UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Pianificazione e gestione Data Breach: case study

Annalisa Madeo

Morolabs S.r.l.

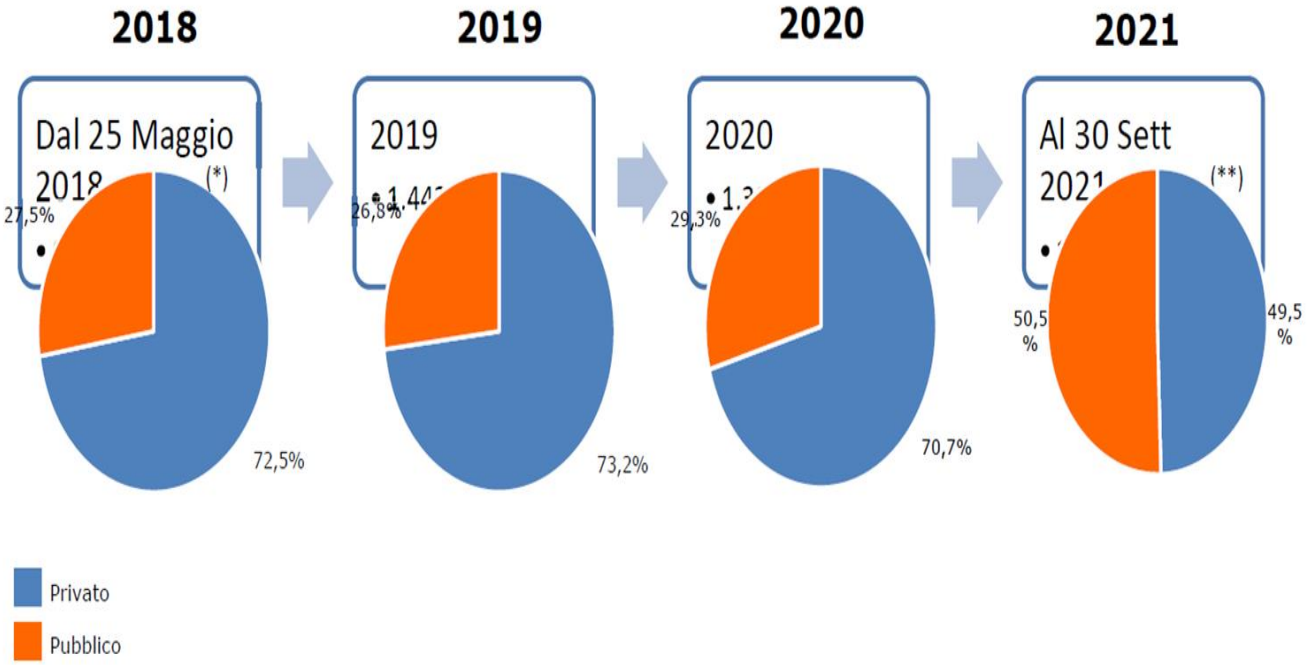
madeo.annalisa@yahoo.com

Martedì 19 Luglio 2022

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

VIOLAZIONE DEI DATI PERSONALI (DATA BREACH) art. 4, punto 12 GDPR

Boom di notifiche di Data Breach



Boom di notifiche di Data Breach

25 1997-2022 | GPDP
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

RELAZIONE ANNUALE
2021

www.gpdp.it

Cosa può succedere?

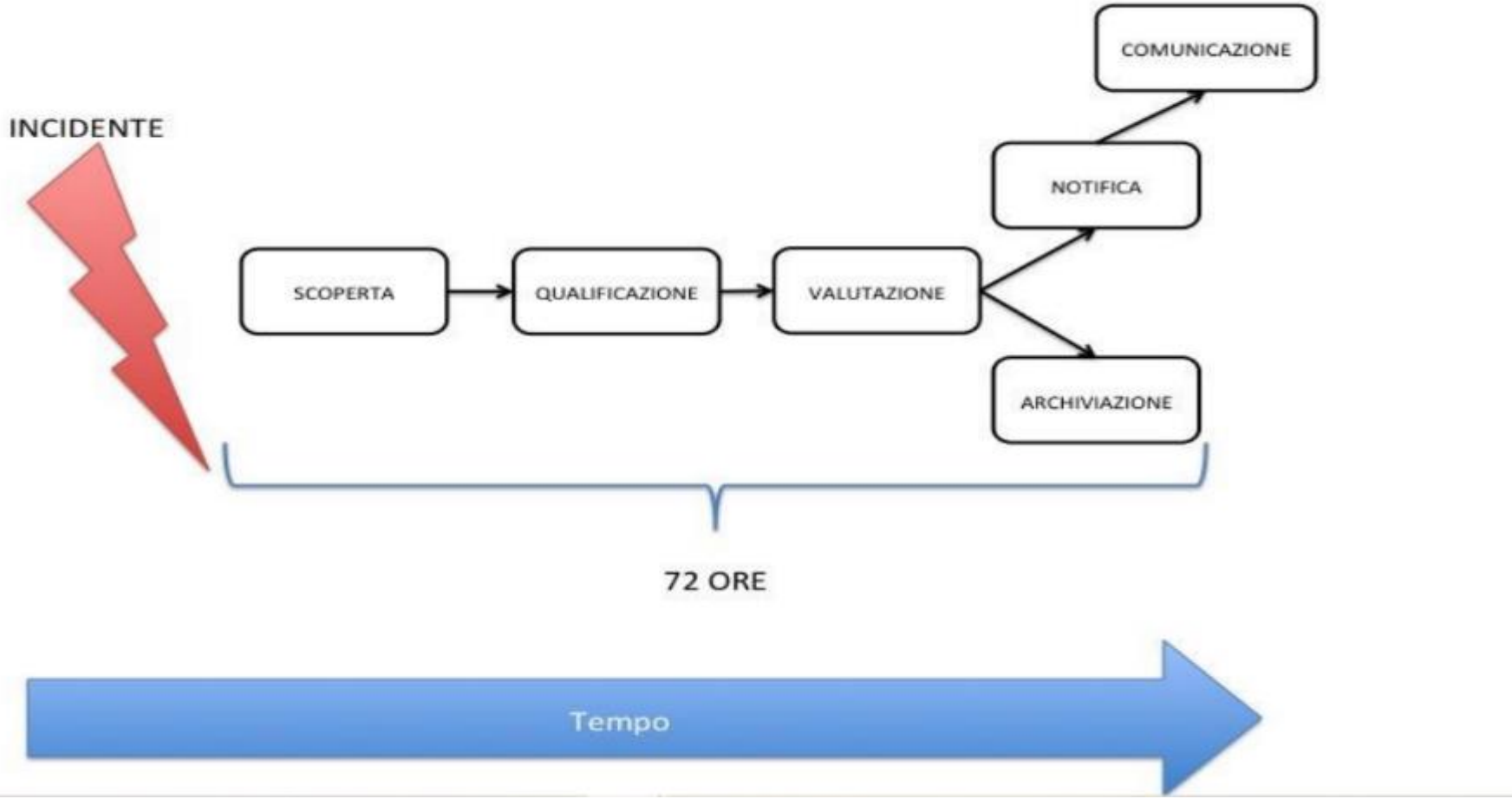
DISTRUZIONE
I dati personali non esistono più

DANNEGGIAMENTO
I dati personali sono stati modificati, corrotti o sono incompleti

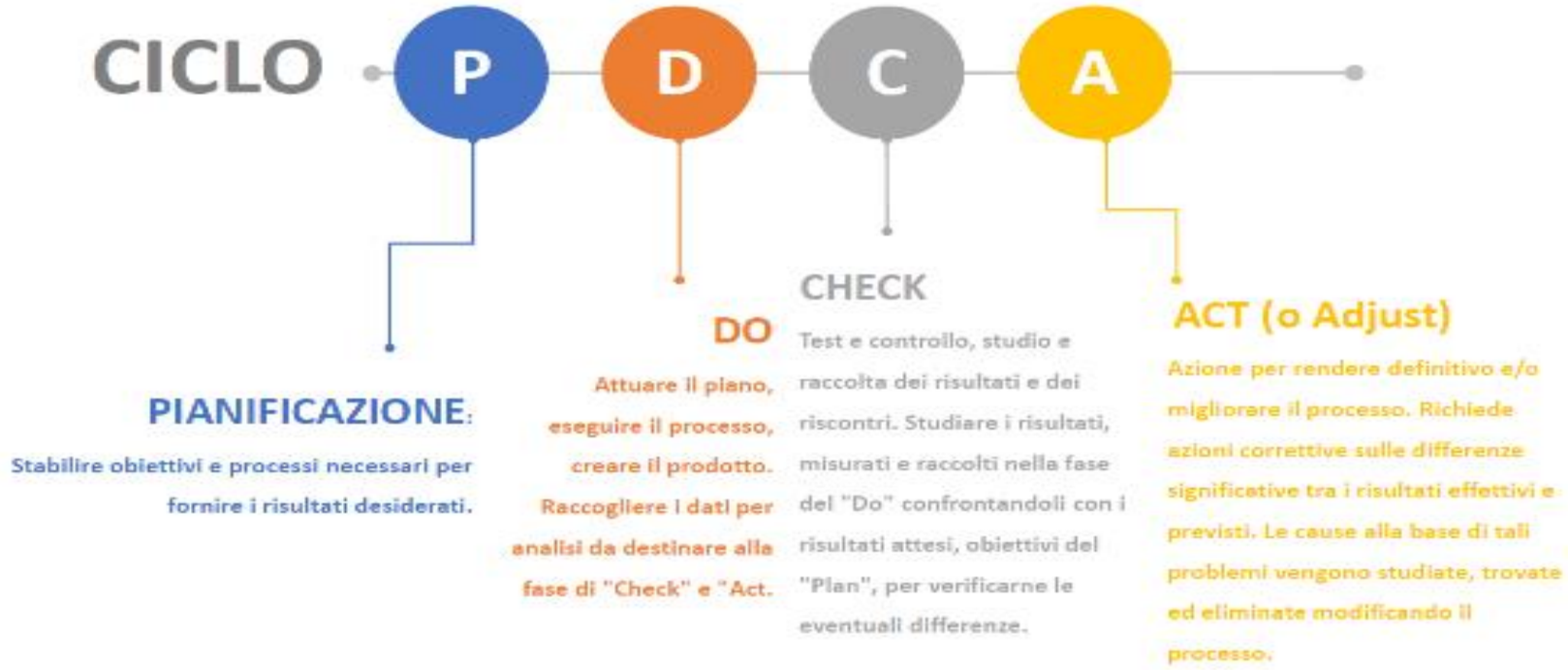
PERDITA
Perso il controllo, l'accesso o la disponibilità

TRATTAMENTO NON AUTORIZZATO O ILLECITO
Qualsiasi forma di trattamento in violazione del regolamento (divulgazione o accesso)

Pianificazione e gestione

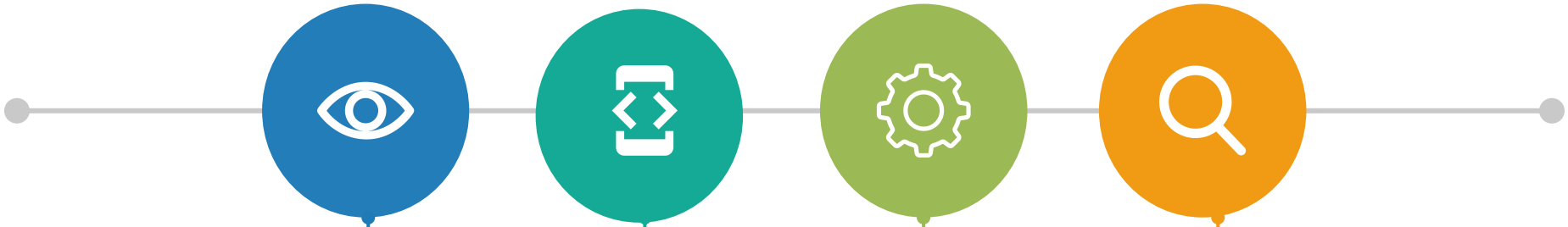


Approccio proattivo



Ruolo del dpo

Nella gestione dei data breach



FORNISCE CONSULENZA SULLA NECESSITÀ DELLA NOTIFICA DI VIOLAZIONE DEI DATI PERSONALI, OVE RICHIESTO

RACCOMANDA MISURE DI MITIGAZIONE

PUNTO DI CONTATTO PER GLI INTERESSATI E PER L'AUTORITÀ

COLLABORARE CON I RESPONSABILI DELLA SICUREZZA SULLA GESTIONE DEI RISCHI COLLABORA NELLA REDAZIONE E AGGIORNAMENTO DELLA POLITICA DI GESTIONE DELLE VIOLAZIONI DEI DATI

Incident response

processo coordinato per reagire alle conseguente di un incidente alla sicurezza, finalizzato al ripristino dell'operatività e articolato in:

Discovery

Determinare se vi è stata una violazione (potrebbe provenire da aree diverse)

Investigation

Contenere la violazione (per evitare propagazioni e danni), acquisire evidenze

Eradication

Eliminare le cause della violazione Porre tutto in massima sicurezza

Recovery

Ripristino e riattivazione dei servizi dell' organizzazione

Resolution

Lessons Learned Documentare violazione e rafforzare con misure tecniche e organizzative

Incident response

Le domande da porre/porsi

Discovery

Quando è avvenuto l'evento?
Come è stato scoperto?
Chi l'ha scoperto?
Sono state interessate altre aree?
Qual è la portata della compromissione?
Influisce sulle operazioni?
È stata scoperto il punto di ingresso?

Investigation

Cosa è stato subito fatto per contenere la violazione?
Cosa si è fatto per contenere a lungo termine? Abbiamo evidenze?
Abbiamo backup?
Accessi solo con 2FA?
Verificate le credenziali di accesso? Sono state modificate?
patch e aggiornamenti di sicurezza recenti?

Eradication

Le cause e gli strumenti dell'attaccante sono stati rimossi? in modo sicuro?
Il sistema è stato rafforzato, applicate le patch e aggiornato?
Sono stati attivati strumenti di verifica di comportamenti anomali di persone o sistemi?
È attivo un SOC?

Recovery

Quando è possibile tornare in produzione?
Tutto testato?
Abbiamo ripristinato tutti i dati o gestito la finestra dei dati persi?
Continueremo a monitorare i sistemi?
Quali strumenti garantiranno che attacchi simili non si ripetano?

Resolution

Quali misure di sicurezza necessitiamo?
Cosa dobbiamo fare per la consapevolezza degli operatori?
Quale è il punto debole sfruttato nella violazione?
Come assicuriamo che una violazione simile non si ripeta?

Dal data breach al provvedimento

illiceità dei trattamenti di dati personali effettuati dall'Azienda, in violazione dei principi di integrità e riservatezza e degli obblighi del titolare del trattamento in materia di sicurezza del trattamento e di valutazione d'impatto sulla protezione dei dati.

ASUR Marche
€ 14.000

Notizia stampa del 6 gennaio 2021
L'Organizzazione veniva a conoscenza della violazione da un articolo pubblicato in una testata giornalistica che evidenziava una vulnerabilità nel sistema di acquisizione e gestione dei dati dello screening del Covid-19, in relazione alla possibilità di accesso da parte di malintenzionati ai dati personali degli assistiti dell'ASUR. Attraverso l'App , era possibile leggere il Codice Qr presente sul talloncino rilasciato a chiunque si era sottoposto allo screening per Covid-19, al fine di consultare il proprio esito tampone. Il codice era elaborato in maniera progressiva che permetteva di accedere senza particolari difficoltà.

Contesto di emergenza sanitaria – Operazione screening di massa

AV 5 – modalità di prenotazione differente (piattaforma https://www.cureprimarie.it - sezione “Screening popolazione di San Benedetto del Tronto" e APP mobile “Smart4you" (funzione di lettura del QR-code generato sequenzialmente con una associazione diretta partecipante esito-tampone)

Rilascio di un indirizzo e-mail e un numero di cellulare valido per ricevere la notifica del risultato

Mancata adozione di una codifica complessa (APP) nonché possibilità di decodifica del codice fiscale (piattaforma)

Perdita di riservatezza e di integrità

Episodio determinato da un’azione intenzionale esterna
Forzatura del sistema e accesso abusivo da parte dei 2 soggetti

Notifica nei termini delle 72 ore e successivamente integrata
Memoria difensiva

Misure adottate per
Contenere: protocollo https, log accessi e attività effettuate, monitoraggio dei sistemi, utilizzo QR code per pseudonimizzazione degli esiti tamponi, registrazione tramite invio SMS di parte del codice di attivazione

Rimediare: codifica più complessa di tipo hash ed eliminazione funzionalità SMS; eliminazione della funzionalità di decodifica del C.F. con nominativi assistiti e dell’ SMS con nominativo e esiti (fornitore)

Prevenire: procedura più rigorose nell’acquisizione piattaforme aziendali web, applicativi software nonché delle App mobili

- Utilizzo non conforme degli SMS per comunicare esito tamponi
- Mancata valutazione d’impatto dei trattamenti sulla protezione dei dati personali
- Misure di sicurezza inadeguate
- Falla

Considerazioni generali

ADOZIONE DI PROCEDURE E POLICIES PRIMA DI UN DATA BREACH

MASSIMA ATTENZIONE NELLA CLASSIFICAZIONE DEL DATA BREACH

GOVERNANCE E ALLOCAZIONE RESPONSABILITÀ
COINVOLGERE IL DPO E IL RESPONSABILE DELLA SICUREZZA IT

IMPARARE
DAI PROPRI ERRORI (LESSON LEARNED)

COINVOLGERE IL DPO E IL RESPONSABILE DELLA SICUREZZA IT

INCORAGGIAMENTO A NOTIFICARE

ACCOUNTABILITY

NOTIFICA POSSIBILE IN PIÙ FASI IN FUNZIONE DELLE NOTIZIE ACQUISITE

IL RESPONSABILE EFFETTUA LA NOTIFICA (DA EVITARE)

NOTIFICA EFFETTUATA IN RITARDO (ELEMENTO DI CRITICITÀ)

GRAZIE PER L'ATTENZIONE

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection