, notizie attinenti all'organizzazione e ai metodi di produzione, campionari, brevetti, marchi, know-how, offerte riservate, ecc.

QUALI REGOLE E CONSEGUENZE 1/2

DATI PERSONALI

Regolamento UE 2016/679 (GDPR)



sanzioni pecuniarie fino a 10 o 20 milioni, o per le imprese, fino al 2% o 4% del fatturato mondiale totale annuo



Richiesta di
risarcimento danni



Lesione
reputazione
aziendale

QUALI REGOLE E CONSEGUENZE 2/2

INFORMAZIONI AZIENDALI RISERVATE

Codice della proprietà industriale / Disciplina concorrenza sleale



**Danno economico e
commerciale**



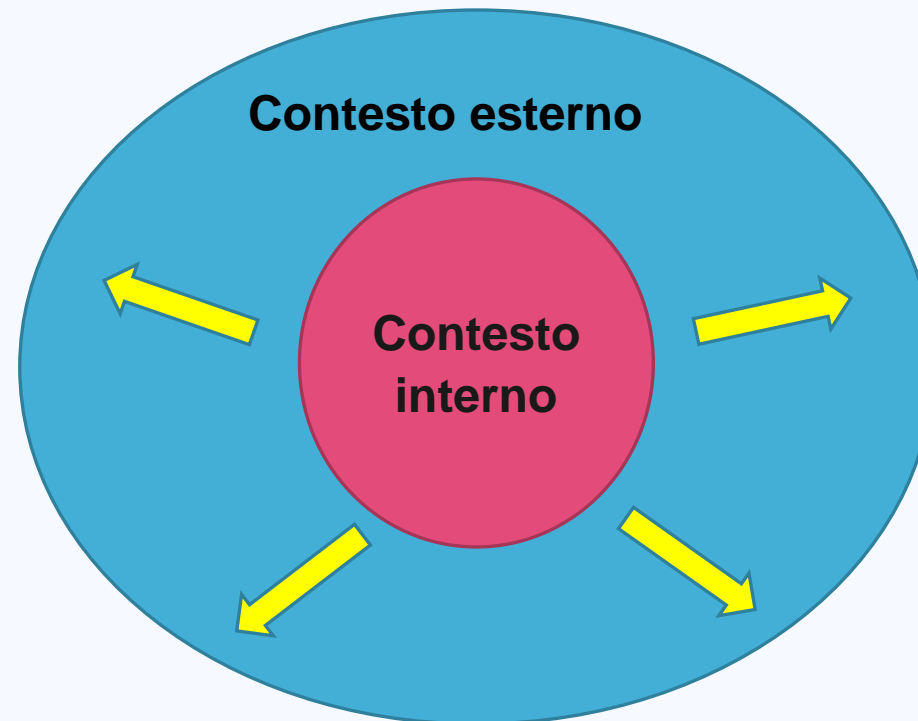
**Obiettivi non raggiunti e
perdita valore distintivo
dell'azienda**



**Lesione
reputazione
aziendale**

PERIMETRO DI SICUREZZA

**ALLARGARE IL PERIMETRO DI ATTENZIONE ANCHE AL CONTESTO
ESTERNO DELL'AZIENDA, NON SOLO A QUELLO INTERNO**



CONTESTO INTERNO 1/3

ORGANIGRAMMA E FUNZIONI INTERNE (chi fa cosa)

- Definire e identificare le mansioni e i compiti del personale (p.es. nel contratto di assunzione e nella nomina come incaricato al trattamento);
- Determinare quali dati e informazioni possono / devono trattare i lavoratori (p.es. limitare accesso a determinate cartelle, file o schedari);
- Definire e aggiornare l'organigramma e comunicarlo adeguatamente
- Deleghe di funzioni chiare e dettagliate
- Stabilire regole chiare, funzionali ed efficaci (p.es. regolamenti interni, codici disciplinari, codici etici, policy, procedure, sistemi di gestione)

CONTESTO INTERNO 2/3

FORMAZIONE – INFORMAZIONE - CONSAPEVOLEZZA

- Formare e informare il personale
- Prevedere degli strumenti per misurare l'efficacia della formazione e la consapevolezza del personale (p.es. survey, test di apprendimento della formazione, audit interni)
- Registro e mappatura dei processi in cui sono trattati dati personali e le informazioni aziendali
- Attenzionare anche l'attività sui social, app e chat

CONTESTO INTERNO 3/3

REGOLARIZZARE I SISTEMI DA CUI PUÒ DERIVARE UN CONTROLLO A DISTANZA DEI LAVORATORI (p.es. videosorveglianza, monitoraggio navigazioni web, log di sistema, GPS, Tag RFID)

- Solo per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale
- Necessario accordo collettivo con rappresentanza sindacale unitaria (RSU) o rappresentanze sindacali aziendali (RSA)
- In mancanza di accordo sindacale, necessaria autorizzazione Ispettorato del lavoro
- Non necessario per strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e per la registrazione degli accessi e delle presenze
- Le informazioni raccolte sono utilizzabili per fini connessi al rapporto di lavoro se data adeguata informazione al lavoratore

CONTESTO ESTERNO 1/4

Fornitori – Partner commerciali – Collaboratori – Consulenti

- Aggiornare periodicamente l'elenco dei soggetti esterni a cui vengono trasmessi i dati
- Sceglierli non solo in base alle competenze tecniche e all'offerta economica, ma anche sulla serietà e attenzione nella gestione dei propri dati
- Verificare periodicamente la loro competenza e solidità (p.es. invio di questionari)
- Nominarli responsabili del trattamento (se trattano dati personali per vostro conto)
- Indicargli le misure minime da adottare a protezione dei dati (personali e non) e prevedere clausole e penali in caso di violazione (p.es. clausole risolutive del contratto)
- Stabilire clausole di riservatezza nei contratti e accordi commerciali

CONTESTO ESTERNO 2/4 FOCUS SERVIZI IT

Fornitori di servizi informatici

(p.es. cloud, account mail, help-desk, gestione sito web, server dedicati, ecc.)

Cosa verificare nei contratti:

- Cosa accade ai dati alla cessazione del rapporto contrattuale?
- Dove si trovano i server dove sono conservati i dati (p.es. trasferimenti extra-UE, presenza di subappaltatori del fornitore)?
- Il fornitore può monitorare l'utilizzo che fate dei servizi o può accedere e trattare i vostri dati? Come e cosa può vedere?
- È possibile effettuare verifiche, test o chiedere garanzie al fornitore, anche da parte di nostri tecnici di fiducia?
- Com'è la reputazione del fornitore? Ci sono stati episodi o eventi critici (p.es. notizie di perdite di dati, problemi societari, inchieste)?
- Il fornitore presenta garanzie di rispetto del GDPR) e degli standard di sicurezza riconosciuti (p.es. certificazione ISO 27001)?
- Il contratto prevede l'obbligo del fornitore di segnalare tempestivamente e in modo circostanziato eventuali violazioni dei dati (data breach)?
- È prevista la possibilità di richiedere la copia dei nostri dati in un formato facilmente fruibile (portabilità dei dati), ad esempio per poterli trasferire facilmente su altro servizio senza rischiare di perdere i dati o doverli ricaricare?

CONTESTO ESTERNO 3/4 FOCUS SERVIZI IT

Fornitori di servizi informatici

ATTENZIONE Esempio di clausola standard di un fornitore di servizi cloud in cui non sono previsti alcuni servizi utili

[il fornitore], salvo che tale operazione non sia espressamente ricompresa e prevista dal Servizio acquistato non effettua nessun backup specifico dei dati e/o informazioni e/o contenuti trattati dal Cliente, per se o per terzi o da questi ultimi se autorizzati dal Cliente, nell'infrastruttura virtuale ad eccezione del backup su tutto il contenuto degli storage che [il fornitore], per sua cautela, effettua periodicamente ai fini dell'eventuale ripristino del Servizio; ciò non solleva tuttavia il Cliente dall'effettuare il backup completo dei dati e/o informazioni e/o contenuti da egli immessi e/o trattati nell'Infrastruttura virtuale e dal prendere tutte le necessarie misure di sicurezza per la salvaguardia dei medesimi. [il fornitore] in ogni caso non offre alcuna garanzia relativamente all'utilizzo del Servizio per quanto riguarda la tutela e la conservazione dei suddetti dati e/o informazioni e/o contenuti, salva l'attivazione da parte del Cliente di specifico servizio accessorio

CONTESTO ESTERNO 4/4 FOCUS SERVIZI IT

Fornitori di servizi informatici

Verificare se il fornitore offre garanzie di sicurezza e tutti i servizi a voi necessari.

Non scegliere solo in base al costo!

GRAZIE PER L'ATTENZIONE!

Avv. William Di Cicco

w.dicicco@legalevda.it

www.legalevda.it

Tel. +39 0668136714

