Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Streaming Edition 2021

ASTREA Advanced Security, Training Research, Events Agency

ISO 27701, dall'information security alla data protection

Modera: ***Paolo Asioli***

Partecipano: ***Marco Bruno*** *(Alpitour),* ***Silvio Colloca*** *(Inpeco),* ***Fabio Cucciniello*** *(Gruppo Bracco),* ***Matteo Nasi*** *(CPL Concordia),* ***Guido Arrigoni*** *(Consoft Sistemi)*

#securitysummit #streamingedition

Streaming Edition

Associazione
Utilizzatori
Sistemi
E tecnologie
Dell'informazione

"DAL 1976...
BE THE CHANGE"

Vision

“ CONTRIBUIRE ALLA CRESCITA DIGITALE DELLE AZIENDE E DEL PAESE, PROMUOVENDO L'INNOVAZIONE TECNOLOGICA SECONDO PRINCIPI DI ETICA E SOSTENIBILITÀ. ”

Mission

Connettere, formare, Ispirare ed attivare la Comunità ICT generando valore per il Paese.

Per le aziende e per il paese, AUSED ambisce ad essere un imprescindibile punto di riferimento, un leader nella raccolta di risorse economiche e umane da destinare ai temi di Innovazione, non solo digitale,

Appartenere ad AUSED significa condividere la passione per le tecnologie IT ed attivarsi per la loro diffusione seguendo principi etici e sostenibili.

CONSIGLIO DIRETTIVO 2020/21

Tesoriere e Segretario Generale

Francesca Gatti

Presidente

Andrea Provini – CIO Bracco

Consiglieri

Massimiliano Bartolozzi – CIO Lucart

Andrea Bettoni – IT Manager Nexion

Alessandro Caleffi – CIO ACS Dobfar

Francesco Ciuccarelli –CIO Alpitour

Enrico Curzietti – CIO Colacem

Giovanni Daconto – CIO Ariston Thermo

Luca Guerra – CIO Primapower

Giuseppe Ingletti – Senior Advisor

Stefano Lombardi – MKTG Director Npo Sistemi

Mario Moroni – CIO Federchimica

Francesco Pezzutto – CIO Vimar

Riccardo Salierno – CIO Sapio

Diana Setaro – IT Manager Bosch Rexroth

Team «Be The Change»

Marco Perucchetti – CIO Ed. Quadratum

Daniele Vanzanelli – Analytics Advisor

Orietta Campironi – CIO Messinaline

Maurizio Bonomi – CIO AC Milan

Luigi Pignatelli – CIO Carl Zeiss

Virginio Basilico – CIO Vibram

Barbara Poli – CIO GNV

Roberto Boselli – CIO Lifestile Design

Mirco Destro – Group CIO Beltrame

Fulvio Guglielmelli - Consoft

AIUSE Associazione Utilizzatori Sistemi E tecnologie Dell'Informazione

Competenze e tecnologie per la Digital Transformation

Sviluppiamo soluzioni *end to end* capaci di generare valore d'impresa e di supportarvi nell'allineamento alla trasformazione digitale.

Le nostre attività di consulenza e formazione, la realizzazione di sistemi integrati e l'erogazione di servizi in outsourcing e insourcing sono frutto di competenze costantemente aggiornate e focalizzate in aree tematiche.

Parte di ALTEN GROUP

Data Protection vs Information Security

- La **Data Protection**, o Protezione dei Dati Personali, è da tempo un requisito normativo

- *Prima* **D.Lgs 196/2003** "Codice Privacy" ➔ approccio **«prescrittivo»** (Allegato B)
- *Poi* Regolamento Europeo 2016/679 "**GDPR**" efficace dal 25 maggio 2018
  - ✓ Accountability
  - ✓ Valutazione del rischio
  - ✓ Misure adeguate

- Questo approccio ben si sposa con i **principi dell'Information Security**

ISO 27001 e ISO 27701

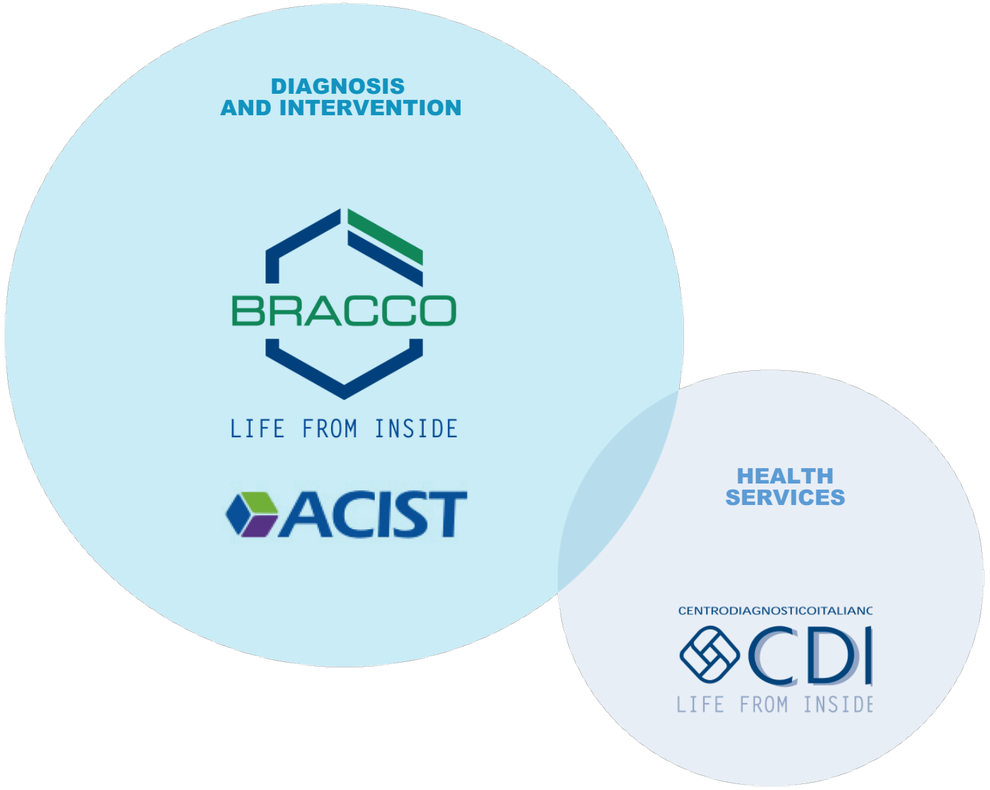
- La **ISO 27001** è probabilmente la **norma volontaria** relativa alla **Sicurezza delle Informazioni** più diffusa ed adottata
  - ✓ **Sistema di Gestione** per la Sicurezza delle Informazioni (SGSI o ISMS)
  - ✓ Approccio basato sulla **Valutazione del Rischio**
  - ✓ Un **ricco set di controlli** nella ISO 27002 (in fase di aggiornamento)

- Nel 2019 viene approvata la **ISO 27701**
  - ✓ **Privacy** Information Management System (PIMS)
  - ✓ **Estensione** della ISO 27001
  - ✓ **Convergenza tra Information Security e Data Protection ?**

Fabio Cucciniello

Gruppo Bracco

Bracco Group Charter of Identity



- An integrated Group with private capital, **3,420 employees** and a consolidated turnover of **€ 1.29 billion euros, 86%** of which made in **foreign markets**

- Bracco works in the following areas:
  - > **Diagnosis**
  - > **Healthcare Services**

A Global Presence

The Bracco Group **operates all over the world**, either directly or through joint ventures, partnerships, or distribution and agency agreements

Sales in more than 100 Countries

Privacy & Security

- 2018 istituzione del «**data protection program**» a cura dell'ufficio legale;
- 2018 istituzione del DPO;

- 2019 creazione del «**security framework**» a cura della direzione IT ispirato alla ISO 27001 con i suoi principi cardine quali:
  - risk based
  - continuous improvement
  - accountability
- 2020 istituzione del CISO.

Streaming Edition

Next steps…

- Far «parlare» i due set documentali;
- Razionalizzare le misure di sicurezza previste;
- Allineare l'approccio su, per esempio:
  - Data Breach
  - Gestione dei vendor
  - Security & privacy by design

La scrittura di un unico framework (legale e IT) ispirato alla ISO 27701 è una opzione in corso di valutazione per raggiungere questi obiettivi.

Silvio Colloca

Inpeco

Streaming Edition

709
Headcount Total

218
Headcount in R&D

39
Mean age of employees

Our mission:

reduce errors in healthcare

78+
Countries of business

2000+
Systems manufactured

67%
Business outside Europe

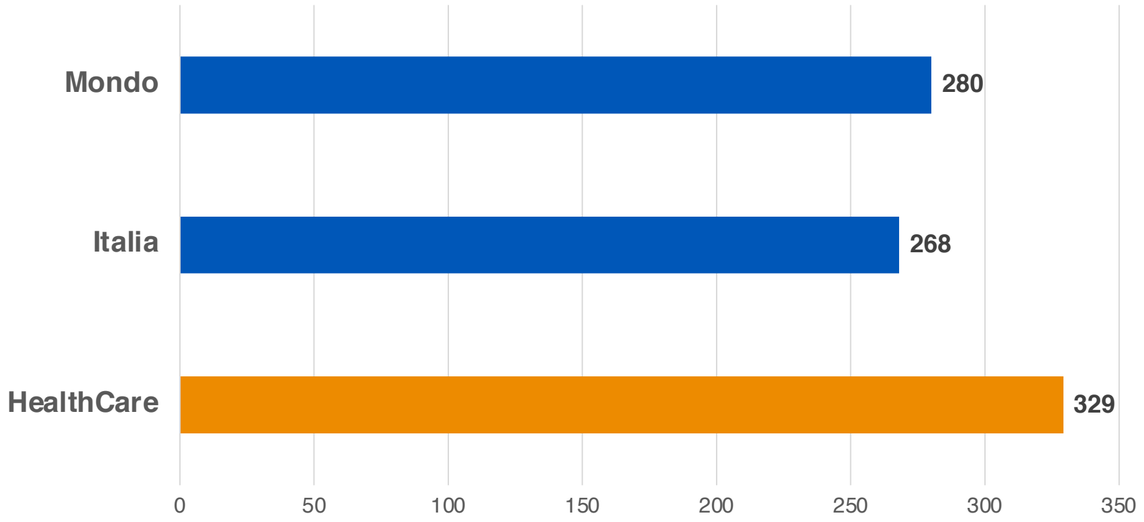
inpeco
Automation in Healthcare

Streaming Edition

Data Breach nel mondo

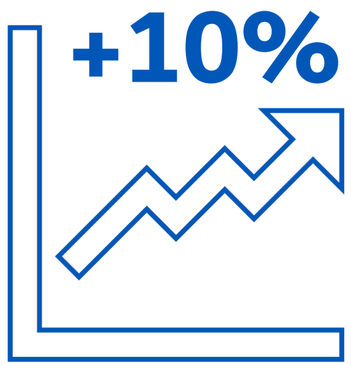
Automation in Healthcare

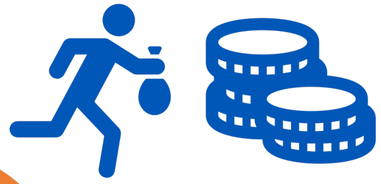
Tempo medio di identificazione e risoluzione data breach



+20%

+40%



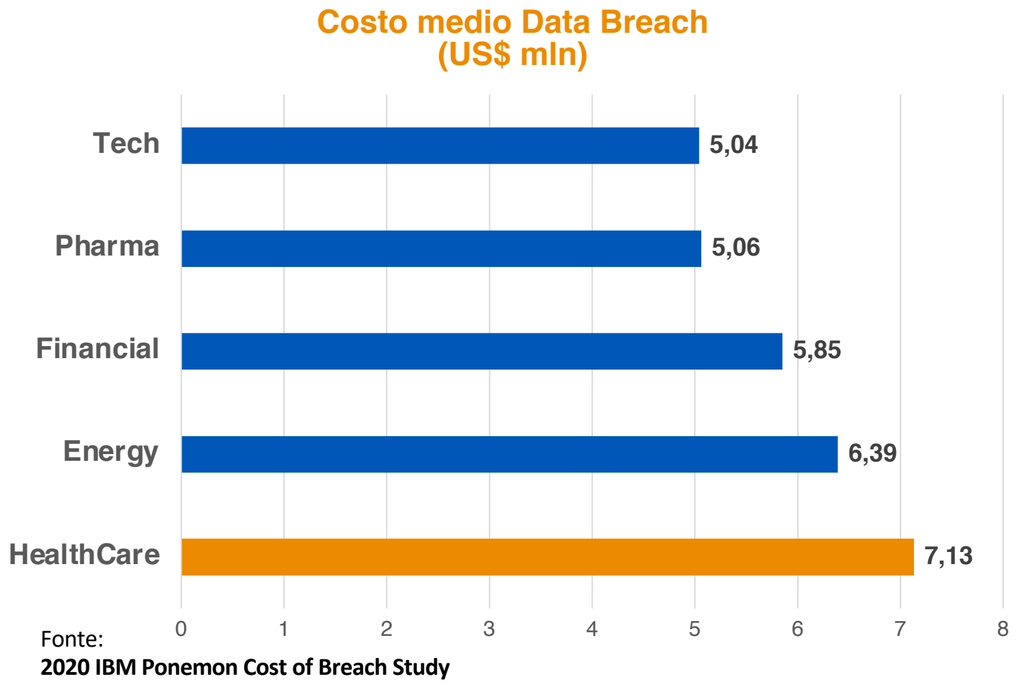


2X

PII

Fonte:
2020 IBM Ponemon Cost of Breach Study

Il mondo HealthCare è un nuovo «far west» digitale



Fonte:
2020 IBM Ponemon Cost of Breach Study

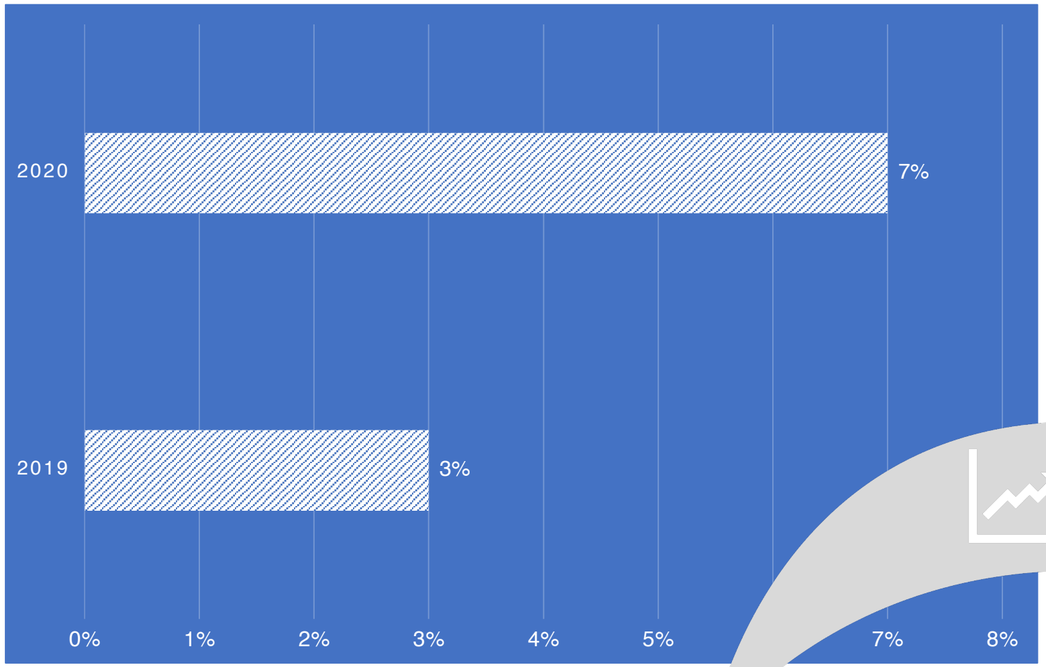
+90% degli attacchi parte da una mail

BEC - PHISHING - SOCIALEERING: Le persone sono il bersaglio

«Da grandi poteri derivano grandi responsabilità» (Benjamin "Ben" Parker - Marvel)

L'Information Security Awareness in «healthcare» è ***ineluttabile***

Anche in Italia…



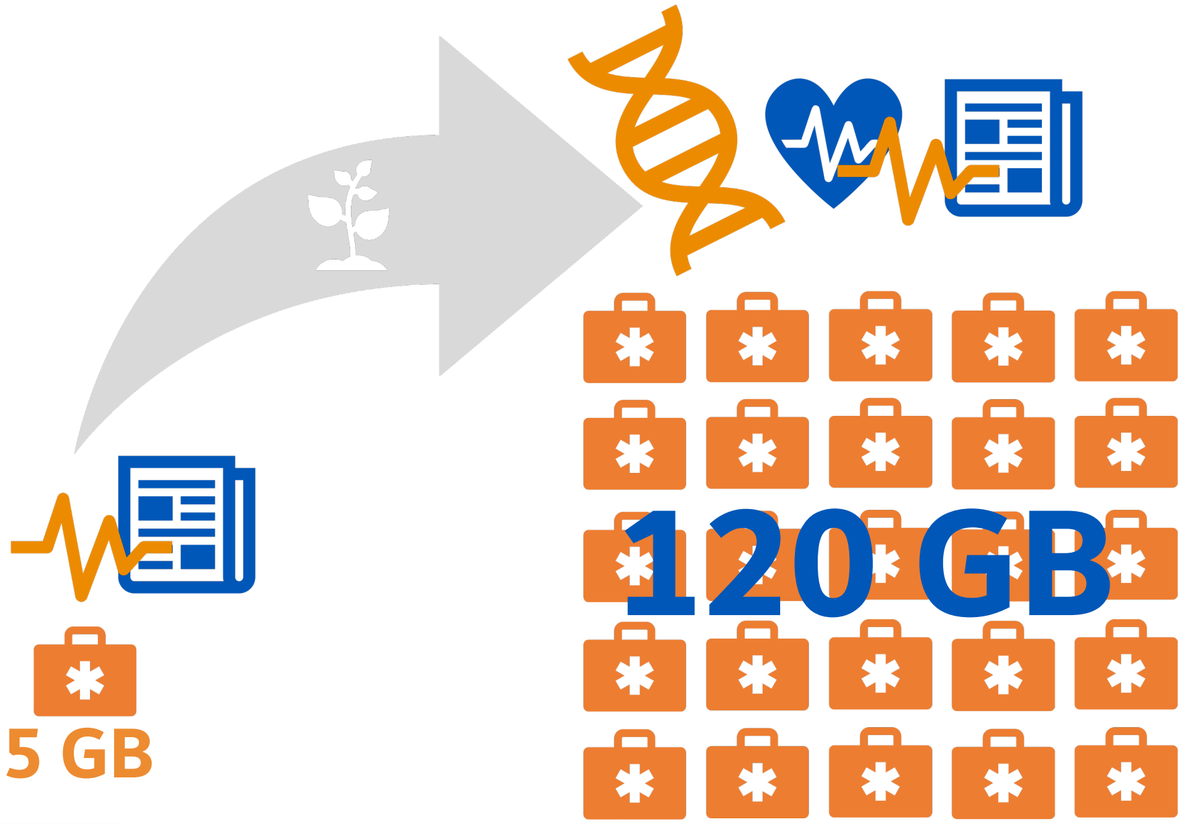
RA 2020

230%

	2019	2020
	1%	4%
	14%	20%

Fonte:
RELAZIONE SULLA POLITICA DELL'INFORMAZIONE PER LA SICUREZZA 2020
Sistema di informazione per la sicurezza della Repubblica

I big data sanitari sono davvero «big»



2
ZETTABYTE/YEAR

60+
TERABYTE/SEC

I dati sanitari hanno bisogno del cloud

MFA
CRYPTO
...

GDPR
ISMS
PIMS
...

Marco Bruno

Alpitour

All’inizio…

SECURITY

- ✓ **RACF - definizione delle utenze e dei profili, classificazione dei dati**
- ✓ **Canali di vendita:**
  - ➢ **B2B -** Agenzie di Viaggio – Gestione delle credenziali di accesso
  - ➢ **B2C -** Cliente finale - CRM – Preservare la sicurezza e la privacy

SECURITY

La compliance…

- ✓**Assessment e definizione di un framework di sicurezza basato su standard e best practises internazionali (NIST, ISO27001)**
- ✓**ITSP1 Security Program**: programma volto ad incrementare il livello di sicurezza negli ambiti tecnologico, operativo, governance
- ✓**ITSP2 Security Program:** l'evoluzione su nuove aree e tecnologie

PRIVACY

All’inizio…

- ✓Creazione di un **ufficio Privacy**
- ✓Conformità alle **norme vigenti**

PRIVACY

La compliance…

GDPR

- ✓**Adozione di un tool sw**:
  - *Registro dei trattamenti*
  - *Censimento degli asset (fisici e logici)*
  - *Analisi dei rischi*
  - *Gestione Data Breach*
- ✓**Privacy by default/design**
- ✓**Accountability**
- ✓**Organigramma Privacy**

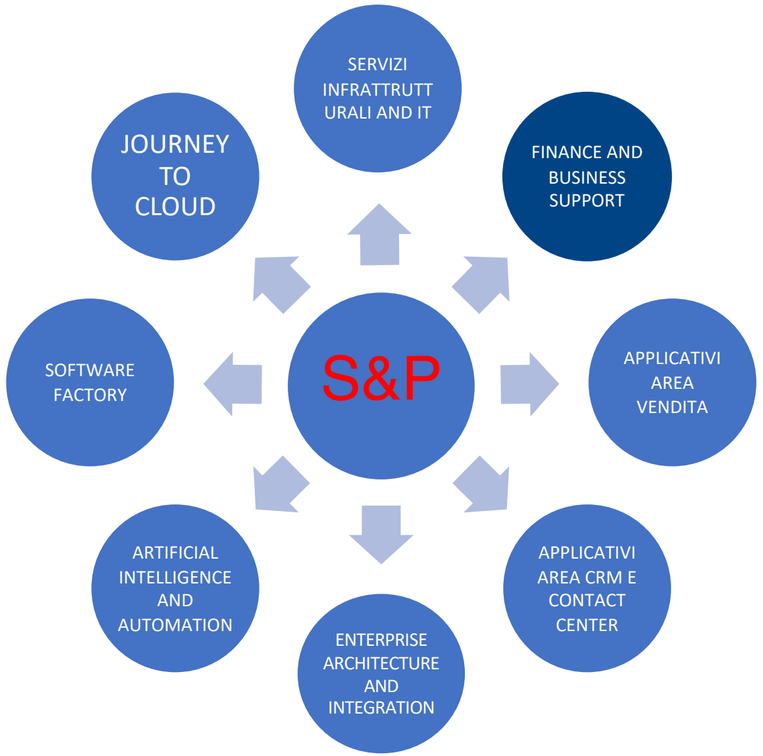
SECURITY & PRIVACY

Un’unica struttura

- Contribuire a far sì che l'azienda possa raggiungere i propri obiettivi di business in modo **sicuro ed efficace**.
- **Ridurre i rischi** senza impattare sull’operatività.
- Colloquiare con i business manager delle varie aree aziendali in modo da supportarli efficacemente nel **raggiungere in sicurezza i loro obiettivi**.

SECURITY & PRIVACY

*Non un punto di arrivo ma un **punto di partenza** con l'obiettivo principale di garantire una sempre più corretta protezione delle informazioni*



Una struttura al centro del Business è necessaria per avere un legame costante con le attività IT ed essere aggiornati sull'avanzamento delle iniziative sia dal punto di vista Security che Privacy

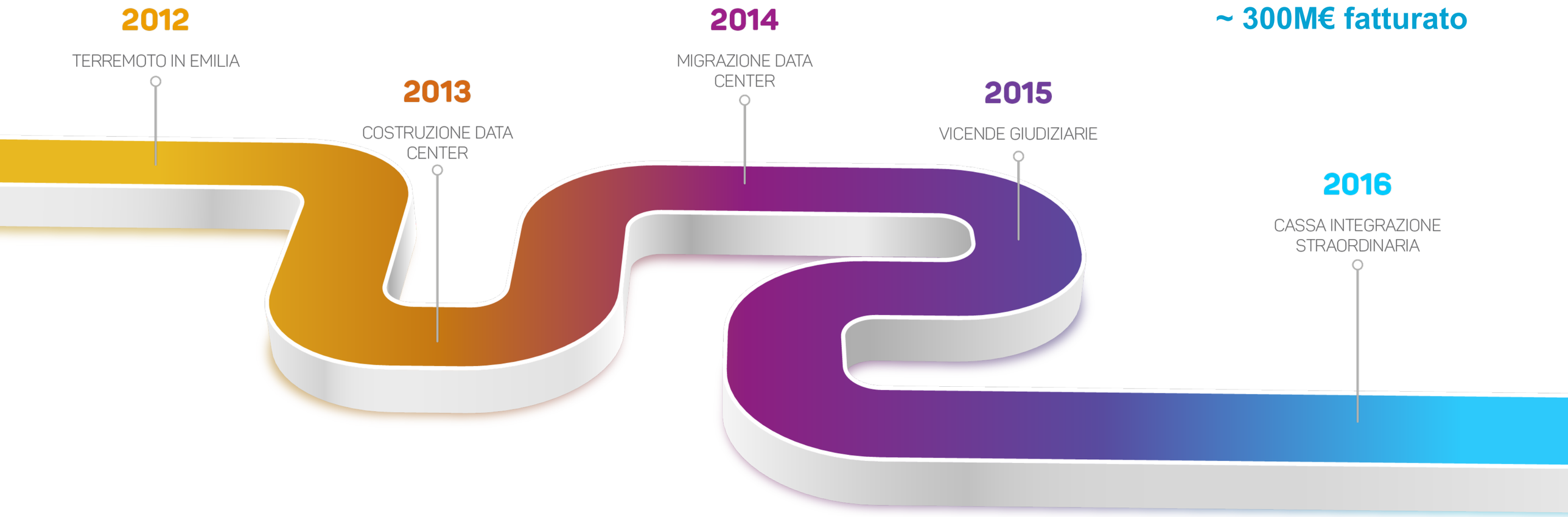
Matteo Nasi

CPL CONCORDIA

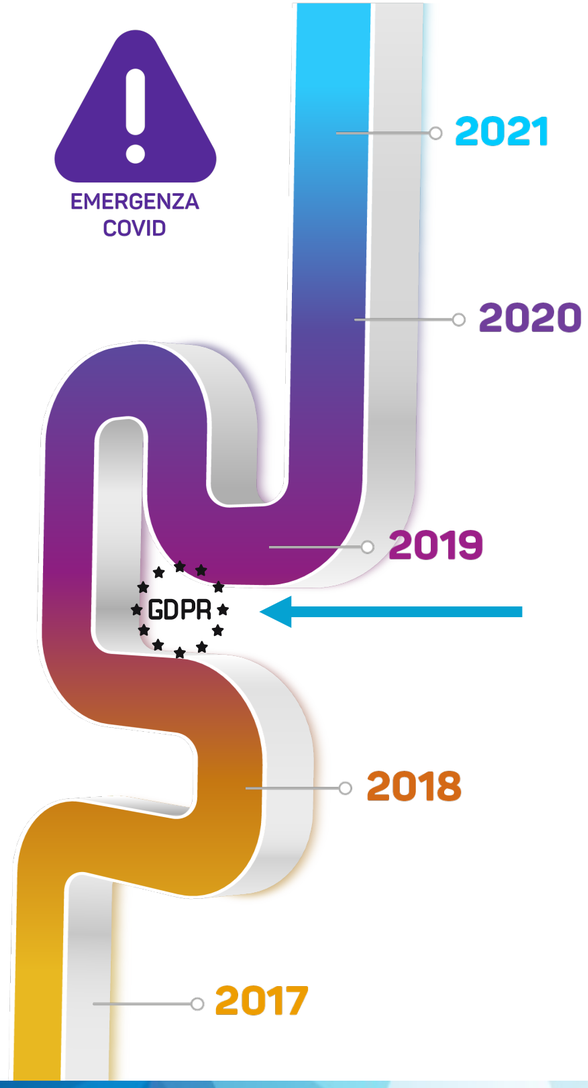
Il percorso di Evoluzione dell'IT e la Digitalizzazione

CPL CONCORDIA Group
SINCE 1899

~1600 dipendenti
~ 300M€ fatturato



Dalla protezione dei dati personali al Sistemi di gestione della sicurezza delle informazioni



BUSINESS CONTINUITY,
DISASTER RECOVERY,
ISO 27001

AI, SMART ANALYTICS,
BIGDATA, IOT,
DIGITAL TWINS
INTEGRAZIONE SISTEMI

CYBER SECURITY

RIORGANIZZAZIONE IT
BUDGET IT INTEGRATO
AGILE MANAGEMENT OFFICE
DIGITALIZZAZIONE

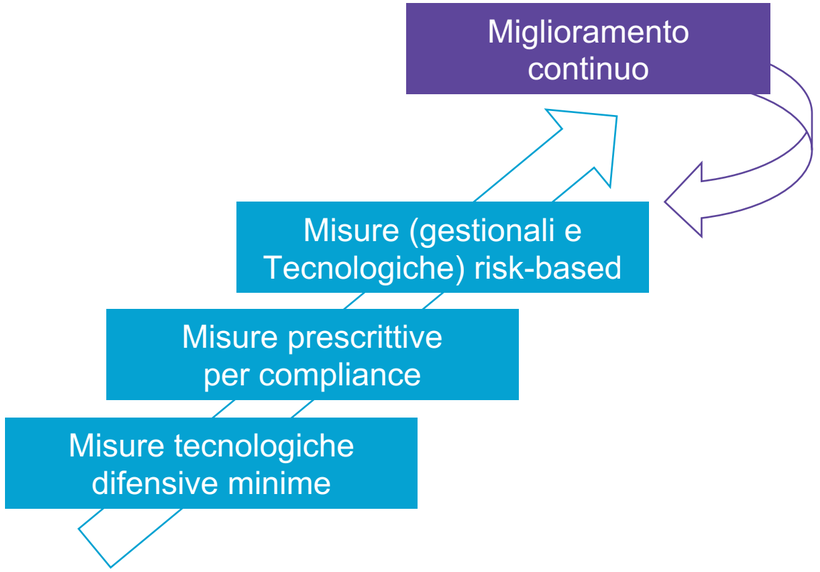
AUDIT SISTEMI IT

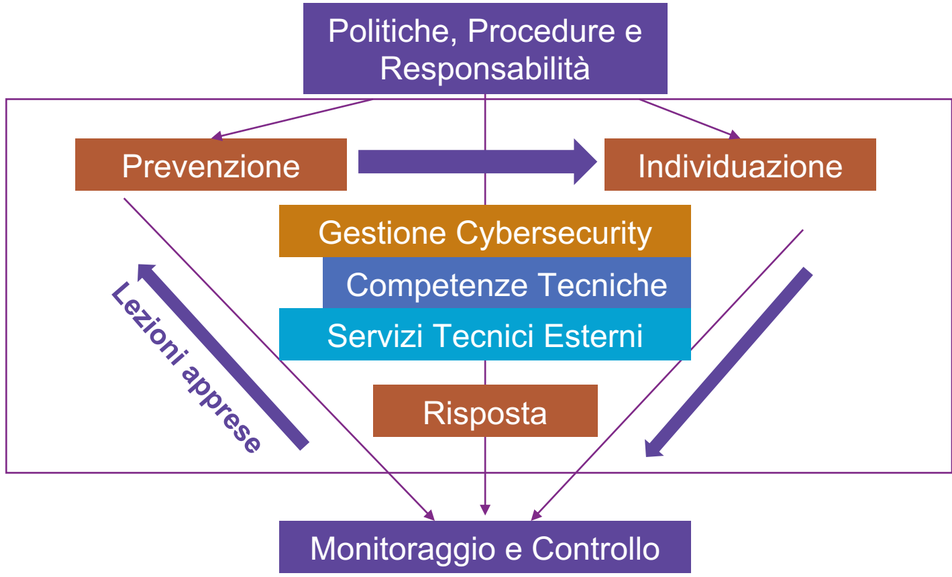
Da esigenza di compliance a sistema di gestione

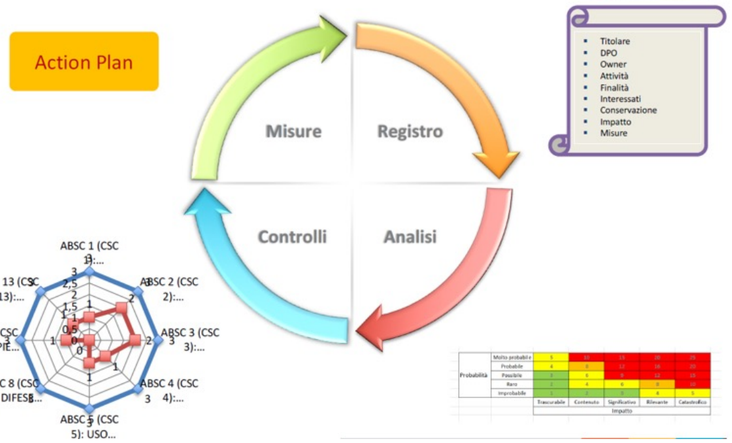
Maturità crescente intervenendo su:

- ✓ Persone
- ✓ Procedure
- ✓ Tecnologie

Maturity Model: **AGID**



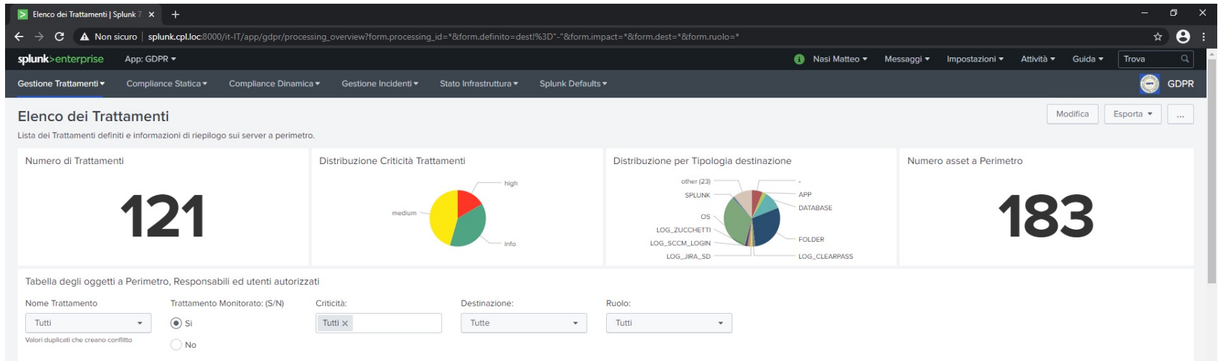


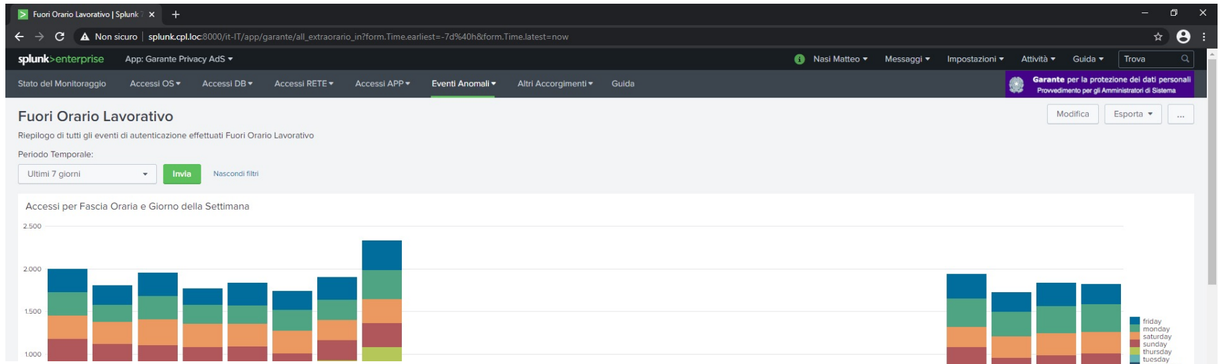


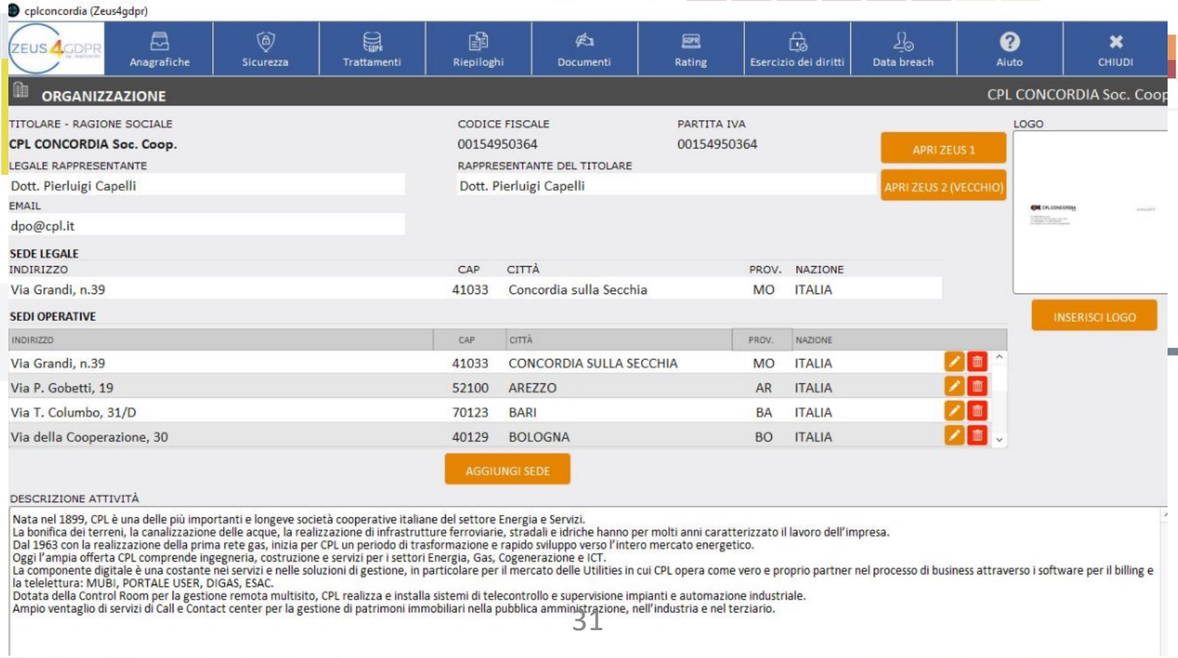
Cercando un equilibrio con:

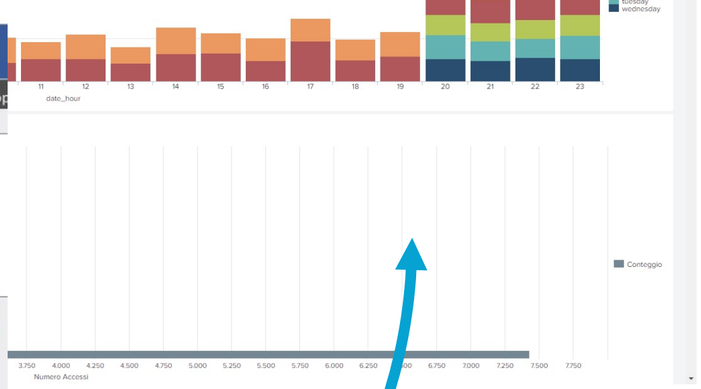
- ✓ Costo
- ✓ Usabilità
- ✓ Sicurezza

Integrazione architetturale di **Persone** – **Processi** – **Tecnologia**: sistema di monitoraggio e registro dei trattamenti









Streaming Edition
SECURITY SUMMIT
Clusit Associazione Italiana per la Sicurezza Informatica

Guido Arrigoni

Consoft Sistemi

Streaming Edition

ISO/IEC 27701

- **È una norma volontaria, pubblicata nel 2019, che può essere oggetto di certificazione e in ogni caso come guideline**
- **È una norma internazionale, non limitata ai confine dello spazio econominco europeo**
- **Il PIMS integra ed estende l'ISMS (o SGSI)**
- **Supporta la definizione di processi e misure di sicurezza a protezione dei dati personali entro il perimetro e nell'ambito dello *scope* di applicazione**

GDPR e non solo

- **È una norma cogente, che regola le modalità di trattamento nonchè di trasferimento dei dati personali**
- **La normative cogente in materia di protezione dei dati personali include il Codice della Privacy**
- **Le indicazioni per la compliance sono completate dalle line guida redatte a livello europeo dall'EDPB e nazionale dal GPDP.**

Adottare la ISO/IEC 27701 non significa essere compliant al GDPR!

ISO/IEC 27701: la certificazione

ISO 27701

- **Per la sua composizione, l'applicazione della ISO/IEC 27701 non può essere considerata autonoma ma deve basarsi sull'applicazione della ISO/IEC 27001 e ISO/IEC 27002.**
- **Può essere oggetto di estensione della certificazione ISO 27001, anche in modo a sè stante (se l'organizzazione è già certificate ISO/IEC 27001) anche da ente distinto**
- **Può essere oggetto di estensione della certificazione ISO 27001 in occasione di rinnovo o sorveglianza della compliance dell'ISMS alla ISO/IEC 27001**
- **Qualora l'organizzazione utilizzi il cloud, l'estensione richiede l'implementazione del controlli della ISO 27017 e ISO 27018**

Servizi Google Cloud che rientrano nell'ambito della certificazione ISO/IEC 27701 di Google Cloud Platform

Google Cloud

ISO/IEC 27701: I vantaggi

- **Consente di definire processi e misure di sicurezza per la protezione dei dati personali, che vengono riconosciuti come patrimonio (asset) aziendale**
- **L'implementazione del PIMS consente di controllare, mantenere, migliorare nel tempo il proprio sistema di gestione dei dati personali, in grado di affrontare problematiche che non possono essere circoscritte al mondo IT**
- **Costituisce un importante strumento di accountability (cfr. Art. 5.2 del GDPR) diventando al contempo sia dimostrazione dell'impegno dell'organizzazione sia misura di sicurezza organizzativa a protezione dei dati personali**

La ISO/IEC 27701 aiuta l'organizzazione nel perseguire la compliance alla normativa in materia di data protection!

Q&A

Grazie per l’attenzione

RIFERIMENTI

Guido Arrigoni	guido.arrigoni@consoft.it
Paolo Asioli	paolo.asioli@consoft.it
Marco Bruno	marco.bruno@alpitourworld.it
Silvio Colloca	silvio.colloca@inpeco.com
Fabio Cucciniello	fabio.cucciniello@bracco.com
Matteo Nasi	mnasi@cpl.it