# CYBER SECURITY E SMART WORKING:
## LE BUONE PRATICHE PER METTERE IN SICUREZZA LA TUA IMPRESA


**Sandro Di Giovanni**

Cyber Security - IT Manager - System Administrator - sandro.dg@digisconsult.com

**329 80 59 655**

https://www.linkedin.com/in/sandro-di-giovanni-4ba9bb39/

# BREVE RIFERIMENTO AL GDPR

Il 25 Maggio 2018, in tutti gli stati europei viene applicato un regolamento generale, valido per tutti gli stati dell'unione il GDPR.


Il principio di **accountability** (letteralmente "principio di responsabilizzazione") pone, in capo al titolare del trattamento, l'onere di provare la conformità della propria struttura organizzativa e procedurale in ambito privacy alla normativa di settore.
**Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento**. Dette misure sono riesaminate e aggiornate qualora necessario (art. 24)

# BREVE RIFERIMENTO AL GDPR art. 32

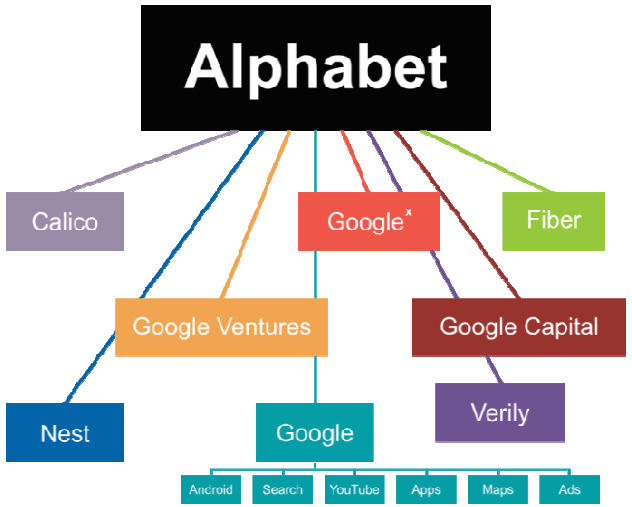
1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle **persone fisiche**, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) **la pseudonimizzazione** e la **cifratura** dei dati personali; b) la capacità di assicurare su base permanente la **riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi** e dei servizi di trattamento; c) la capacità di **ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico**; d) **una procedura per testare, verificare e valutare** regolarmente **l'efficacia delle misure tecniche e organizzative** al fine di garantire la sicurezza del trattamento.

(83) Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

# IMPORTANZA DEI DATI

Da molti definiti il nuovo petrolio, i dati, sono in assoluto il valore più grande del momento, ce lo fanno capire la corsa ad accaparrarsene il più possibile e la legislazione che rincorre gli eventi per mettere un freno e regolamentare il trattamento

amazon




Alibaba.com™

Microsoft

# IMPORTANZA DEI DATI

Ora proviamo ad immaginare cosa succederebbe se di punto in bianco dovessimo rimanere senza dati. Perdendo anche lo smartphone e l'agenda cartacea dei contatti.

Come prima cosa per evitare ulteriori danni, dovremmo denunciare il data brech al garante, anche se sarebbe il nostro ultimo problema.

Chi poterebbe essere stato?

# LE MINACCE (MALWARE)

Spyware

Adware

Worm

Trojan

Ransomware

RootKit

Phishing

# SINTOMI (MALWARE)

**Di seguito sono riportati alcuni segni comuni, che vi possono far pensare di aver contratto un'infezione da malware:**

1 - Ridotta funzionalità dei programmi e dell’accesso ad internet.

2 - Uno o più browser web che smettono di funzionare completamente oppure la pagina iniziale viene modificata.

3 - Popup di annunci intrusivi che ti inondano lo schermo.

4 - Arresti anomali e frequenti, del computer o dei programmi.

5 - Lo spazio dell’hard disk diminuisce senza ragione.

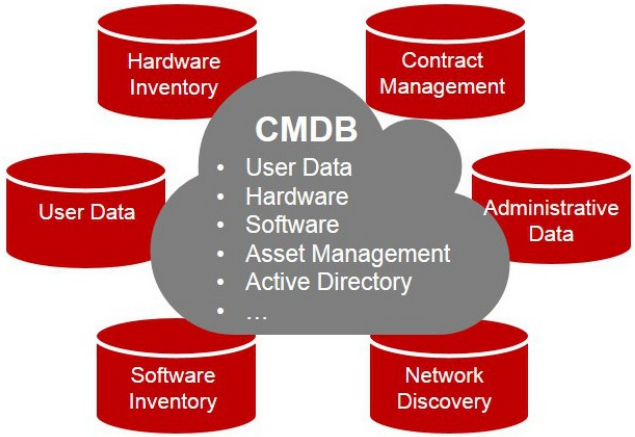
6 - I tuoi contatti si lamentano di ricevere da te e-mail strane e insignificanti oppure (peggio) con link che non funzionano.

Come ci proteggiamo…..

# INDIVIDUAZIONE DEGLI ASSETS

La prima cosa da fare, è comprendere cosa dobbiamo proteggere ( anche se sembra banale dirlo) dobbiamo capire quali sono, dove si trovano e con quali strumenti gestiamo i dati.

C’è chi usa il database dei database, acronimo CMDB (Configuration management database). Questo database mette in relazione tutti gli utenti, computer, server, servizi, procedure.




Ovviamente alle PMI non viene richiesto di dotarsi di questi strumenti, ma un buon punto di partenza è avere un inventario degli assets o quantomeno averli ben presenti.

# CONNESSIONE

Bisogna intanto avere una buona base di partenza

Non diamo nulla per scontato, **sconsigliando** le connessioni ”Home”

Una buona connessione aziendale (soprattutto se pensata per lo smartworking) dovrebbe avere come requisiti minimi:

- Un contratto di tipo business
- Almeno n.1 IP Fisso
- Una buona banda
- Una connessione di backup es. SIM (in un’ottica di business continuity)

# SWITCH

E’ uno degli asset principali infrastrutturali.

Tutti sappiamo che consente di far comunicare tra loro gli apparati di rete.

Ma non tutti sanno che gli switch non sono tutti uguali a tal punto che per gestirli spesso ci si affida a degli specialisti di rete.

Ad esempio una funzione , tra le più utili, in ambito cybersec è quella di poter “chiudere” le porte inutilizzate, ma anche suddividere la rete in VLAN.

# WIFI

Il concetto fondamentale da tenere a mente è che la reale estensione di una WLAN supera i confini fisici dell'edifico in cui è installata.


- Configurare SSID in modo che non venga visualizzato
- Utilizziamo password complesse e crittografia WPA2
- Evitiamo disabilitandolo il WPS e se proprio non possiamo farne a meno usiamolo con il PIN
- Separiamolo dalla rete LAN se non è necessario connettervi strumenti che utilizzano i servizi presenti su quest'ultima rete.

**- Impostiamo lo spegnimento del wifi in automatico se nelle ore serali e nei week end o quando in azienda non c'è nessuno.**

# UTM

Volutamente non ho parlato di Firewall, perché oggi, le imprese di tutte le dimensioni, a costi abbordabili, possono avvalersi di veri e propri partner virtuali, che offrono servizi proattivi di gestione delle minacce.

L'evolversi delle metodologie di attacco, ha fatto si che si debba ricorrere a soluzioni sempre più sofisticate e competenze sempre maggiori per la protezione dei dati. Gli UTM forniscono un insieme di funzionalità adatte allo scopo e **consentono di gestire in modo unificato le minacce.**

Tra alcune delle funzionalità più note troviamo, **firewall**, **gestione profili**, IPS/IDS, DPI, Bilanciamento del carico di rete WAN e Failover, etc. In modo particolare possono tornare utili quando si parla di smart working, perché risultano essere dei veri e propri server per la gestione del traffico di rete incluse le **VPN**

# PRIVILEGI UTENTE

## Che si abbia una rete gestita o meno…

La gestione degli utenti, permette di associare le persone a determinati profili

Usiamo gli account Root o Administrator, solo per creare un altro account con profilo amministratore dal quale **disabiliteremo** quello di default.
Una persona competente (solitamente l'amministratore di sistema) lo userà solo per le prime configurazioni e le installazioni dei programmi necessari, ma in scenari di lavoro quotidiano meglio lasciarlo disattivato.

Tutti gli account **devono avere una password d'accesso**, anche quelli disabilitati, perché se ad esempio, lasciamo l'utente amministratore senza password, un virus lo potrebbe riabilitare, e dal momento che non è protetto, viene regalato il controllo dell'apparato.

Queste impostazioni devono essere applicate di base ai PC/Server , ma valgono per tutti gli apparati di rete.

# PRIVILEGI UTENTE

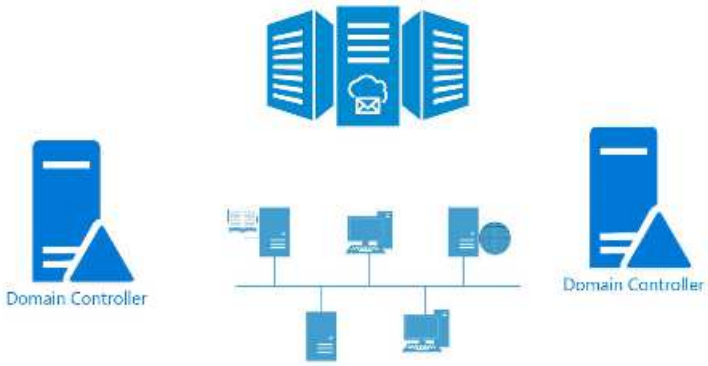
## Cosa può capitare ad un pc con utente administrator (poco pratico) in rete

Rendere difficoltosa l'amministrazione del PC cambiando la password del reale amministratore.
Compromettere il Sistema Operativo della propria macchina, anziché solo il suo profilo.
Installare programmi potenzialmente pericolosi o incompatibili per il sistema operativo.
Corrompere l'ambiente necessario ai programmi aziendali o corrompere i programmi stessi
Perdere la configurazione delle stampanti locali o di rete
Cambiare la configurazione della connessione alla rete locale (IP, DNS, ….)
Cambiare la configurazione della connessione alla rete internet (gateway, proxy, ….)
Installare un hotspot e bypassare tutte le protezioni perimetrali aziendali
Disinstallare o rendere inefficace l'antivirus aziendale
Navigare su internet con poteri da amministratore e rendere così amministratore un eventuale malintenzionato esterno il quale a sua volta potrebbe attaccare la rete aziendale o una rete esterna (testa di ponte e computer zombie).
Permettere (anche involontariamente) l'installazione di codici malevoli quali worms, backdoor, keylogger, trojan horse, ecc infettando l'intera macchina.
Installare un altro browser e cosi  bypassare tutte le protezioni aziendali
……
…..

# GESTIONE POLITICHE AZIENDALI

## IL CONTROLLER DI DOMINIO

Per gestire al meglio quanto appena detto, Dobbiamo introdurre il concetto di **dominio,** che è un insieme di sistemi che utilizzano risorse di rete e database utenti secondo una regolamentazione comune, dettata dall'amministratore di sistema.

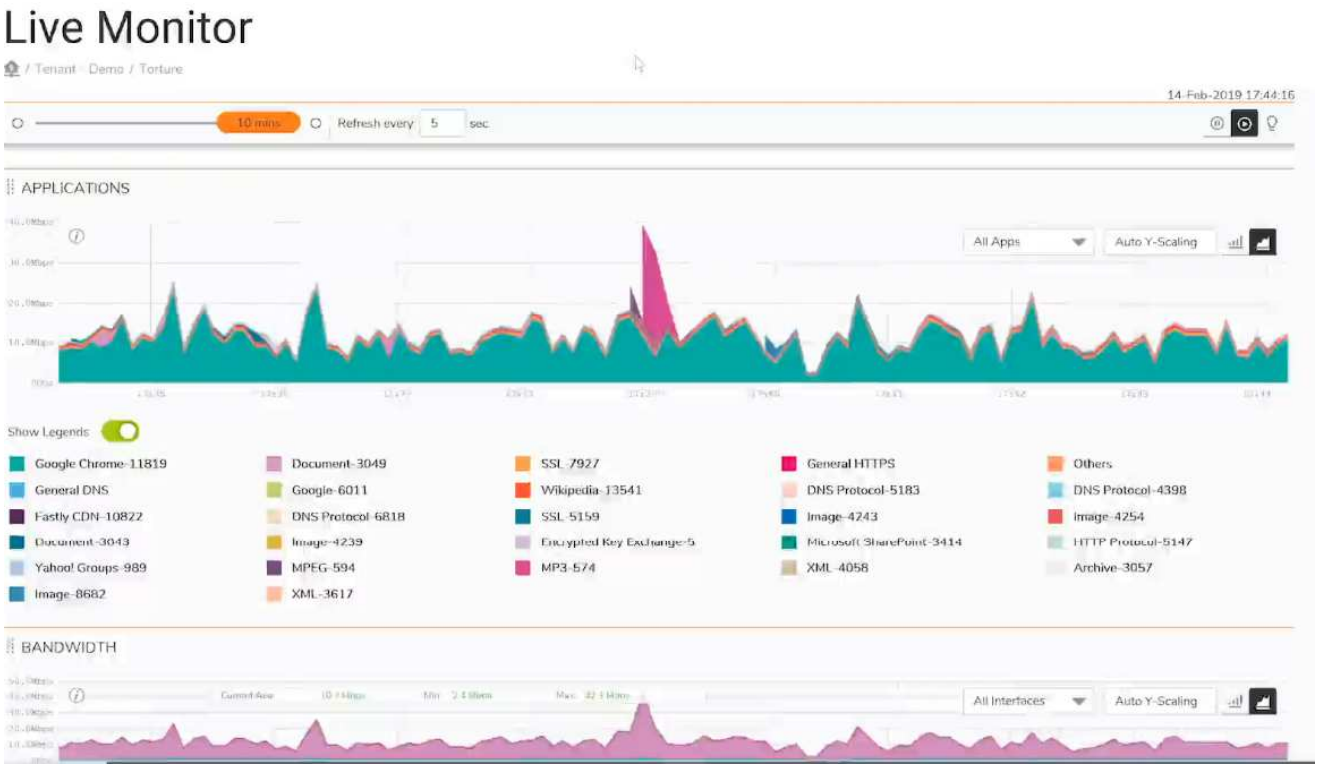



Uno o più controller di dominio, in una rete Microsoft based, consentono di gestire al meglio dai privilegi degli utenti, fino alle policies di funzionamento del singolo computer.

# ANTIVIRUS

Gli antivirus non sono tutti uguali, ci sono quelli di nuova generazione, che controllano il comportamento del sistema, attenuano gli attacchi, prima dopo e durante la loro esecuzione e poi ci sono gli altri con il superato sistema a firme.

**In ogni caso, assicuriamoci che ci siano e siano aggiornati**



# ANTIVIRUS

Alcuni sono parte integrante di un sistema UTM e gestiscono le vulnerabilità con una visione globale dell'intero ecosistema di rete sfruttando l'intelligenza artificiale e Machine learning.

# NAS

## Veri e propri server

Pensati nativamente solo per lo storage, oggi dispongono di funzioni evolute, sono utilizzati per la condivisione dei dati in rete, rendendoli disponibili per diverse piattaforme.

All'interno hanno più dischi per fare le più disparate configurazioni **RAID**.

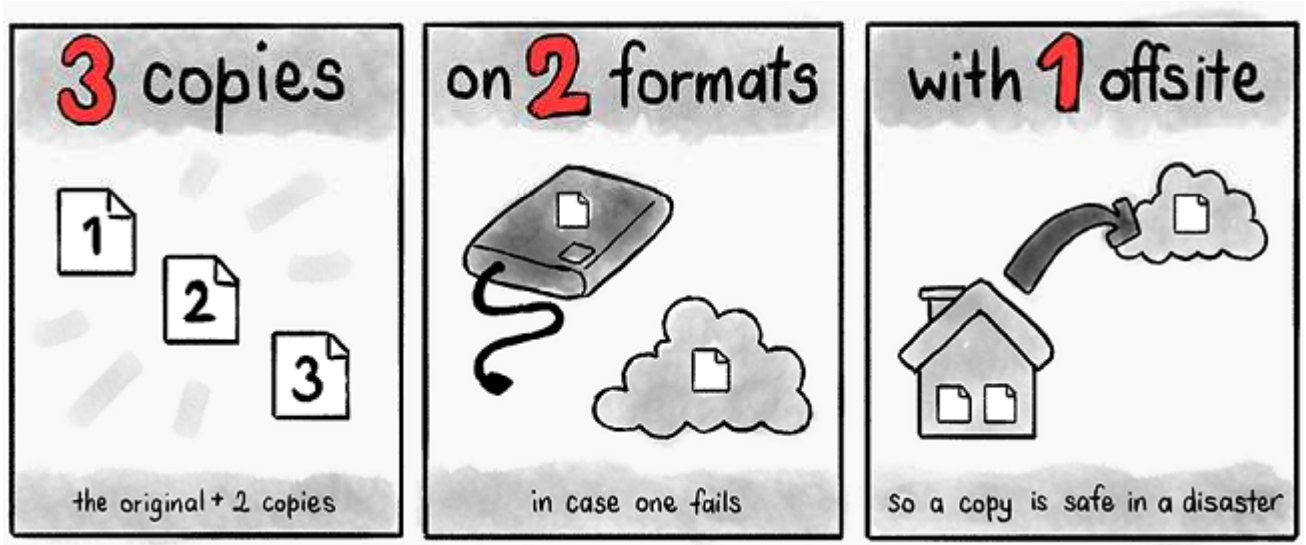
Si possono interfacciare con un domain controller per la gestione delle utenze o possono gestire utenze locali.

Un ottimo uso che si può fare della porta usb è il collegamento di un disco esterno di backup

# BACKUP

## …Regola 3-2-1

Per dormire sonni abbastanza tranquilli, una buona regola di backup è la seguente




**Avere 3 COPIE, dello stesso dato**

**Farla su 2 media differenti**

**Averne 1 SU un SITO REMOTO**

N.B. NESSUNO BACKUP E' PERFETTO…fare sempre verifiche quotidiane e test di ripristino

# APPLICAZIONI DI WEBMEETING

Ce ne sono molte, gratuite e a pagamento.

https://zoom.us/

https://meet.jit.si/

Whatsapp, skype, bluejeans

# APPLICAZIONI DI WEBMEETING

## Furto delle password, possesso di webcam e microfono, accesso e conferenze registrate

e molto altro accedere con i software di videoconferenza.

**Nicola Vanin** • 1°
Data Governance & Information Security Manager | Artificial Intelligence Auditor | 5G
1s • Modificato •

La "S" in #Zoom, sta per #sicurezza
Il #software di videoconferenza #Zoom salito alle stelle in popolarità a causa dell'epidemia di #coronavirus , si sta rapidamente trasformando in un incubo per la #privacy e la #sicurezza.
Due ricercatori di sicurezza che hanno trovato un #bug nella piattaforma Zoom che può essere abusato per rubare le #password di Windows.
Un altro ricercatore di sicurezza ha scoperto 2 bug che possono essere utilizzati per assumere il controllo del Mac di un utente Zoom, incluso #webcam e il #microfono.

Questo non è l'unico problema relativo alla privacy / alla sicurezza che è stato scoperto in Zoom nelle ultime due settimane.
Proprio ieri si è scoperto che Zoom non utilizza una connessione crittografata end-to-end per le sue chiamate, nonostante affermi di farlo.
In conclusione, se come datore di lavoro ti preoccupi della #sicurezza e #privacy, smetti di usare #Zoom.

# APPLICAZIONI DI WEBMEETING

E’ bene dire che l’azienda è subito corsa ai ripari.

**Nicola Vanin** • 1°
Data Governance & Information Security Manager | Artificial Intelligence Auditor | 5G
2 giorni • Modificato •

Non 1, non 2 , ma un comitato di #CISO
#Zoom annuncia la creazione di un Consiglio #CISO ( chief information security officer) per aiutare il suo CEO Eric Yuan nelle questioni relative alla #sicurezza e alla #privacy degli utenti
"All'interno del nostro Consiglio CISO, stiamo istituendo un comitato consultivo che includerà un sottoinsieme di #CISO che fungeranno da consulenti per me personalmente", ha detto Yuan.
"Questo gruppo mi consentirà di essere un leader più efficace e attento e contribuirà a garantire che la #privacy e la sicurezza siano in prima linea in tutto ciò che facciamo in Zoom.
Inoltre l'ex Chief Security Officer (CSO) di #Facebook e #Yahoo Alex Stamos si unisce a Zoom come consulente esterno per la sicurezza.

E' utile sapere che ad oggi + del 38% delle aziende presenti nell'elenco #Fortune 500 non ha un #CISO

# Skype

Una buona applicazione, per comunicare con un buon livello di sicurezza è skype, disponibile anche nella versione business, permette di fare videochiamate, condividere desktop e inviarsi messaggi instantanei.

# Lavorare da remoto

## Teamviewer – AnyDesk – RDP

**Sono dei programmi che consentono di prendere da remoto il controllo della postazione, praticamente utilizzando una tastiera e un mouse di una postazione remota, posso controllare un PC in rete**

**(attenzione alla privacy lo schermo potrebbe essere visto all'insaputa dell'utente)**

**L'accesso avviene tramite un ID e una password preimpostate (oppure l'IP se in VPN)**

## Suite di programmi in Cloud

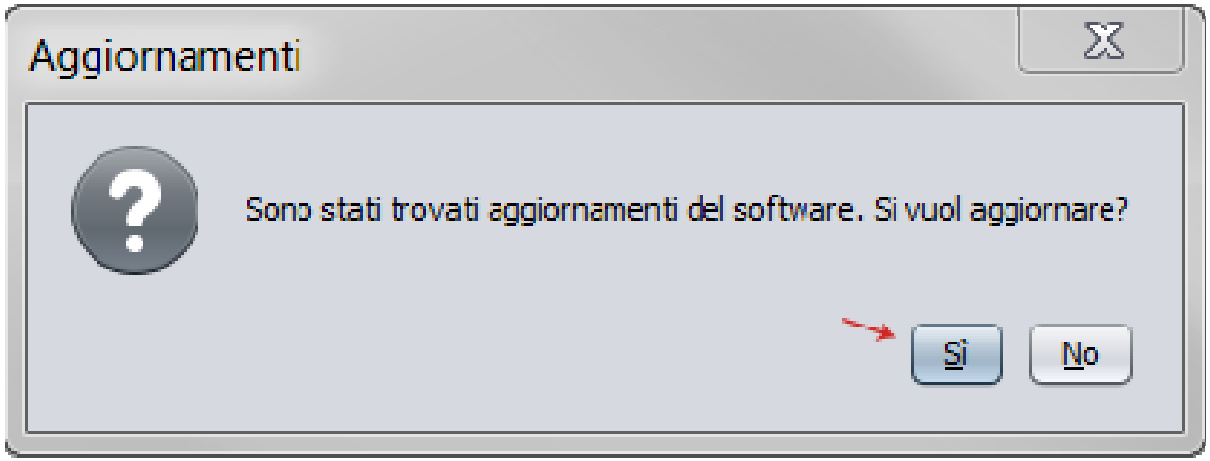
Office 365 – Gsuite, sono pacchetti software che permettono di condividere uno spazio, su un server remoto dal quale è possibile anche lavorare con delle applicazioni office (dati a terzi e fuori europa)

## Connessione VPN alla rete

**Come più volte specificato, a mio avviso, il miglior metodo che abbiamo, anche se vogliamo combinarlo ad una applicazione di controllo remoto del desktop, è sempre la creazione di una VPN, la possiamo fare con un firewall e può essere configurata sia LAN-to-LAN, che per singolo accesso dall'esterno.**

# AGGIORNAMENTI VERSIONI

Ogni produttore che si rispetti, rilascia degli aggiornamenti di volta in volta che aggiunge nuove funzionalità al proprio software o rileva dei bug.




Di solito…..

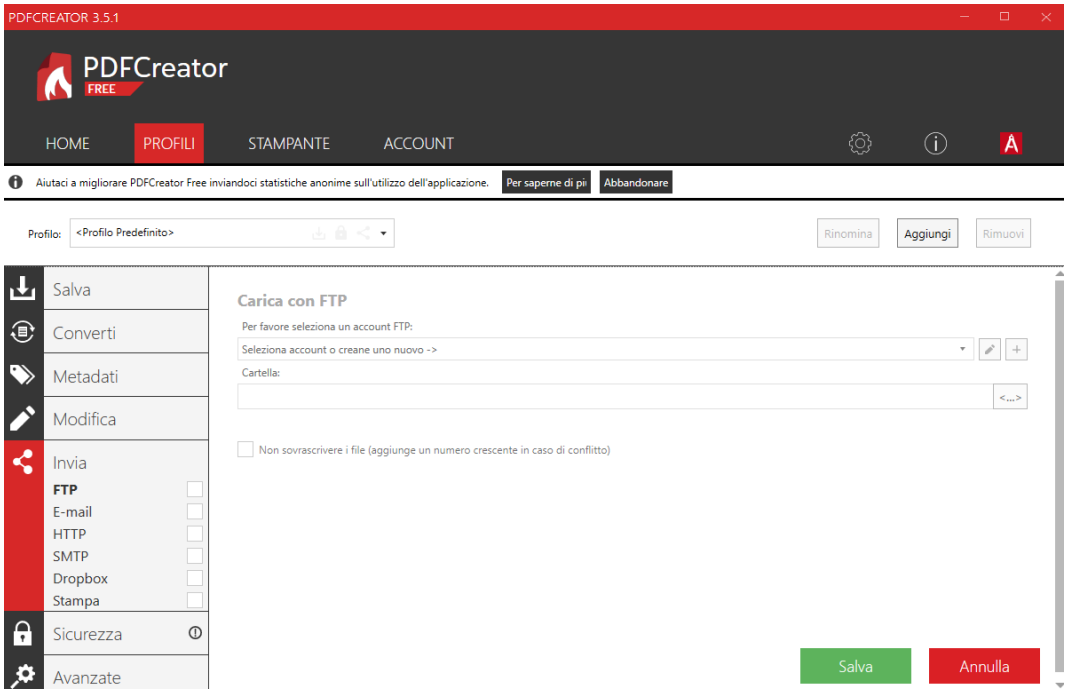
perché **non** abbiamo tempo

perché abbiamo **paura di perdere** la tanto amata **configurazione personalizzata**

CHE FACCIAMO??

# STAMPA

Per chi avesse ancora necessità di stampare, consiglio l'uso di un software per la creazione di "stampe" in pdf, il software PDF creator oltre ad essere gratuito, è un prodotto che permette di selezionare diverse opzioni, tra cui la gestione dei profili e consente di creare delle stampanti virtuali, anche qui le stampe possono circolare in diversi modi, **meglio tramite VPN** che su servizi esterni.



# TELEFONIA

**In un contesto di smart working che si rispetti, anche la reperibilità telefonica deve essere considerata dal punto di vista aziendale. Per forza di cose entra in gioco il VOIP, per fare in modo che si possa rispondere dalla propria postazione remota come se si fosse presenti in azienda, ci sono diverse soluzioni.**

**Ne descriverò fondamentalmente 2 che prevedono 2 soluzioni differenti**
**La prima, in uno scenario aziendale dotato di VPN**

**La seconda, in uno scenario che espone il centralino Voip direttamente all'esterno** (per ovvi motivi preferisco di gran lunga la prima).

# SECURITY AWARENESS

- Volutamente non ho parlato solo di formazione, non perché questa non sia necessaria, anzi, ma perché sull'argomento, va aumentata la consapevolezza della sicurezza.
- Bisogna coinvolgere gli utenti e attrezzali contro gli attacchi informatici reali, avvalendoti di una formazione personalizzata e basata su servizi di intelligence sulle minacce. I contenuti per tutti, non stanno avendo successo, basta un solo click per ritrovarsi la rete crittografata.
- La formazione è un must, sancito anche dall'art.29 del GDPR. Il titolare (per il suo interesse) deve istruire il dipendente al fine di trattare in maniera conferme il dato personale.

# Log management, gestire i file di log per la sicurezza aziendale

Ogni apparato nella nostra rete produce LOG.

I LOG rappresentano un insieme di dati dai quali si può risalire alle operazioni compiute sui sistemi informatici.

Spesso però, essendo prodotti da apparati con specifiche diverse tra loro non sono semplici da comprendere in modo immediato.

# Log management: il SIM

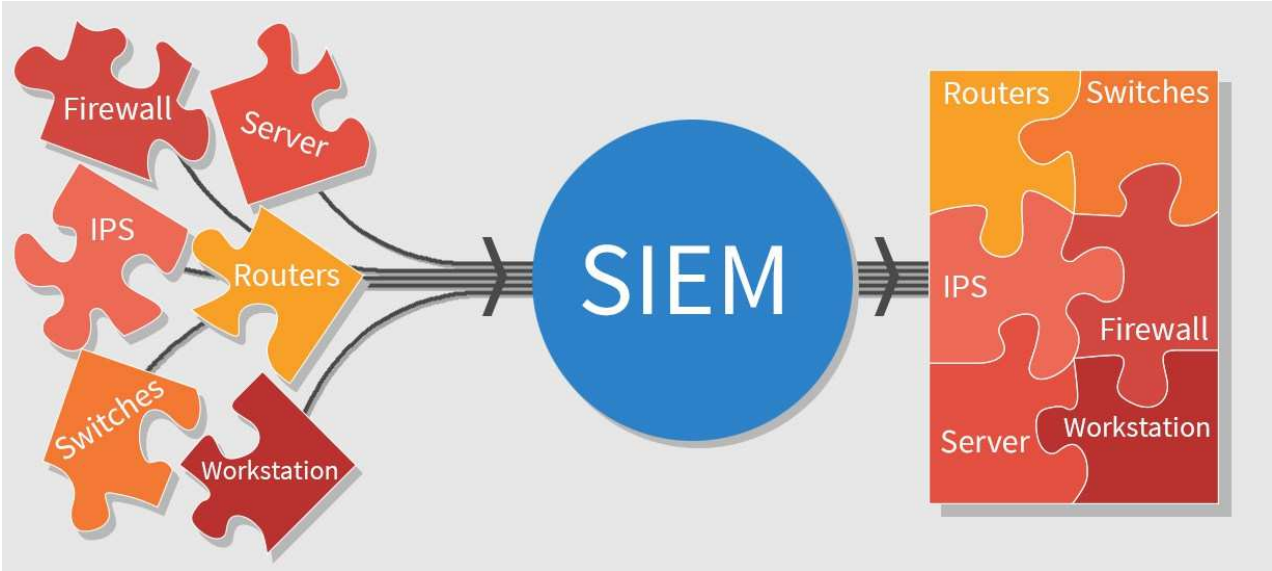
Per venir meno al problema di gestione delle informazioni generate dai LOG ed aggregare i dati, nascono i SIM, Security Information Management, che consentono di raccogliere dati in tempo reale delle apparecchiature che si vuole monitorare.

La raccolta avviene con protocolli standard e/o agenti installati sulle varie macchine. Possono essere utilizzati per l'analisi forense.

# Log management: il SIEM

Il passo da SIM a SIEM è breve.

Vista la quantità di informazioni raccolte, dal momento che ogni apparato produce molti LOG, per poterli analizzare entra in gioco il SIEM. Che è un software che viene affiancato a un database di raccolta LOG per analizzare e correlare eventi, sia in tempo reale che in differita per creare reportistica.



# CERTIFICAZIONI

**Lo standard internazionale che certifica la sicurezza delle informazioni è**

## ISO 27001

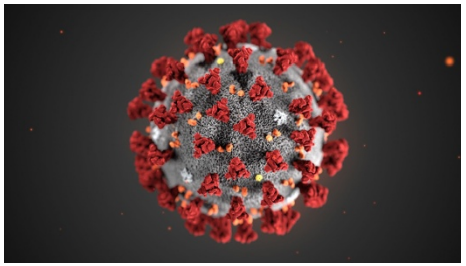
ISO 27001 è lo standard internazionale che definisce i requisiti di un sistema di gestione della sicurezza delle informazioni (SGSI, anche conosciuto con l'acronimo inglese ISMS). Un ISMS è un insieme di politiche, procedure, processi e sistemi che gestisce i rischi delle informazioni, come gli attacchi informatici, le violazioni dei dati, la perdita o il furto dei dati.

# CONCLUSIONI ☺

GRAZIE!!! ☺

#iorestoacasa

## UN CONSIGLIO
## NON RACCOGLIETE IN AZIENDA
## DATI SUL CORONAVIRUS



- L'accertamento e la raccolta di informazioni relative ai sintomi tipici del Coronavirus e alle informazioni sui recenti spostamenti di ogni individuo spettano agli operatori sanitari e al sistema attivato dalla protezione civile, che sono gli organi deputati a garantire il rispetto delle regole di sanità pubblica recentemente adottate.

- Resta fermo l'obbligo del lavoratore di segnalare al datore di lavoro qualsiasi situazione di pericolo per la salute e la sicurezza sui luoghi di lavoro. Al riguardo, il Ministro per la pubblica amministrazione ha recentemente fornito indicazioni operative circa l'obbligo per il dipendente pubblico e per chi opera a vario titolo presso la P.A. di segnalare all'amministrazione di provenire da un'area a rischio. In tale quadro il datore di lavoro può invitare i propri dipendenti a fare, ove necessario, tali comunicazioni agevolando le modalità di inoltro delle stesse, anche predisponendo canali dedicati; permangono altresì i compiti del datore di lavoro relativi alla necessità di comunicare agli organi preposti l'eventuale variazione del rischio "biologico" derivante dal Coronavirus per la salute sul posto di lavoro e gli altri adempimenti connessi alla sorveglianza sanitaria sui lavoratori per il tramite del medico competente, come, ad esempio, la possibilità di sottoporre a una visita straordinaria i lavoratori più esposti.

https://www.linkedin.com/in/sandro-di-giovanni-4ba9bb39/