Privacy e Cybersecurity: principali rischi e misure tecnico organizzative da adottare

Carlo Guastone, GdL Sicurezza Informatica di Assintel

Milano, 12 marzo 2018

Breve profilo di C. Guastone

- PM Progetti ASDO e COGE Divisioni chimiche Montedison
- PM Progetto Blue Bird Datamont (DR Sistemi ICT in USA)
- Direttore Operativo Datamont (insourcig ICT Montedison)
- Direttore Sistemi Montedison
- Assistente AD Montedison (Finanza e Controllo)
- Direttore generale SIME (Servizi informatici Montedison)
- Progetto internazionalità (Advisor A. Ambrosetti) e Responsabile Progetto SUI, Gruppo Montedison

- Direttore Sistemi Standa
- Direttore Organizzazione e Sviluppo Fininvest
- Direttore Sistemi, Servizi generali e Sicurezza Mediaset
- PM Progetti Y2K, Euro, Sap Mediaset

- VP Business Development Sernet
- Business Manager ICT Governance & Security Sernet

Strategie ed esperienze Assintel

L’ approccio

Cybersecurity e GDPR

Allegato: i 7 step…….

Strategie ed esperienze Assintel

Assintel e la Security

- ✓ Assintel è l'Associazione Nazionale di riferimento delle imprese di **Information & Communication Technology e Digitali**
- ✓ Aderisce a **Confcommercio – Imprese per l'Italia**, la più grande federazione delle imprese del Terziario italiano
- ✓ Rappresenta le piccole, medie e grandi aziende ICT su **tutto il territorio nazionale.**

Focus Security

- ✓ **Gruppo di Lavoro** dedicato e attivo sul tema della sicurezza delle informazioni aziendali, della cyber security e della protezione dei dati
- ✓ **Codice di condotta e linee guida GDPR**
- ✓ **Servizio DPO** per le aziende socie

Gruppo di Lavoro
SICUREZZA INFORMATICA
Assintel

Sicurezza Informatica

Il Gruppo di Lavoro Sicurezza Informatica ASSINTEL è promotore anche di iniziative trasversali affinché possano beneficiarne le imprese di qualsiasi settore merceologico e di ogni dimensione, con particolare attenzione alle MPMI.

Tra le varie iniziative promosse ricordiamo:

✓**Metti al sicuro il tuo Business:** Vademecum per la protezione dei dati per dare agli imprenditori delle pmi concrete indicazioni sulle cose da fare (e non fare) per difendere il business da possibili “violazioni” della sicurezza delle informazioni aziendali.

Il Vademecum è scaricabile gratuitamente dal sito Assintel e dal sito Confcommercio Milano.

Sicurezza Informatica e GDPR

✓**TOOL di auto-assessment in ambito Sicurezza informatica**: un supporto pratico e gratuito a disposizione delle MPMI che hanno così la possibilità di fotografare il proprio «stato di fatto» in tre macro aree generali: organizzazione, servizi e tecnologia.

- ✓ **TOOL di auto-assessment GDPR** per valutare i principali adempimenti che aziende dovranno realizzare entro il 25 maggio 2018. Il Tool sarà disponibile entro la fine di marzo.

- ✓ **Master in Cyber Security & Data Protection** organizzato da Assintel e Business Campus, è finalizzato alla formazione di **professionisti ed esperti** fornendo una visione completa ed esaustiva di ciò che significa occuparsi di Cyber Security e Data Protection in tutte le sue sfaccettature. >> Scopri di più

- ✓ **Sportello Confcommercio Milano GDPR & Privacy** powered by Assintel

I 7 STEP per adempiere al nuovo GDPR

…in Allegato

L’ approccio

Le priorità del business

Approccio interdisciplinare risk based

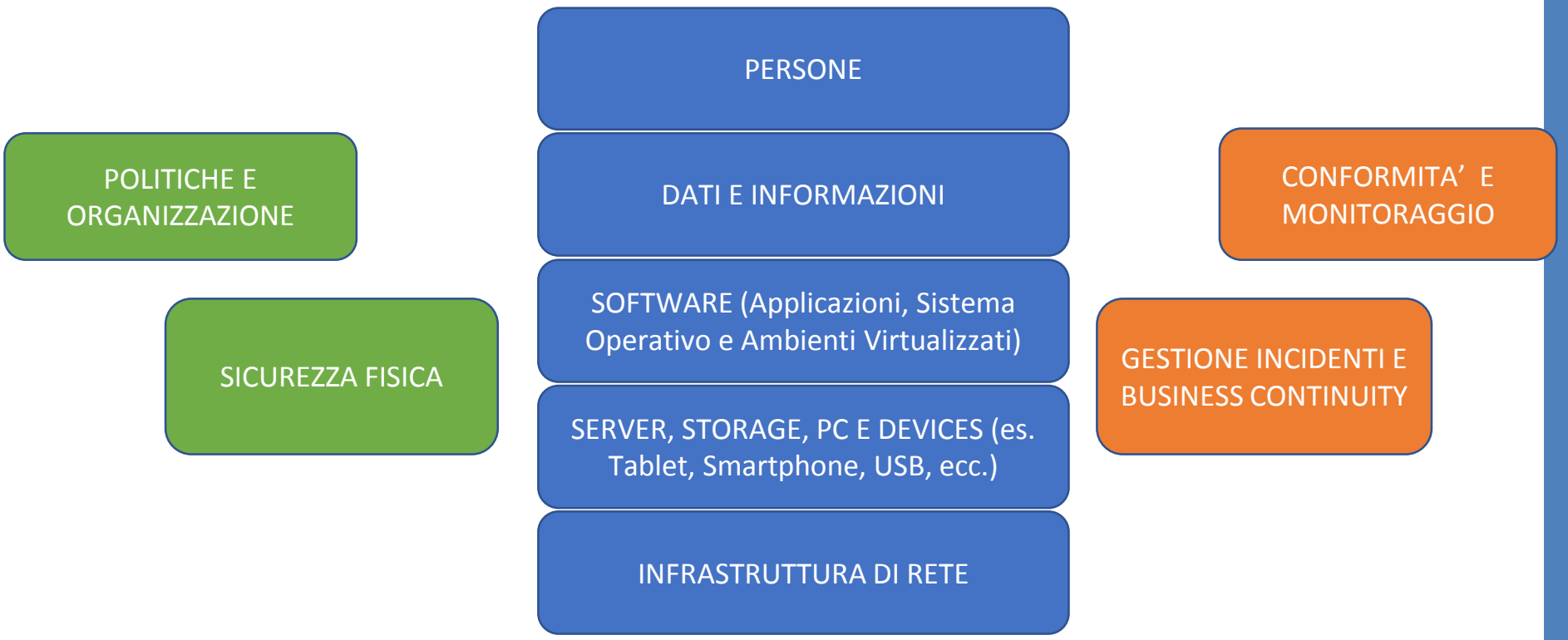
Gruppo di Lavoro
SICUREZZA INFORMATICA
Assintel

Approccio adottato in tutte le iniziative

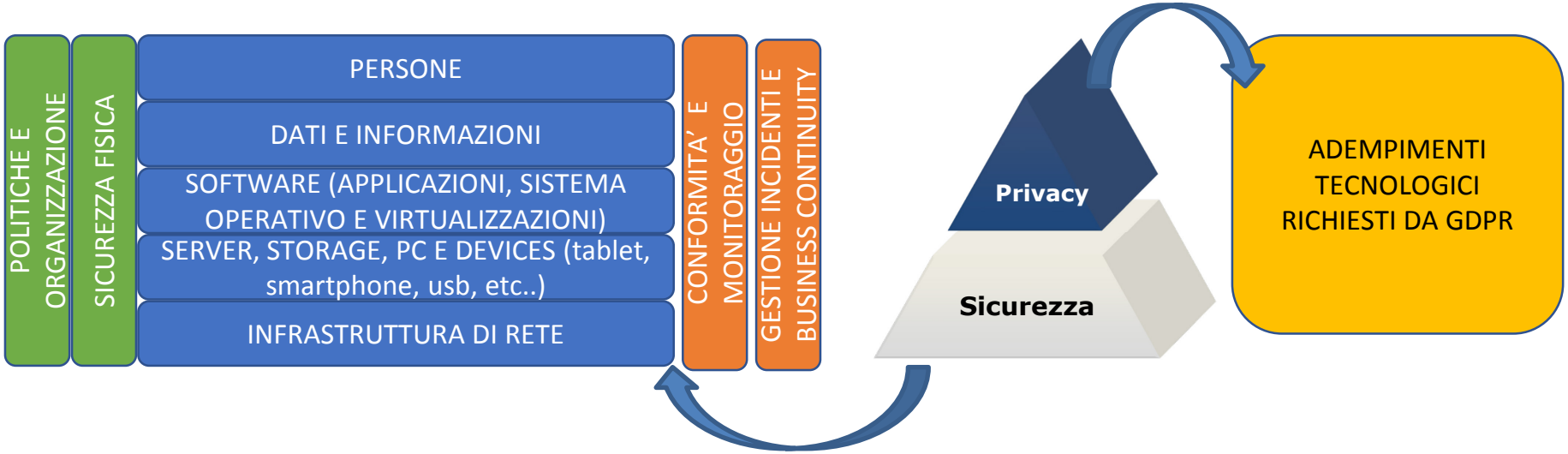
The INTERNATIONAL COUNCIL OF MANAGEMENT CONSULTING INSTITUTES
CMC - GLOBAL

Organismo accreditato per la qualificazione
CMC
CERTIFIED MANAGEMENT CONSULTANT

Le misure di sicurezza



Misure di sicurezza e GDPR



Le Sezioni del Tool di auto-assessment GDPR

L'AZIENDA e I DATI PERSONALI TRATTATI
-7 domande-

IMPATTI E RISCHI DEI TRATTAMENTI
-3 domande-

PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE (by design e by default)
-4 domande-

REGISTRO DEI TRATTAMENTI
-3 domande-

RUOLI, RESPONSABILITA' E PROCEDURE (es. Incidenti di sicurezza)
-17 domande-

MISURE DI SICUREZZA NEI TRATTAMENTI

-13 domande-

RELAZIONI CON I FORNITORI (RESPONSABILI ESTERNI DEI TRATTAMENTI)
-4 domande-

PROFILAZIONE
(es. abitudini di consumo dei clienti, automatizzate su larga scala)
-3 domande-

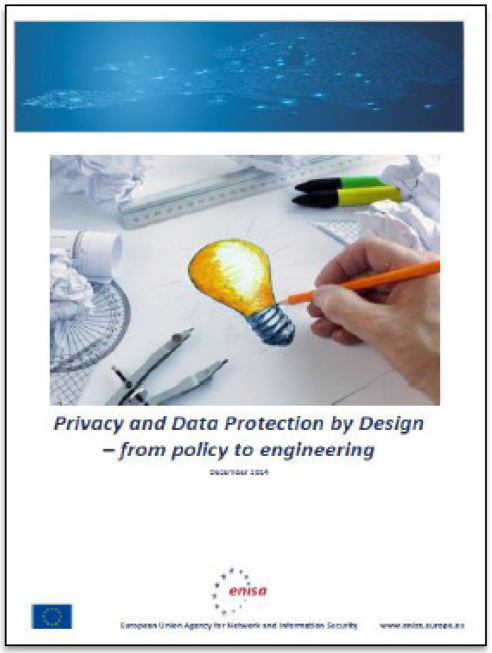
CONSENSO
-4 domande-

PROVVEDIMENTI DEL GARANTE APPLICABILI (es. videosorveglianza)
-8 domande-

PET (Privacy enhanced technologies)-Accenni

«Considerando…» N° 78 di GDRP:

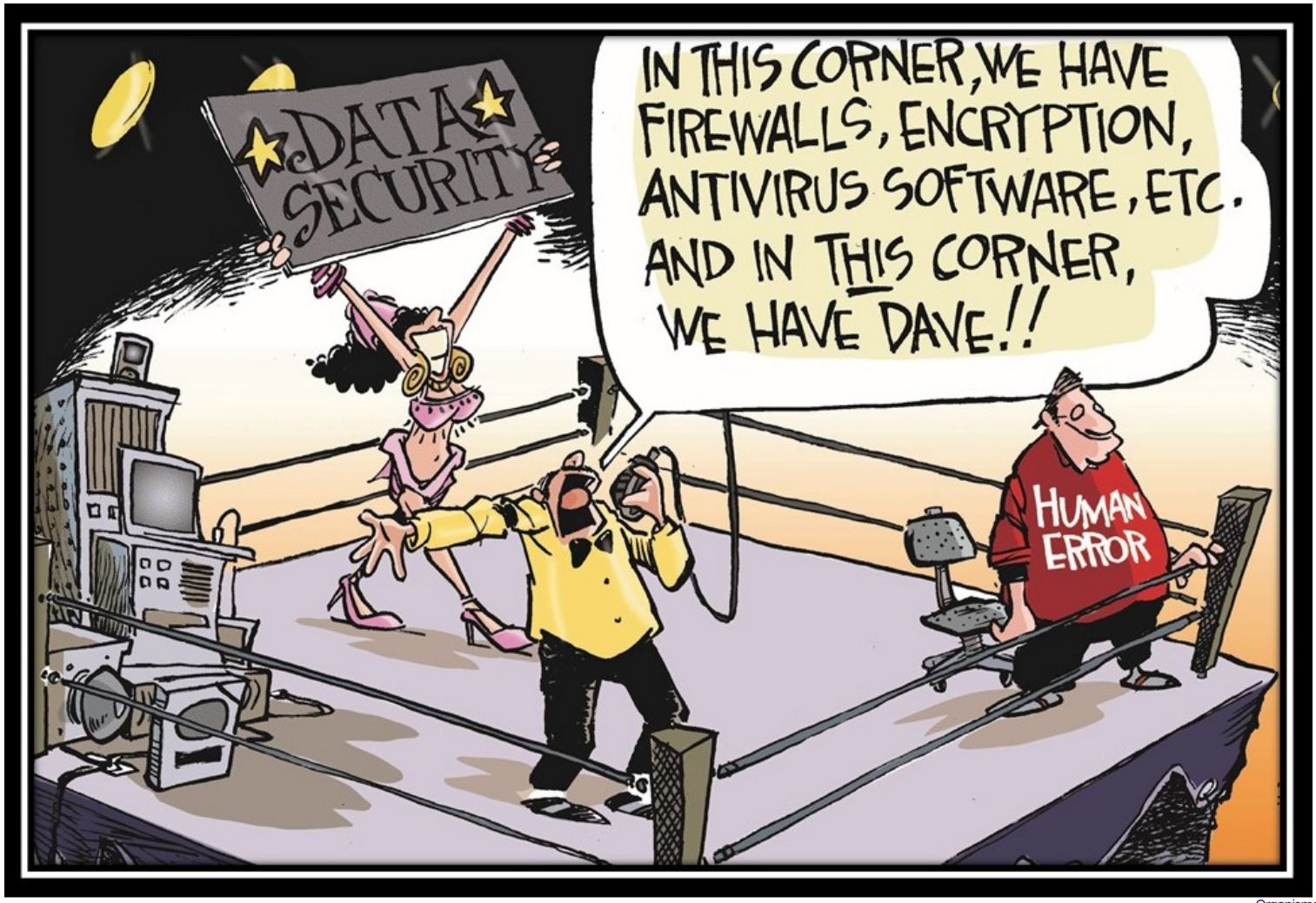
……..**i produttori dei prodotti, dei servizi e delle applicazioni** dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a **far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati…….**



Tecnologie (PET) per ridurre il rischio di violazione dei principi privacy

"Privacy-Enhancing Technologies (PET) is a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system." (ENISA – «Privacy and Data Protection by Design»)

L'importanza del «fattore umano»



Le priorità organizzative

- ✓ Ruoli e responsabilità (gerarchia vs matrice, specializzazione vs interfunzionalità)
- ✓ Project management e Change management
- ✓ Controllo interno e Reporting
- ✓ Sensibilizzazione e Formazione
- ✓ Coaching
- ✓ Team Building
- ✓ Empowerment
- ✓ …….

Sensibilizzazione sulle minacce

Le priorità tecnologiche

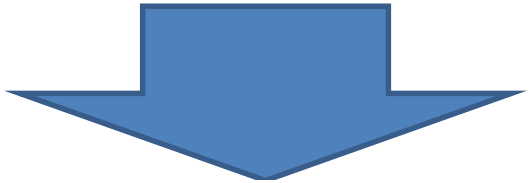
Le misure di protezione tecnologiche vanno individuate:

a. In coerenza con le tipologie dei trattamenti e con le valutazioni di rischio……..

b. Tenendo conto della specificità delle esigenze di sicurezza dei trattamenti di dati personali…….

c. In ottemperanza ai Principi Privacy

d. Applicando la «Privacy by design e by default»



La cybersecurity è una disciplina fondamentale per i trattamenti particolari (art. 9) e per i trattamenti a rischio elevato (es. profilazioni, e-commerce, etc) ma l'equazione **GDPR=Cybersecurity non è uno slogan valido in tutte le aziende.**

La più importante leva per minimizzare i rischi di attacchi di hackers è la adozione di misure di sicurezza di base (es. password forti, reti cifrate, allegati mail protetti, dati personali protetti nelle fasi di test, sensibilizzazione utenti e specialisti IT, back up protetti, etc)

In pratica…….per i siti WEb

- ✓ Utilizzo di canali cifrati per trasmissione dati su reti pubbliche (attenzione ai curricula con dati sensibili…….inviati via Web)

- ✓ Adozione di misure di sicurezza nell'architettura e infrastruttura delle applicazioni web e nella codifica del software:

  - ❑ Adottando linee guida con consigli sulla creazione di applicazioni Internet sicure (es. OWASP), per evitare di introdurre vulnerabilità;

  - ❑ Svolgendo sistematiche istruttorie di vulnerability assessment e penetration test;

  - ❑ Sottoponendo il codice sviluppato a «code review» per identificare bugs e vulnerabilità.

Cybersecurity e GDPR

Framework Nazionale di Cybersecurity

CIS SAPIENZA
Cyber Intelligence and Information Security

2015 Italian Cyber Security Report

Un Framework Nazionale per la Cyber Security

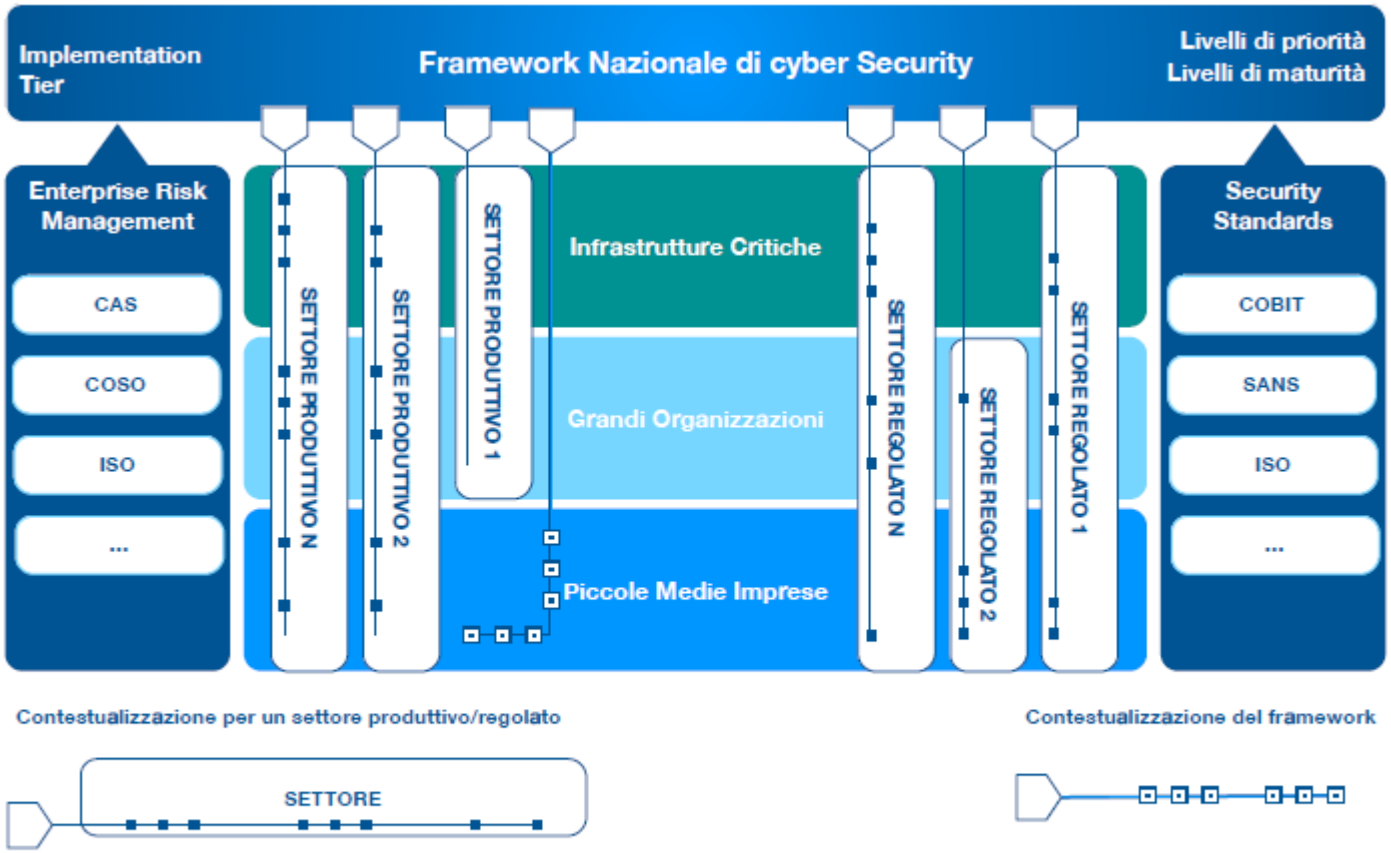
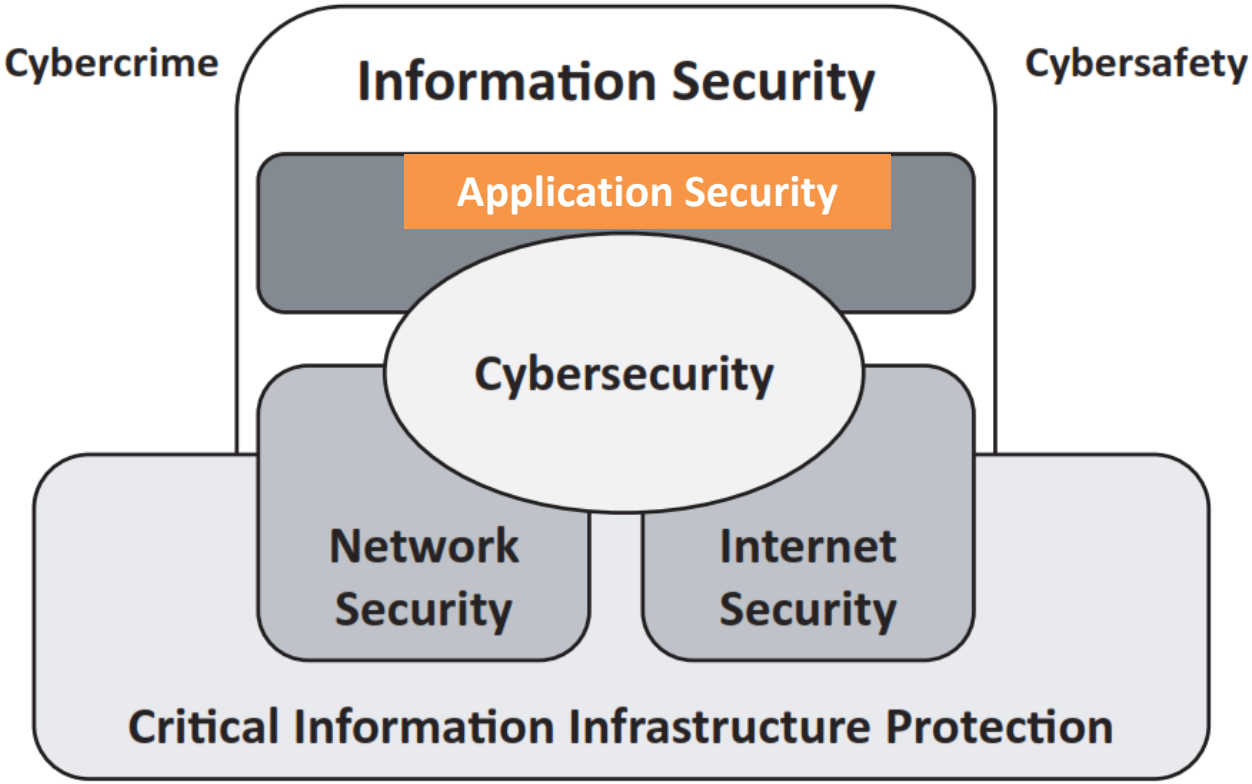


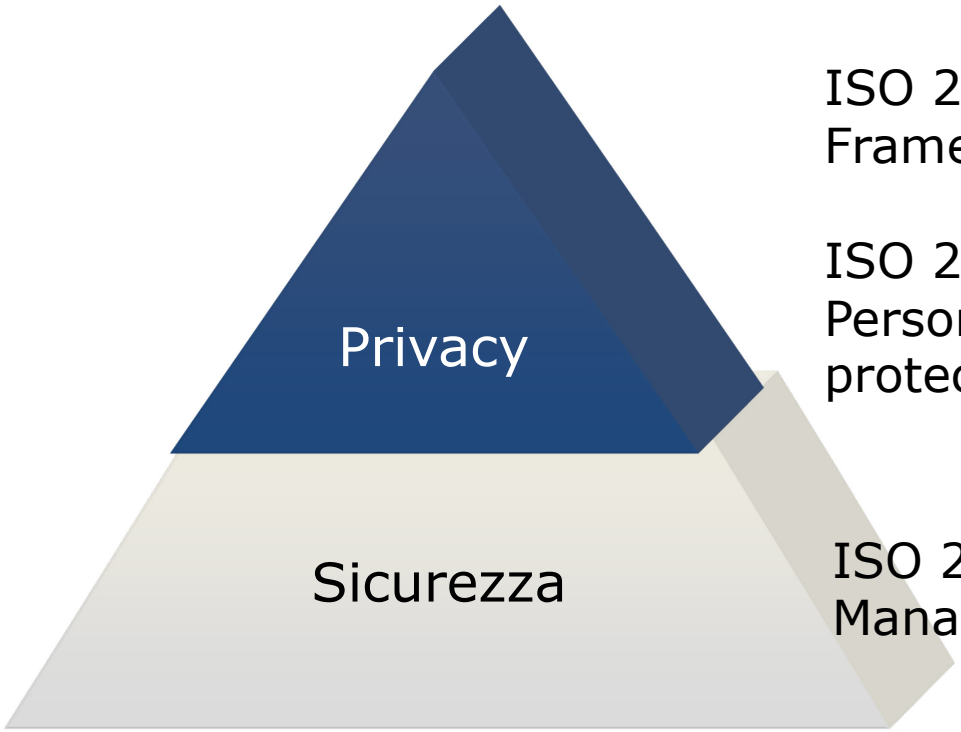
Figura 1.1: Framework nazionale di cyber security e sua relazione con enterprise risk management, standard di sicurezza informatica, dimensione delle imprese e settori produttivi

Cybersecurity e gli altri domini della sicurezza



ISO 27032 – Guidelines for Cybersecurity

GDPR - Gli standard di riferimento



ISO 29100 – 29101 (Privacy Frameworks)

ISO 29151 (Code of Practice for Personally Identified Information protection)

ISO 27001/2 (Information Security Management System)

ISO 29151

Stabilisce obiettivi di controllo, **controlli e linee guida** per l'attuazione dei controlli al fine di soddisfare i requisiti identificati da una valutazione di rischio e di impatto connessi alla protezione dei dati personali.

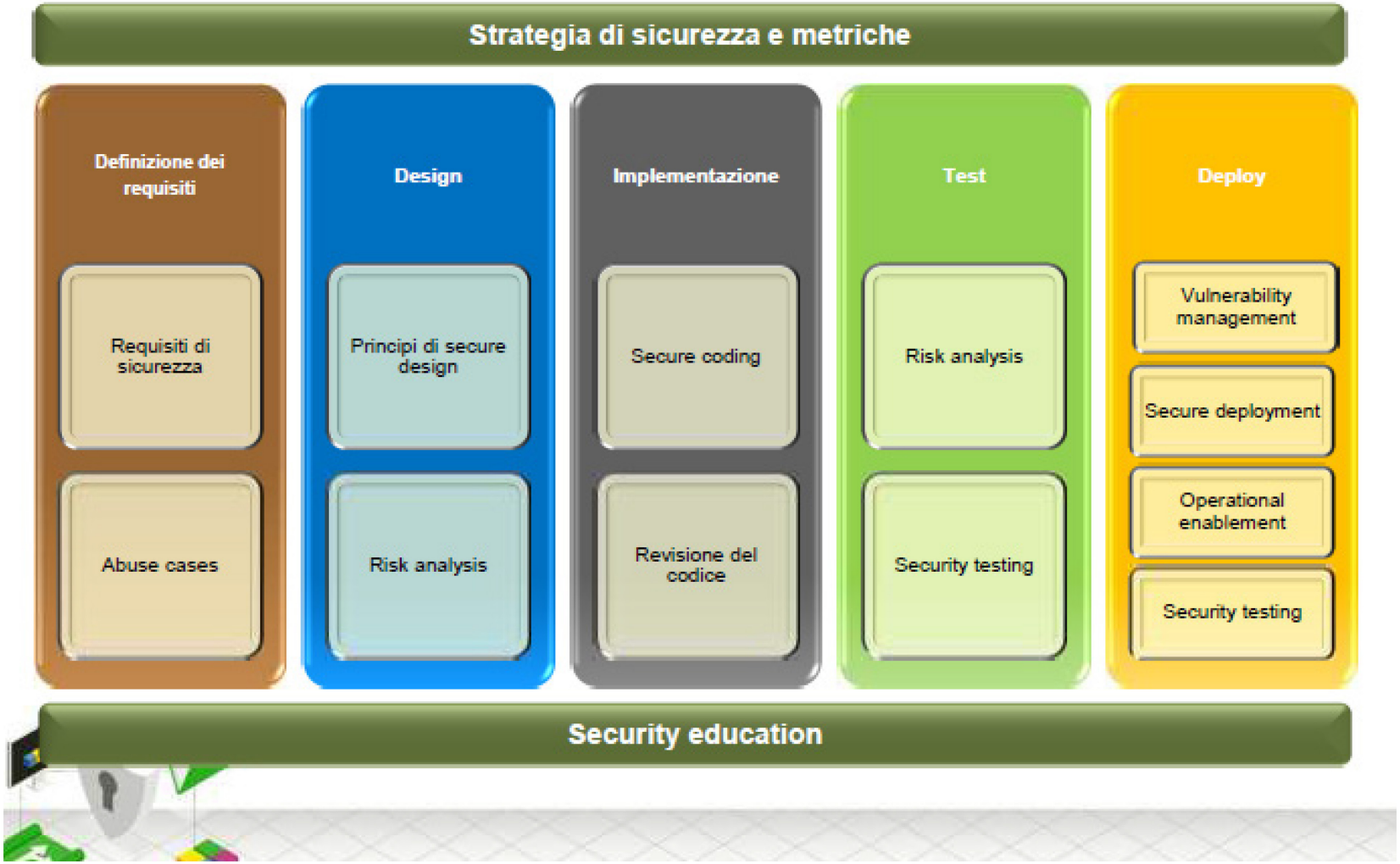
Si basa su ISO 27002, tenendo conto dei requisiti per l'elaborazione di dati personali che possono essere applicabili nel contesto dell'ambiente di rischio di sicurezza di un’azienda.

Application Security

Per sicurezza applicativa si intende la sicurezza delle applicazioni, in modo particolare delle applicazioni web

- Le applicazioni web sono soggette a vulnerabilità che possono comprometterne il funzionamento, permetterne un utilizzo fraudolento, permettere il furto di identità, permettere il furto di informazioni e dati gestiti dalle applicazioni stesse

Security Engineering & Software Development lifecycle



Design

…..circa il 50% dei problemi di sicurezza sono dovuti ad errori architetturali

Secure Coding

Quali sono le principali cause di vulnerabilità del codice?

1. Requisiti di sicurezza non definiti o poco chiari
2. Implementazione errata di requisiti corretti
3. Nella fase di deployment e configurazione non rispecchia i requisiti e le modalità operative previste

Allegato

Abstract

STEP 1: PRIVACY BY DESIGN

Il Regolamento introduce il principio di protezione dei dati personali già **in fase di progettazione** (*byDesign*) per qualsiasi tipo di progetto che comporti l'utilizzo di dati personali (sito internet, software, soluzione IT, ambiente di lavoro, etc.).

- Pseudonimizzazione dei dati;
- Crittografia del database;
- Sistemi già predisposti alla cancellazione dei dati dopo il termine stabilito;
- Sistema integrato per la registrazione e gestione dei consensi;
- Predisposizione di informative chiare ed esaustive ;
- Adeguati processi di backup e ripristino dei dati in casi avversi;

STEP 1: PRIVACY BY DEFAULT

Il Regolamento impone che il titolare adotti opportune misure per garantire che siano trattati di **default solo i dati personali necessari in ogni fase del trattamento**:
dalla raccolta alla cancellazione dei dati e non soltanto durante l'elaborazione

- Minimizzazione dei dati personali già in fase di raccolta;
- Pseudonimizzazione dei dati personali;
- Periodo di conservazione dei dati limitato;
- Accesso ai dati consentito solo per soggetti autorizzati al trattamento;
- Accesso ai dati consentito per intervalli temporali brevi in caso di attività occasionali;

Individuare i Ruoli, Responsabilità, Compiti

Ai fini della gestione dei Dati Personali raccolti presso l'azienda il GDPR ha previsto l'individuazione di un vero "direttore d'orchestra" che eserciti una funzione di informazione, consiglio e controllo interno:

Il DATA PROTECTION OFFICER (DPO)

Definire e attuare gli adempimenti necessari per priorità d'azione

Dopo aver mappato i trattamenti effettuati, è necessario identificare per ciascuno di questi le attività da effettuare per essere conformi al Regolamento.
Gi adempimenti dovranno essere categorizzati per priorità in base ai rischi per i diritti e le libertà dei soggetti.

STEP 3: DEFINIRE E ATTUARE GLI ADEMPIMENTI PER PRIORITA' D'AZIONE

Le principali attività saranno:

- Assicurarsi che siano trattati solo i dati personali strettamente necessari alle finalità di trattamento;
- Identificare la base giuridica del trattamento (consenso, interesse legittimo, contratto, obblighi legali);
- Revisionare tutte le informative per essere conformi al Regolamento;
- Regolamentare i rapporti con i Responsabili del trattamento;
- Verificare che gli incaricati del trattamento siano a conoscenza degli obblighi in materia di protezione dei dati personali e che siano presenti clausole di riservatezza;
- Prevedere le modalità d'esercizio dei diritti degli interessati
- Valutazione delle misure di sicurezza da adottare.

STEP 3: DEFINIRE E ATTUARE GLI ADEMPIMENTI PER PRIORITA'D'AZIONE

Se l'azienda:

- Tratta dati particolari o giudiziari;
- Effettua attività di sorveglianza sistematica di un'area accessibile al pubblico;
- Svolge attività di valutazione sistematica di aspetti personali dei soggetti, tra cui la profilazione;
- Trasferisce dati personali fuori dall'UE

Ulteriori adempimenti:

- **Valutazione di impatto per la protezione dei dati personali (PIA);**
- **Informative specifiche e dettagliate;**
- **Raccolta di consensi specifici;**
- **Garanzie per il trasferimento dei dati Extra UE;**
- **Determinazione delle misure di sicurezza adeguate da mettere in atto in considerazione dei rischi.**

Definizione delle Misure di sicurezza Adeguate
Gestire i rischi

Se sono stati individuati trattamenti di Dati Personali suscettibili di generare dei rischi elevati per i diritti e le libertà dei Soggetti Interessati, dovrà essere eseguita, per ognuno dei trattamenti, un'analisi d'impatto sulla protezione dei dati

STEP 4: GESTIRE I RISCHI

Ogni Titolare del Trattamento dovrà determinare le **misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio e al trattamento**

Se l'azienda ha identificato dei trattamenti di dati personali che possano comportare dei **rischi per i diritti e le libertà dei soggetti interessati**

Condurre una Valutazione d'impatto per ciascun trattamento di dati personali a rischio

STEP 4: DATA PROTECTION IMPACT ASSESSMENT (DPIA)

La DPIA è una procedura che ha lo scopo di **Costruire e Dimostrare la Compliance** ai requisiti del Regolamento 679/2016.
Importante **strumento di Accountability** si realizza attraverso:

La **valutazione delle attività** di cui si compone il trattamento dei dati personali alla luce dei principi di necessità e proporzionalità;

La **gestione dei rischi** nei confronti dei diritti e libertà individuali derivanti dal trattamento dei dati personali.

Eseguire una DPIA non è obbligatorio per ogni operazione, ma soltanto quando il trattamento dei dati ha **un'alta probabilità di rischi nei confronti dei diritti e libertà individuali** derivanti dal trattamento dei dati personali, **sebbene in termini di buona prassi costituisca un modo per il Titolare/Responsabile di dimostrare responsabilità e trasparenza** attraverso la predisposizione di misure di sicurezza adeguate al contesto e al rischio.

STEP 4: MISURE TECNICHE E ORGANIZZATIVE

Il Regolamento introduce l'obbligo di attuare misure di sicurezza **ADEGUATE** in considerazione dei seguenti elementi:

Lo stato dell'arte e i costi di attuazione

La natura e il campo di applicazione del trattamento

Il contesto e le finalità del trattamento

Il rischio, la probabilità e la gravità delle conseguenze per i diritti e le libertà delle persone.

STEP 4: MISURE TECNICHE E ORGANIZZATIVE

Il Regolamento stabilisce che la sicurezza dei dati deve basarsi sui seguenti aspetti fondamentali:

MISURA TECNICA →

Pseudonimizzazione o crittografia dei dati;

REQUISITI DI SICUREZZA →

Garanzie di riservatezza, integrità, disponibilità e recupero dei dati personali e dei sistemi che li custodiscono e li elaborano;

Accesso tempestivo ai dati in caso di un evento dannoso fisico o tecnico;

Processi di verifica periodica dell'efficacia ed effettiva applicazione delle misure di sicurezza in atto.

Definizione di Policy e Procedure
Procedure Organizzative Interne

Per garantire un alto livello di protezione dei Dati Personali porre in essere delle Procedure Interne che garantiscano la protezione dei Dati in tutti i momenti, tenendo in considerazione gli eventi che possono sopravvenire nel corso del Trattamento.

STEP 5: PROCEDURE ORGANIZZATIVE INTERNE

Per **garantire un adeguato livello di protezione dei dati personali**, implementare procedure interne organizzative che tengano in considerazione qualsiasi evento che possa avere un impatto sul trattamento di dati personali nel caso si verifichi
(vulnerabilità, incidenti, violazione dei dati, esercizio dei diritti, etc.)

Procedure interne che comprendano:

- Il rispetto del principio della protezione dei dati già in fase di progettazione di un'applicazione o di un trattamento e di default;
- La formazione e la sensibilizzazione dei soggetti interni che trattano dati personali;
- La gestione dei reclami e delle richieste di esercizio dei diritti da parte degli interessati;
- La prevenzione e la gestione di violazioni ai dati personali, tra cui l'obbligo di notifica all'autorità Garante ed eventualmente agli interessati.

Procedura di Data Breach

Attuare misure tecniche, organizzative e procedurali al fine di individuare e gestire tempestivamente una violazione dei dati personali e la relativa notifica

STEP 6: DATA BREACH

Nel caso in cui si verifichi una violazione dei dati personali che possa in qualche modo tradursi in un rischio per i diritti e le libertà degli individui, qualsiasi **titolare del trattamento** ha l'obbligo normativo di notificare l'avvenimento all'Autorità di controllo.

Il titolare del trattamento è tenuto ad **informare gli interessati** tempestivamente se la violazione può comportare una **grave ed elevata compromissione dei loro diritti e delle libertà**, come nel caso di:

Danni fisici, materiali o morali	**Limitazione dei diritti**	**Discriminazione**	**Furto o usurpazione d'identità**	**Perdita del controllo dei dati**

Non è necessaria la comunicazione ai soggetti interessati se il titolare del trattamento ha applicato le **opportune misure tecnologiche e organizzative preventive**(esempio crittografia dei dati) o è stato in grado di **evitare tempestivamente il verificarsi di rischi elevati**.

STEP 6: DATA BREACH

Elementi essenziali da riportare all'interno della Notifica di violazione all'Autorità:

- La natura della violazione dei dati personali e le circostanze in cui si è verificata;
- Il numero approssimativo di soggetti interessati coinvolti ;
- Le categorie e il numero approssimativo di registrazioni dei dati oggetto della violazione;
- I riferimenti del responsabile della protezione dei dati o di un altro punto di contatto;
- Le probabili conseguenze della violazione dei dati personali;
- Le misure già adottate o che il titolare intende adottare per ridurre le conseguenza e porre rimedio alla violazione dei dati personali.

STEP 6: DATA BREACH

Contromisure necessarie per la **gestione di una violazione** e per limitarne gli effetti:

Misure tecniche che riconoscano all'istante la violazione e allertino prontamente il titolare o il responsabile;

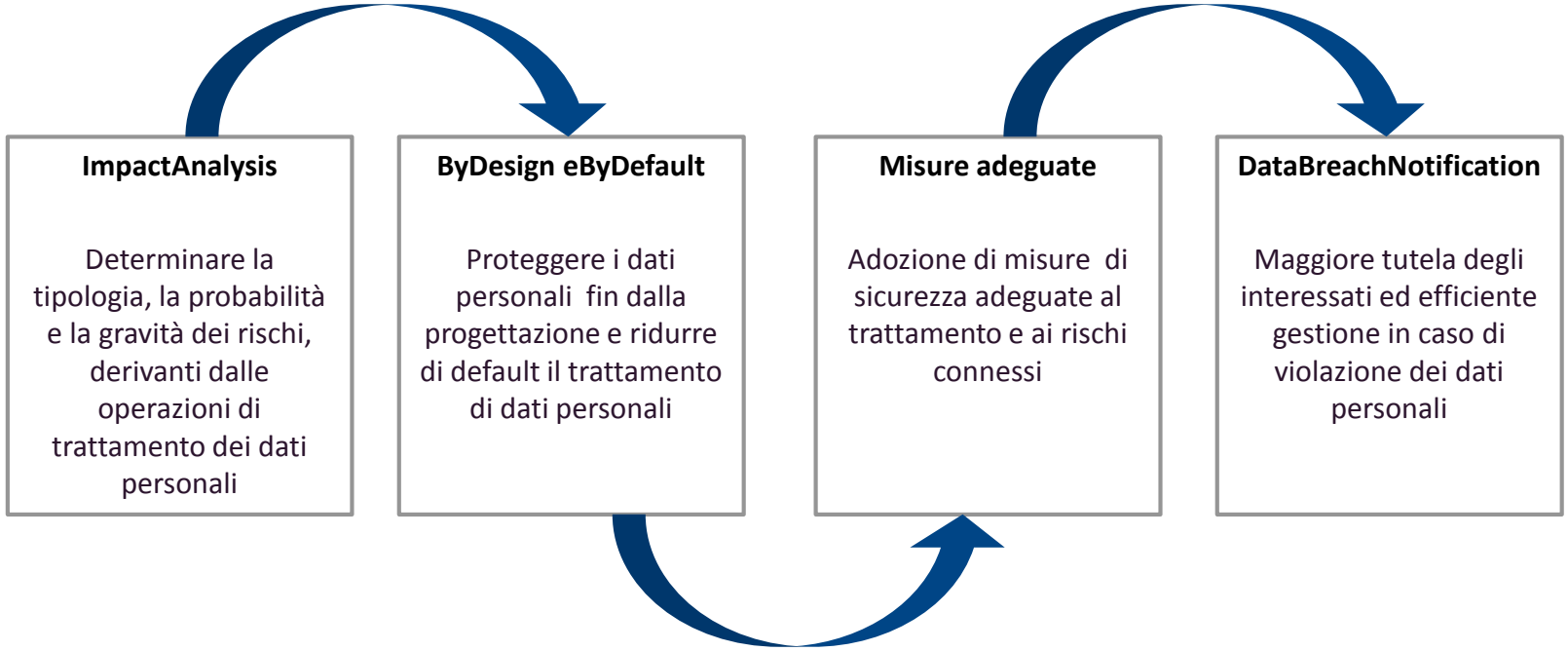
Sensibilizzazione dei responsabili del trattamento e dei soggetti autorizzati al trattamento, anche tramite adeguate policy, affinché si possa agire correttamente e tempestivamente in caso di databreach;

Mezzi adeguati per l'invio della comunicazione ai soggetti interessati quando dovuto, tenendo in considerazione che la violazione potrebbe anche compromettere i dati presenti a sistema;

Misure atte a rendere non intellegibili e criptati i dati oggetto di violazione per chiunque non sia autorizzato ad accedervi;

STEP 6: ADEGUATO LIVELLO DI PROTEZIONE

DALL'IMPACT ANALYSIS AL DATA BREACH



Documentare la conformità

Per dimostrare di essere conformi al GDPR è necessario raccogliere la documentazione necessaria. Le attività e i documenti posti in essere in ogni fase del Trattamento dovranno essere riesaminati e aggiornati regolarmente per assicurare una protezione dei Dati permanente

STEP 7: DOCUMENTARE LA CONFORMITA'

Per provare la conformità al Regolamento, predisporre e tenere aggiornata la documentazione necessaria.

- Documentazione attestante i trattamenti di dati personali svolti (Registro delle attività di trattamento, valutazione d'impatto, la documentazione prevista per il trasferimento dei dati Extra UE);

- Documentazione attestante il rispetto dei diritti e delle libertà dei soggetti interessati (le informative, i moduli di raccolta consensi, l'attestazione dei consensi raccolti, la gestione dei diritti esercitati);

- Documentazione che definisce i ruoli e le responsabilità in materia di protezione dei dati personali (i contratti e le nomine dei responsabili esterni, la gestione degli incaricati del trattamento, le procedure interne, etc.);

- Comprova delle misure di sicurezza tecniche implementate (analisi dei log, report, configurazioni, policy, etc.).

Grazie per l'attenzione

Carlo Guastone
Vice Presidente Business Development
SERNET SPA
carlo.guastone@sernet.it
Cell. 335-5833862
www.sernet.it

Gruppo di Lavoro
SICUREZZA INFORMATICA
Assintel

segreteria@assintel.it

@Assintel

GdL Assintel Sicurezza Informatica