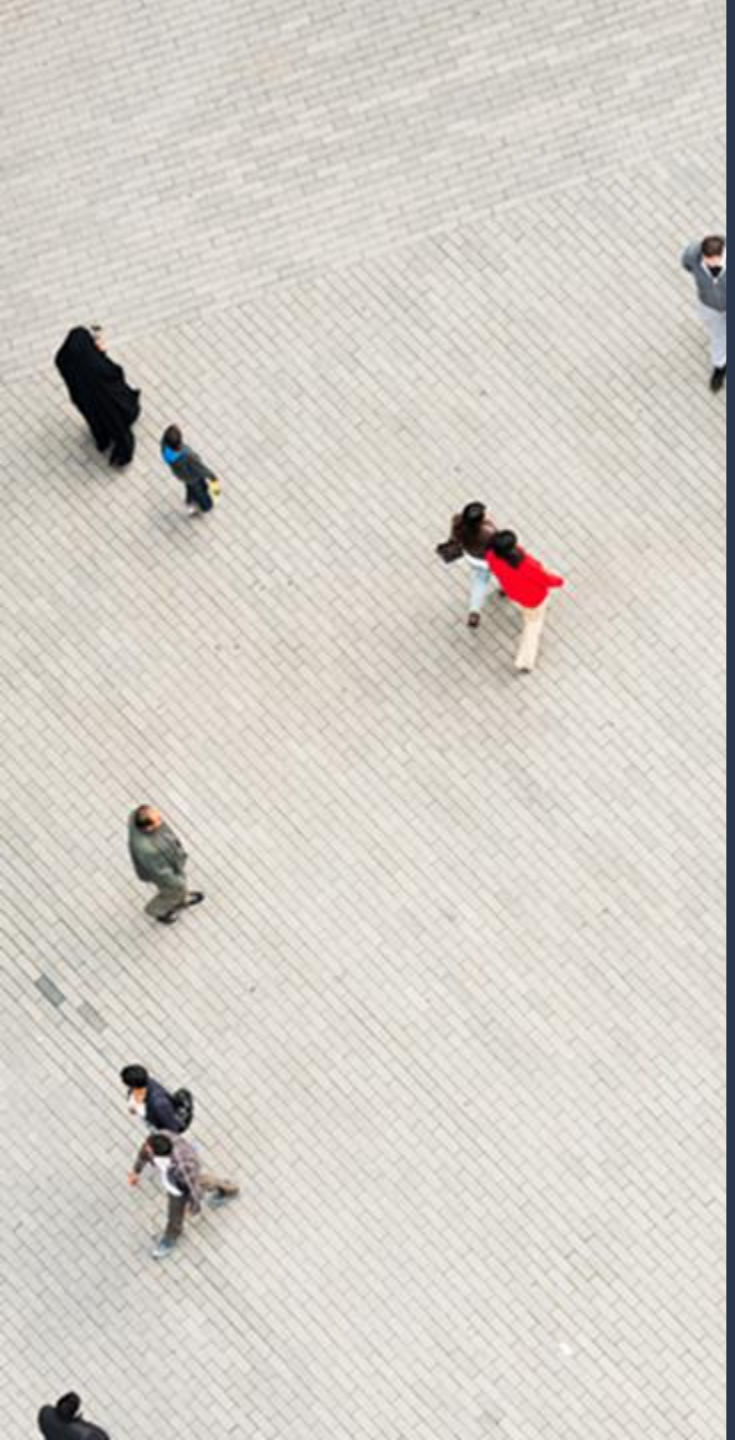


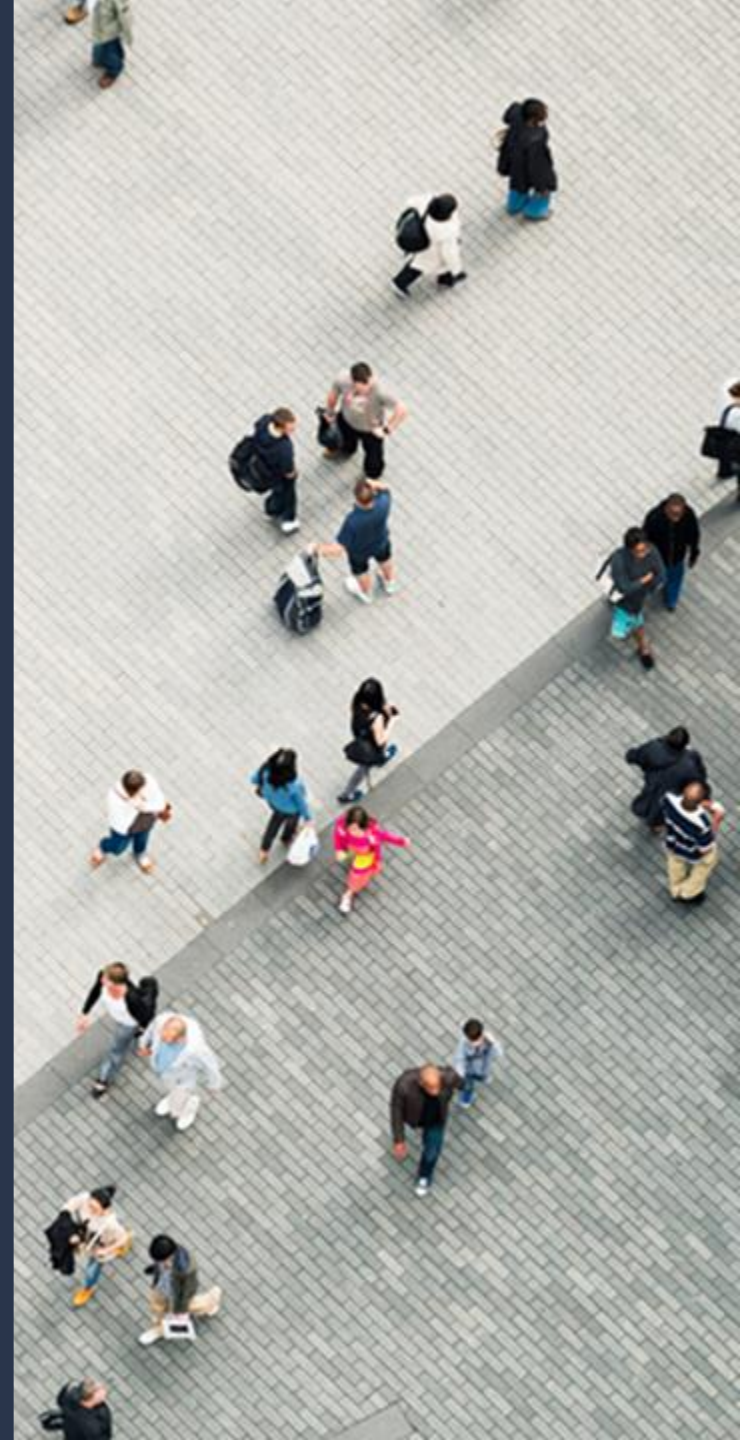
RegioneEmilia-Romagna

Cybersecurity

Tavolo Tecnologie – Aprile 2021

VELA
VELOCE
LEGGERO
AGILE
EMILIA-ROMAGNA SMART WORKING

Questo prodotto è stato realizzato con il supporto di **SCS AzionInnova Spa** nell'ambito delle forniture relative al progetto VELA-Emilia-Romagna Smart Working.



TAVOLO TECNOLOGIE – Focus Sicurezza

- Agenda in poche parole

  - Kit VELA
  - Esperienza Regione E-R
  - L'ingrediente essenziale…

TAVOLO TECNOLOGIE – Focus Sicurezza

Accesso ai servizi in VPN/SSL: NECESSARIO

	• Richiedere un'attività minima da parte dell'utente in caso di accesso con dispositivi aziendali sia con dispositivi personali (introducendo alcune limitazioni funzionali)
	
	• Avvenire in completa trasparenza valido in caso di accesso con dispositivi aziendali (nessuna attività richiesta)

ACCESSO SICURO

 **Must: : M**inimo

 **Should:** Auspicabile

 **Could:** Massima efficacia

RegioneEmilia-Romagna

EMILIA-ROMAGNA SMART WORKING

TAVOLO TECNOLOGIE – Focus Sicurezza

Certificazione del dispositivo da cui si accede: NON NECESSARIO

	• Offrire l'apertura dell'accesso ai servizi da qualsiasi rete pubblica o privata facendo ricorso a modalità di autenticazione sicure (dual factor authentication se il collegamento avviene da dispositivi non certificati)
	
	

DEVICE SICURO

 **Must: : M**inimo

 **Should:** Auspicabile

 **Could:** Massima efficacia

RegioneEmilia-Romagna

EMILIA-ROMAGNA SMART WORKING

TAVOLO TECNOLOGIE – Focus Sicurezza

Aggiornamenti di sicurezza e applicativi in mobilità: NECESSARIO

	• Offrire l'apertura dell'accesso ai servizi da qualsiasi rete pubblica o privata facendo ricorso a modalità di autenticazione sicure (dual factor authentication se il collegamento avviene da dispositivi non certificati)
	
	• Offrirla con connettività 4G (o superiore)

APP SICURE

 **Must: : M**inimo

 **Should:** Auspicabile

 **Could:** Massima efficacia

RegioneEmilia-Romagna

EMILIA-ROMAGNA SMART WORKING

TAVOLO TECNOLOGIE – Focus Sicurezza

Adozione di una piattaforma di Asset Management/MDM: NON NECESSARIO

	• Consentire il controllo/gestione remota dei device in dotazione
	• Offrire servizi di assistenza remota
	

CONTROLLO SICURO

Must: : Minimo

Should: Auspicabile

Could: Massima efficacia

TAVOLO TECNOLOGIE – Focus Sicurezza

Analisi del traffico sviluppato da remoto da VPN: NECESSARIO

	• Essere in linea con le analisi del traffico int r.et aziendale
	
	

TRAFFICO SICURO

 **Must: : M**inimo

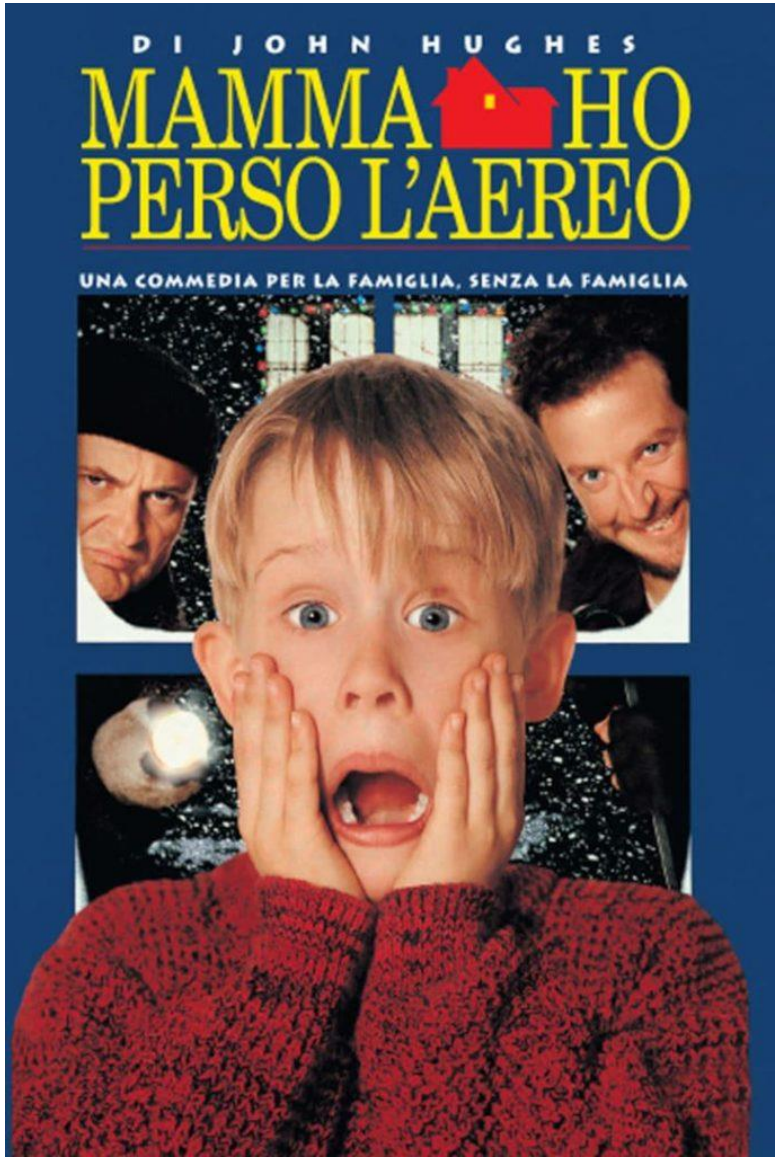
 **Should:** Auspicabile

 **Could:** Massima efficacia

RegioneEmilia-Romagna

EMILIA-ROMAGNA SMART WORKING

TAVOLO TECNOLOGIE – Focus Sicurezza



Regione Emilia-Romagna

EMILIA-ROMAGNA
SMART WORKING

TAVOLO TECNOLOGIE – Focus Sicurezza

- Smart working ordinario e straordinario
  - Il «computer di casa»: limiti e antivirus

- Dotazioni aziendali: notebook e smartphone
  - Accessi VPN diversificati non una sola e unica soluzione
    - Microsoft VPN Always On
    - Check Point VPN

- Esigenze puntuali? Citrix e l'accesso ad applicazioni specifiche (es. SAP GUI)

RegioneEmilia-Romagna

TAVOLO TECNOLOGIE – Focus Sicurezza

- VPN Check Point:
  - VPN Site-to-Site dedicati all'automazione fra sistemi con altri Enti
  - VPN mobile access sia con client che via browser (MAB) attivo già da anni come prima soluzione per la gestione dei Telelavoratori con PdL Regionale e collegamenti ad Internet privati e per gli accessi puntuali con configurazione ad-hoc in funzione dei servizi da raggiungere dei consulenti delle ditte fornitrici identificati tutti nominalmente
    - Accreditamento utenti
- Procedura di validazione delle VPN (Provisioning e Deprovisioning)

TAVOLO TECNOLOGIE – Focus Sicurezza

AMBITI DI CRITICITA’

Smartworking in sicurezza

- aggiornamento costante dei sistemi
- corretto utilizzo delle dotazioni informatiche
  secondo le policy dell’Ente
- strong authentication

TAVOLO TECNOLOGIE – Focus Sicurezza

La sicurezza informatica è un processo che coinvolge tutte le aree e le strutture della Regione Emilia-Romagna in collaborazione con le Direzioni Generali di Giunta e AL, le Agenzie ed Istituti e tutti gli EE.LL collegati.

NORME e LINEE GUIDA

POLICIES e PROCEDURE

FORMAZIONE e SENSIBILIZZAZIONE

CONTROLLO

TENOLOGIA

RegioneEmilia-Romagna

EMILIA-ROMAGNA
SMART WORKING

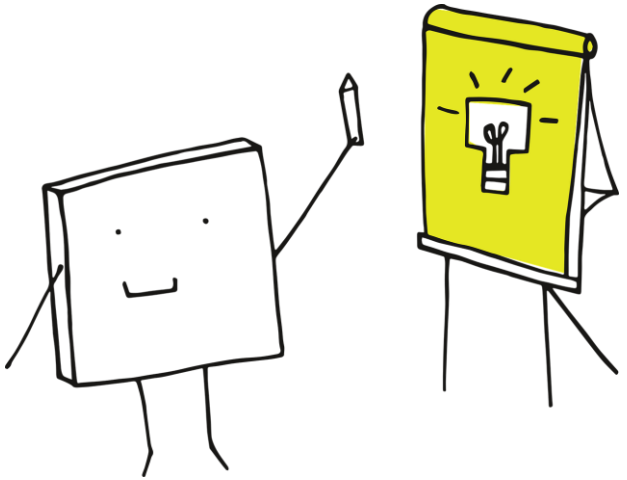
TAVOLO TECNOLOGIE – Focus Sicurezza

- **FORMAZIONE**

  - **Security Awarness Training: Sensibilizzare gli utenti anche con Campagne di phishing simulato**
    Nel 2020 erogati questionari e corsi sui temi: Sicurezza Generale, Sicurezza dei dispositivi mobili, Iniziative relative alla Conformità, Protezione della posta elettronica; le Minacce dal web e le Minacce interne, Password efficaci

  - Corsi in **e-learning** (SELF): corsi SMARTWORKING e ambito privacy GDPR

  - **Corsi tecnici di aggiornamento** per gli specialisti del settore



RegioneEmilia-Romagna

EMILIA-ROMAGNA
SMART WORKING

TAVOLO TECNOLOGIE – Focus Sicurezza

- **Buone Pratiche:**
  - Quando ricevi una e-mail o una pec non attesa:
    - contatta il mittente telefonicamente, anche se è un tuo collega, controlla che sia stato proprio lui ad inviartela prima di aprire eventuali file allegati;
    - sii sospettosa/o se il messaggio cerca di spaventarti, offre un affare incredibile, cerca di estorcere un pagamento in denaro anche virtuale, suggerisce di reimpostare una password o di aggiornare le informazioni dell'account;
    - controlla tutti i link passandovi sopra il mouse per verificarne la vera provenienza. Se l'URL è insolito o è diverso da ciò che ti aspettavi, non cliccare;
    - verifica le richieste e le offerte attraverso un sito web affidabile o un numero di telefono conosciuto.
  - Proteggi la casella e-mail, la pec e in generale tutti gli account che utilizzi:
    - non usare indirizzi di posta elettronica istituzionali/aziendali per scopi personali, che non riguardano l' attività lavorativa;
    - cambia regolarmente la password di ogni account, impostando password complesse (anche per accessi a portali web di altre P.A. o ai social);
    - non usare la stessa password per accedere a servizi diversi.

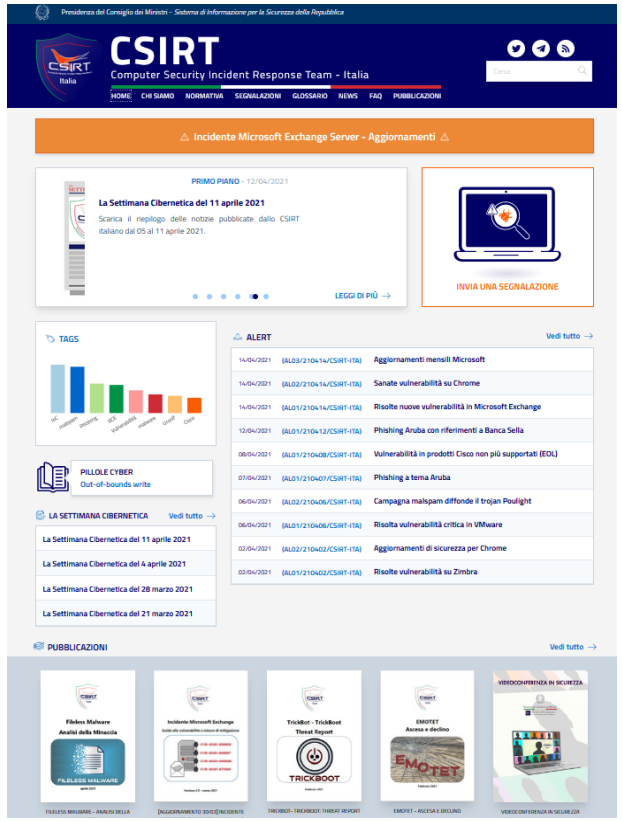
E nel dubbio, se non sei sicura/o, chiedi consiglio al Service Desk

TAVOLO TECNOLOGIE – Focus Sicurezza

- **Buone Pratiche**:
  - **Gestire l'obsolescenza e gli aggiornamenti dei sistemi, delle postazioni sia fisse che mobili (portatili e smartphone) e delle applicazioni**
  - **PASSWORD:** parola chiave conosciuta soltanto dall'utente. Devono essere di una certa lunghezza (almeno 10 caratteri per utenti e di 14 per amministratori), complesse e cambiate regolarmente
  - **Internet:** mantenere comportamenti corretti, "Etica in rete", collegarsi solo a reti (es. WIFI) conosciute e affidabili
  - **Software** autorizzato e **applicazioni** sicure
  - **Protezione dei dati: GDPR e Formazione.**
    Evitare di copiare dati aziendali su PC e chiavette personali (USB). Usare share di rete
  - **Dispositivi mobili:** protezione da furti e danneggiamenti

TAVOLO TECNOLOGIE – Focus Sicurezza

- Security Awarness: bollettini di sicurezza, azioni di mitigazione e riferimenti
- Risk assessment
- Procedura di vulnerability management
- Policy e procedura di gestione degli incidenti
  - In caso di incidenti segnalare all'Incident Handling Leader per valutare la gravità e l'eventuale Data Breach.
    Confronto con il DPO per definire le dovute segnalazioni:
    - Garante della Privacy entro 72 ore
    - Organi di Polizia
    - Comunicazione agli interessati
    - CSIRT ITALIANO: per incidenti rilevanti è obbligatorio per OSE e FSD



TAVOLO TECNOLOGIE – Focus Sicurezza

- Quadro normativo di riferimento
  - Provvedimento del Garante per la protezione dei dati personali del 27 dicembre 2008 in materia di amministratori di sistema e d.lgs. 101/2018 la normativa in materia di protezione dei dati personali: Regolamento Ue 2016/679, GDPR, e Dlgs 196/2003, Codice per la protezione dei dati personali
  - Codice dell'Amministrazione Digitale (CAD) D.Lgs. n. 82/2005 e L. 120/2020 - Semplificazione e innovazione digitale
  - Misure minime di sicurezza ICT per le pubbliche amministrazioni di cui alla Circolare AGID n. 2/2017
  - Norme ISO/IEC 27001 e sue estensioni 27017 e 27018;
  - Decreto legislativo 18 maggio 2018, n. 65 in attuazione della Direttiva (UE) 2016/1148, cd. Direttiva NIS
    decreto-legge n. 105 del 2019, DPCM 131/2020 il primo di 4 che riguardano la sicurezza nazionale.
- Linee guida AGID: per lo sviluppo del software sicuro, sull'accessibilità degli strumenti informatici, per la sicurezza nel procurement ICT

EMILIA-ROMAGNA
SMART WORKING

Regione Emilia-Romagna

VELA
VELOCE
LEGGERO
AGILE
EMILIA-ROMAGNA SMART WORKING

Per info vai su:

lavorasmart.emilia-romagna.it

oppure scrivi a:

smartworking@regione.emilia-romagna.it