GDPR come opportunità per proteggere il proprio patrimonio di DATI e CLIENTI efficientando IT e OPERATIONS

Dott.ssa Elisa Fontana - C-DIRECT Consulting
Avv. Barbara De Cillis - DDS Studio Legale
Ing. Marco Lazzari - L.HOL.US *(focUS on HOLystic sOLUtions)*

Bologna, 23 Maggio 2018

Ing. Marco Lazzari – Esperienze Professionali

- PM per nota SWhouse su progetti ERP e CRM
- Progetti Industria 4.0
- Progetti GDPR
- Consulenze per certificazioni Qualità (ISO 9001)
- Analista Processi IT/Manufacturing
- 20 anni di esperienza in aziende manifatturiere in Ufficio Tecnico, Produzione, IT, Post Vendita

GDPR - DEFINIZIONI

- UE 2016/679 - Regol. Generale sulla Protezione dei Dati

- DATI/ASSET (su supporti informatici e supporti cartacei): sono le informazioni e i dispositivi/supporti che le gestiscono
Fra i primi task => Asset Inventory

- APPROCCIO: il Garante UE parla di Accountability (Responsabilizzazione), imponendo di fatto un'attenta gestione, rendendo certo cosa si fa e perchè (CERTUM + FACERE) => SG

- ISO 27001: riferimento per le valutazioni e per la gestione

GDPR - DEFINIZIONI

- PROTEZIONE DATI - R.I.D. + S.
  - **R**iservatezza: proprietà di non rendere disponibile/rivelare l'informazione a soggetti non autorizzati
  - **I**ntegrità: proprietà di salvaguardare accuratezza/completezza dell'informazione
  - **D**isponibilità: proprietà di garantire accesso/utilizzo dell'informazione a soggetti/dispositivi autorizzati

  - **S**icurezza: conservazione della Riservatezza, Integrità e Disponibilità delle Informazioni

  - GESTIONE RISCHI: è la nuova sfida

GDPR - ALCUNE PILLOLE

- *ART 32: il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*

- *NON DOVRA' PIU' ESSERE ACCETTABILE:*
  - *MISCHIARE IN MANIERA INCONTROLLATA DATI PRIVATI E DATI AZIENDALI,*
  - *ACCEDERE A DATI AZIENDALI DA DISPOSITIVI PERSONALI NON CONTROLLATI*

- *I BENI STRUMENTALI DELL'INDUSTRIA 4.0*
  - *SONO SPESSO I MENO CONSIDERATI DAL MONDO IT AZIENDALE*
  - *MA PER VARI MOTIVI RAPPRESENTANO QUASI SEMPRE UNA CRITICITA'*

- *LE MAGGIORI MINACCE PROVENGONO DAGLI ERRATI COMPORTAMENTI UMANI*

GDPR - OPPORTUNITA' e GESTIONE

- GDPR: COGENZA ma anche OPPORTUNITA'
  - Focus su DATI, su INFORMAZIONI
  - Focus su DATI utilizzati, gestiti, liberandosi di quelli inutilizzati
  - questo porta a Intensificazione Focus su Cliente

- GDPR: approccio STRUTTURATO
  - approccio imprenditoriale
  - analisi e gestione dei rischi
  - appoggio su framework HLS fortemente standardizzato
  - ausilio di altri SG HLS con "più esperienza"
  - disponibilità di norme "tecniche" che forniscono Controlli e Strumenti

0, 1, 2, 3 - NORME e SISTEMI DI GESTIONE

- **UE 679/16 (GDPR)**
  - Cogenza ma anche Opportunità

- **UNI CEI EN ISO/IEC 27001:2017** - Sicurezza Informazioni (*)(**)
  - Standard di riferimento per le Valutazioni (parte non Legale)
  - quindi SG di riferimento per ottemperare alla Cogenza
  - Norma Tecnica: appx. A

- UNI CEI EN ISO/IEC 27002:2017 - Best Practices di sicurezza
- ISO/IEC 27004:2016 - Monitor, Misurazione, Valutazione
- ISO/IEC 27017:2015 e ISO/IEC 27018:2014 - Best Practices di sicurezza cloud

(*) HLS (High Level Structure) e PDCA (Plan-Do-Check-Act / Ciclo di Deming)
(**) Aziende certificate: 1094 in Italia, 59 in E.R. (Accredia 11/2017)

0, 1, 2, 3 - NORME e SISTEMI DI GESTIONE

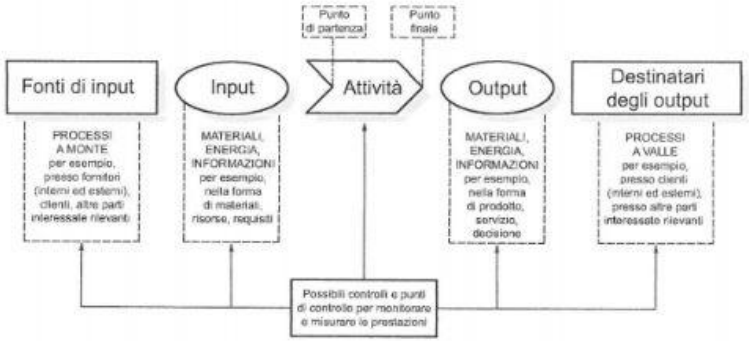
- UNI EN ISO 9001:2015 - Qualità (*)
  - La Madre di tutti i SG HLS
- UNI ISO 31000:2010 - Gestione del Rischio
  - Linea guida trasversale a qualsiasi organizzazione e a qualsiasi tipo di Rischio
- UNI ISO 10014:2007 - Benefici economici e finanziari
  - Linea guida tecnica per Autovalutazione

- Ulteriori norme di rif. per un approccio “virtuoso”
  - UNI ISO 45001:2018 - Salute e Sicurezza sul lavoro (*)
  - UNI EN ISO 14001:2015 - Ambiente (*)
  - UNI CEI EN ISO 50001:2011 - Energia

(*) HLS (High Level Structure) e PDCA (Plan-Do-Check-Act / Ciclo di Deming)

0, 1, 2, 3 - APPROCCIO HLS e PDCA

- APPROCCIO OLISTICO PER PROCESSI



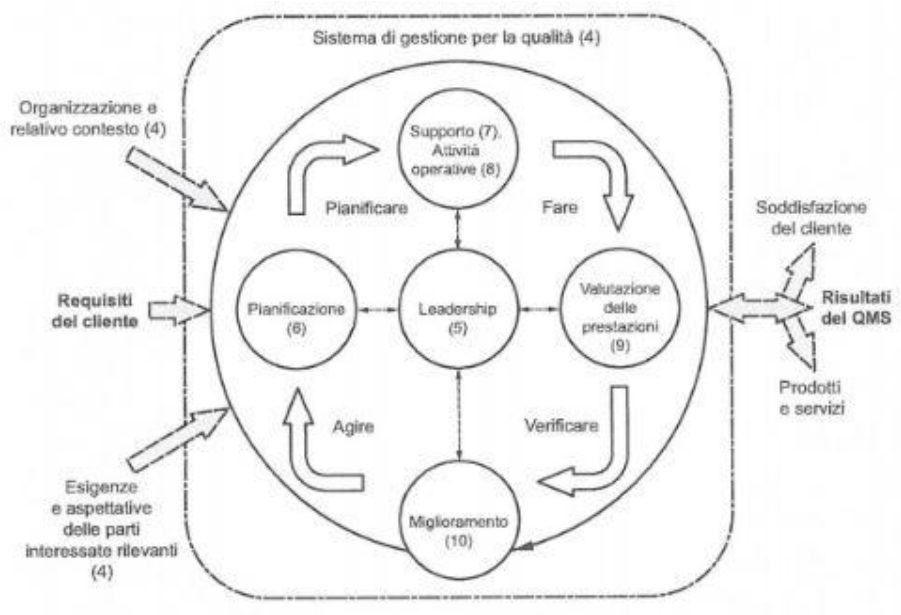
SICUREZZA INFORMAZIONI - ISO 27001	QUALITA' - ISO 9001
Sviluppo, Attuazione, Miglioramento efficacia di un SG per la Sicurezza delle Informazioni	Sviluppo, Attuazione, Miglioramento efficacia di un SG per la Qualità
Accrescimento soddisfazione del Cliente attraverso il soddisfacimento dei requisiti (di sicurezza delle informazioni) del Cliente stesso.	Accrescimento soddisfazione del Cliente attraverso il soddisfacimento dei requisiti (qualitativi) del Cliente stesso.
Definizione/gestione dei Processi Correlati In conformità alla Politica per la Sicurezza delle Informazioni e alla Strategia aziendale	Definizione/gestione dei Processi Correlati In conformità alla Politica per la Qualità e alla Strategia aziendale

Comprensione e gestione dei Processi Correlati come un Sistema contribuisce all'efficacia e all'efficienza dell'organizzazione

Questo approccio sistemico consente di tenere sotto controllo processi e interazioni/interdipendenze per conseguire i propri risultati attesi e incrementare le prestazioni complessive dell'organizzazione.

0, 1, 2, 3 - APPROCCIO HLS e PDCA

- CICLO ITERATIVO PDCA (Plan-Do-Check-Act)



La gestione dei processi e del sistema nel suo complesso può essere realizzata utilizzando il ciclo PDCA

Pianifica, Fai, Verifica, Migliora

….ripetere...

con un orientamento generale al Risk Based Thinking

Valutazione d'Impatto

Rischi / Opportunità

0, 1, 2, 3 - APPROCCIO HLS e PDCA - 11 PUNTI

- Introduzione

1. Scopo e campo di applicazione
2. Riferimenti normativi
3. Termini e Definizioni
4. Contesto dell'Organizzazione (P)
5. Leadership (P)
6. Pianificazione (P)
7. Supporto (D)
8. Attività operative (D)
9. Valutazione delle Prestazioni (C)
10. Miglioramento (A)

4, 5, 6 - FASI

ATTIVITA'	**DOCUMENTI**
Definizione ambito ISMS e i fattori interni ed esterni rilevanti Definizione Ruoli e Responsabilità Identificazione Parti interessate ed esigenze Identificazione Processi Definizione Policy aziendali Identificazione Risorse Identificazione e analisi dei rischi Pianificazione trattamento dei Rischi Selezione di Obiettivi e Controlli Preparazione SOA Approvazione rischi residui	Documento di ambito (sezione) Mappa Processi Policy Asset inventory Elenco Risorse Contratti (es fornitori) Doc gestione rischi (es FMEA rivisto) Procedura di Trattamento Report di Trattamento Lista criteri misurazione Misurazione efficacia trattamenti SOA

6.1.3 - TRATTAMENTO del RISCHIO

- *VALUTAZIONE D'IMPATTO (RISCHI/OPPORTUNITA')*
  - *Appendice A (14 capitoli, 35 obiettivi, 114 controlli)*
  - *Modello/i assessment (147 + 114 check)*
  - *MOP/MdC*
  - *FMEA (rivisto)*

- *in modalità iterativa PDCA*

Politiche per la sicurezza delle informazioni; *Organizzazione della sicurezza delle informazioni;* *Sicurezza delle risorse umane;* *Gestione degli asset;* *Controllo degli accessi;* *Crittografia;* *Sicurezza fisica e ambientale;* *Sicurezza delle attività operative;* *Sicurezza delle comunicazioni;*	*Acquisizione, sviluppo e manutenzione dei sistemi;* *Relazioni con i fornitori;* *Gestione degli incidenti relativi alla sicurezza delle informazioni;* *Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa;* *Conformità*

6.1.3 - TRATTAMENTO del RISCHIO

- *Es. di ISO 27001 FMEA*

Sl.No.	Business / Service	Asset Name	Asset Number	Function	Potential Failure Mode(s)	Potential Technical Effect(s) of Failure	Potential Business Consequence(s) of Failure	Sev	Potential Cause(s)/ Mechanism(s) of Failure	Prob	Current Controls		Det	RPN	Recommended Controls		Responsibility & Target Completion Date	Action Results		New Sev	New Occ	New Det	New RPN
											Preventive Controls	Detective Controls			Preventive Controls	Detective Controls		Implemented Controls: Preventive Controls	Implemented Controls: Detective Controls				
8	Protecting IT Assets	Firewall	5000	To block unauthorized requests	Rules not appropriately configured	IP Spoofing	Diversion of sensitive data traffic, fraud	8	Procedures not followed	2	Procedures available		4	64		Increase audit frequency	XYZ by end Jan 2006		Increase audit frequency	5	3	2	30
4	Protecting IT Assets	Firewall	5000	To block unauthorized requests	Rules not appropriately configured	Entry for External Hackers	Disclosure or modification of business records; prosecution; bad PR; customer defection	7	Procedures not followed	2		Log Monitoring	4	56		Increase audit frequency	XYZ by end Jan 2006		Increase audit frequency	5	3	2	30
9	Protecting IT Assets	Firewall	5000	To block unauthorized requests	Rules not appropriately configured	DDOS Attack	Inability to process electronic transactions; bad PR; customer defection	10	Procedures not followed	2	Procedures available		2	40		Increase audit frequency	XYZ by end Jan 2006		Increase audit frequency	2	5	2	20
7	Protecting IT Assets	Firewall	5000	To identify trusted zones by encryption	User awareness	CIA Compromised	Disclosure of customer database; commercial and privacy issues	5	Procedures not followed	6	Policies Defined		1	30	Not Required	Not Required	Business owner to formally accept risk			5	2	2	20
5	Protecting IT Assets	Firewall	5000	To identify trusted zones by encryption	Authentication mechanism using legacy systems having improper configuration	User may not have access to the requested service	Staff unable to work; backlogs; bad PR	6	Policies not fully implemented	1	Policies Defined		5	30	User Awareness		XYZ by end March 2006	User Awareness		1	5	3	15
3	Protecting IT Assets	Firewall	5000	To block unauthorized requests	Rules not appropriately configured	Entry for External Hackers	Disclosure or modification of business records; prosecution; bad PR; customer defection	7	Procedures not followed	2	Procedures available		2	28		Increase audit frequency	XYZ by end Jan 2006		Increase audit frequency	1	4	2	8
6	Protecting IT Assets	Firewall	5000	To block unauthorized requests	Rules not appropriately configured	DDOS Attack	Inability to process electronic transactions; bad PR; customer defection	10	Procedures not followed	2		Log Monitoring	1	20		Increase audit frequency	XYZ by end Jan 2006		Increase audit frequency	1	4	2	8
2	Protecting IT Assets	Firewall	5000	To identify trusted zones by encryption	Encryption level (56 bit or 128 bit) mismatch	Data will be exposed as plain text	Disclosure of customer database; commercial and privacy issues	7	Policies not fully implemented	2	Policies Defined		1	14	User Awareness		XYZ by end March 2006	User Awareness		2	2	2	8
1	Protecting IT Assets	Firewall	5000	To block unauthorized requests	Rules not appropriately configured	Data Theft	Commercial and privacy consequences	7	Procedures not available	2	Nil		1	14	User Awareness		XYZ by end March 2006	User Awareness		2	2	1	4

7, 8 - FASI (D)

ATTIVITA'	**DOCUMENTI**
Gestione Piano Trattamento Allocazione e formazione risorse Utilizzo controlli Gestione operatività Gestione Risorse Gestione Incidenti sicurezza	Piano Trattamento Piani di formazione Piano di Continuità operativa Registrazioni attività (operative) Procedura gestione incidenti Registro incidenti e NC Cruscotto con indicatori

9 - FASI (C)

ATTIVITA'	**DOCUMENTI**
Monitoraggio Procedure e Controlli Riesame regolare ISMS Riesame delle Direzione	Piani di Audit Procedura di Audit Report degli Audit Verifica efficacia formazione Riesame indicatori Riesame incidenti Controllo SLA Verbali di fase/riunione Verbale di Riesame delle Direzione

10 - FASI (A)

ATTIVITA'	**DOCUMENTI**
Attuazione Piano/i di miglioramento Valutazione efficacia	Piani di Trattamento Procedure di gestione AC e AP

NOSTRO APPROCCIO

- Assessment a 360°
  - **Gestione del Customer DB, Dati Clienti, CRM**
  - **Consulenza legale-contrattualistica**
  - **Supporto informatico (**analisi, audit, **migrazioni verso Cloud,** attività su CRM**)**
- Adeguamento + Formazione incaricati
- **MOP/MdC** (Mod. Organiz. Privacy e Man. Controm.)
- Assessment finale
- Mantenimento

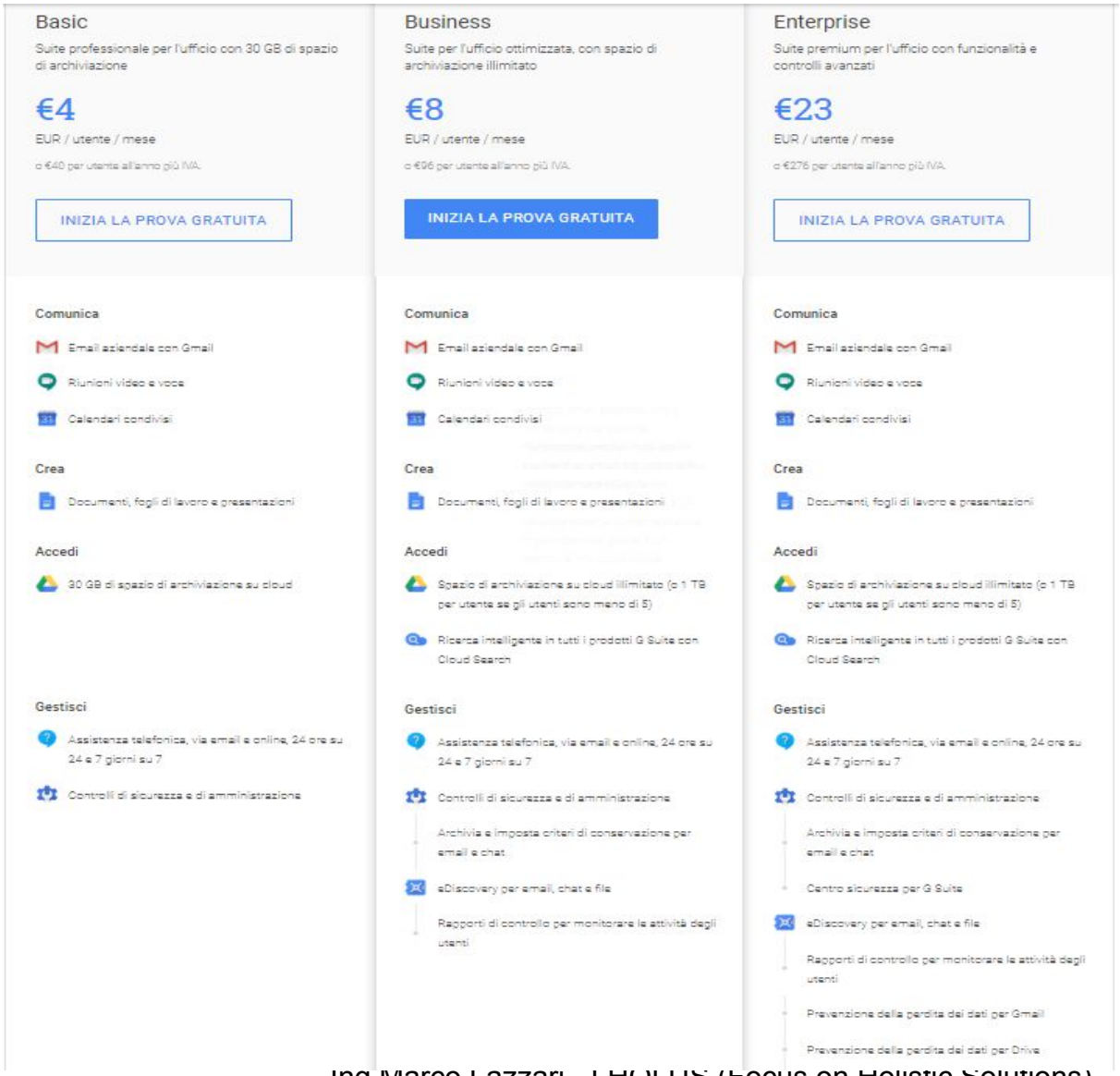
MOP	***MdC***
Analisi, classificazione dati	*Mappatura flusso dati e sistemi*
Gestione Nomine	*Analisi misure di sicurezza adottate*
Verifica valutazione rischio privacy	*Classificazione Informazioni*
Adeguamento informative	*Asset Inventory*
Riesame/definizione contratti coi Responsabili	*Crittografia*
Verifica legittimità trattamento	*Sicurezza fisica/ambientale*
Formazione	*Business Continuity*
Redazione procedura di data breach	*Sicurezza comunicazioni*
Policy di utilizzo dispositivi portatili	*Gestione fornitori*
Procedura riscontro istanze interessati	

SOLUZIONI OPERATIVE

- Migrazione Posta e Dati su Cloud Google G Suite
  - Server in EU (4 location)
  - Aderenza agli standard ISO 27001, 27017, 27018
  - Integrazione con AD Microsoft
  - Console di Governo per la gestione di permessi, strumenti, applicazioni, device, log
  - Trasmissioni dati crittografate
  - Riduzione aprioristica del rischio con l'accesso/la presenza del dato nel solo momento dell'utilizzo
  - Ambiente nativamente collaborativo con apertura semplice e controllata verso l'esterno
  - Gestione efficiente delle versioni file
  - Totale integrazione mondi fisso e mobile (Mac/Win/iOS/Android)
  - Conservazione
  - Disponibilità di un gran numero di applicativi in single-sign-on con la piattaforma
  - Potenziale eliminazione server, relative gestione e costi

SOLUZIONI OPERATIVE

- Cloud Google G Suite - Profili



Basic	Business	Enterprise
Suite professionale per l'ufficio con 30 GB di spazio di archiviazione	Suite per l'ufficio ottimizzata, con spazio di archiviazione illimitato	Suite premium per l'ufficio con funzionalità e controlli avanzati
€4	€8	€23
EUR / utente / mese	EUR / utente / mese	EUR / utente / mese
o €40 per utente all'anno più IVA	o €96 per utente all'anno più IVA	o €276 per utente all'anno più IVA
INIZIA LA PROVA GRATUITA	INIZIA LA PROVA GRATUITA	INIZIA LA PROVA GRATUITA
Comunica	**Comunica**	**Comunica**
Email aziendale con Gmail	Email aziendale con Gmail	Email aziendale con Gmail
Riunioni video e voce	Riunioni video e voce	Riunioni video e voce
Calendari condivisi	Calendari condivisi	Calendari condivisi
Crea	**Crea**	**Crea**
Documenti, fogli di lavoro e presentazioni	Documenti, fogli di lavoro e presentazioni	Documenti, fogli di lavoro e presentazioni
Accedi	**Accedi**	**Accedi**
30 GB di spazio di archiviazione su cloud	Spazio di archiviazione su cloud illimitato (o 1 TB per utente se gli utenti sono meno di 5)	Spazio di archiviazione su cloud illimitato (o 1 TB per utente se gli utenti sono meno di 5)
	Ricerca intelligente in tutti i prodotti G Suite con Cloud Search	Ricerca intelligente in tutti i prodotti G Suite con Cloud Search
Gestisci	**Gestisci**	**Gestisci**
Assistenza telefonica, via email e online, 24 ore su 24 e 7 giorni su 7	Assistenza telefonica, via email e online, 24 ore su 24 e 7 giorni su 7	Assistenza telefonica, via email e online, 24 ore su 24 e 7 giorni su 7
Controlli di sicurezza e di amministrazione	Controlli di sicurezza e di amministrazione	Controlli di sicurezza e di amministrazione
	Archivia e imposta criteri di conservazione per email e chat	Archivia e imposta criteri di conservazione per email e chat
	eDiscovery per email, chat e file	Centro sicurezza per G Suite
	Rapporti di controllo per monitorare le attività degli utenti	eDiscovery per email, chat e file
		Rapporti di controllo per monitorare le attività degli utenti
		Prevenzione della perdita dei dati per Gmail
		Prevenzione della perdita dei dati per Drive

SOLUZIONI OPERATIVE

- Cloud Google G Suite
  - Gestione dispositivi mobili

GDPR - ALCUNE PILLOLE

- *L'utente con cui accedete ai vs pc è amministratore?*
- *Usate pwd sufficientemente complesse? Le modificate spesso? Dove, come le conservate? Usate la verifica in due passaggi?*
- *I pc sono tenuti aggiornati? Dispongono di buoni AV, antispam, antipishing, antimalware, ecc?*
- *Anche quelli in officina o in sedi dislocate o home office?*
- *Fate i backup? Quanti? Dove?*
- *Avete testato il restore?*
- *Gli utenti sono formati ad autoproteggersi e a tenere comportamenti consoni?*
- *E i Vs clienti, contatti, fornitori con cui scambiate dati continuamente o a cui fornite accessi?*
- *E i dispositivi mobili: dispongono di S.O. di ultima generazione? Sono tenuti aggiornati? Sono controllati negli scaricamenti di app? Le app sono aggiornate?*

GDPR - ALCUNE PILLOLE

- Password Manager
  - Keepass (opensource) - Win/Mac/Linux/iOS/Android
    - https://keepass.info/download.html
    - File KDBX conservato su Cloud Google
  - Lastpass
  - Onesafe
  - Keeper
  - Kaspersky
  - Dashlane
  - Passwordbox

Grazie….

Q & A …

Contatti

- Dott.ssa Elisa Fontana
  C-Direct Consulting
  email: elisa.fontana@cdirectconsulting.it
  tel.: +39.349.0902423

- Avv. Barbara De Cillis
  Studio Legale DDS
  email: barbara.decillis@studiolegaledds.it
  tel.: +39.051.5884467

- Ing. Marco Lazzari
  L.HOL.US *(focUS on HOLystic sOLUtions)*
  email: marco.lazzari@lholus.com
  tel.: +39.327.4677205

Credits

- UNI, ISO
- ISMS Online
- IQC
- ClusIT
- Ing. Giorgio Sbaraglia
- Ordine Ingegneri Bologna