



Chi propone lo scambio

Comune ospitante

Unione delle Terre d'Argine

Area, Settore, Ufficio ospitante

Ufficio per la Transizione Digitale

Settore S4 - Servizi Informatici e Innovazione Digitale

Descrizione della *pratica*

Titolo buona pratica

Cybersecurity: Una salvaguardia non solo tecnologica, ma che nella pubblica amministrazione si interseca con un preciso quadro organizzativo e documentale

Descrizione della pratica/soluzione *(scriverla come la si vorrebbe leggere, scegliendo il livello di dettaglio e di sintesi che si ritengono efficaci alla comprensione della "proposta di valore" che viene proposta ai colleghi di altri Comuni)*

L'ultima relazione sulla sicurezza nazionale in materia di cybersecurity, redatta dal DIS (Dipartimento per le Informazioni della Sicurezza), mette in luce un incremento significativo degli attacchi informatici, concentrati in particolare contro la Pubblica Amministrazione (PA). Questo fenomeno è strettamente legato all'accelerato processo di transizione digitale delle PA, agevolato dalle misure del Piano Nazionale di Ripresa e Resilienza (PNRR).

In questo contesto, è cruciale gestire la sicurezza informatica come elemento di processo. Ciò implica assicurare la confidenzialità, integrità e disponibilità dei dati e dei servizi, seguendo principi "by design" e "by default". Tale tutela non si limita unicamente agli aspetti tecnologici, ma coinvolge anche aspetti organizzativi e decisionali.

A parità di sistemi di protezione e dotazioni tecnologiche, è ormai un fatto consolidato che il punto critico nella catena della sicurezza informatica di un'organizzazione risieda nelle persone. Ciò sottolinea la necessità di gestire la sicurezza informatica attraverso precise azioni organizzative e decisionali, partendo dai vertici dell'amministrazione. È di fondamentale importanza agire su tre fronti principali: fornire linee guida per l'uso sicuro degli strumenti ICT (come previsto dall'art. 12 comma 3-bis del Codice dell'Amministrazione Digitale - CAD), implementare una formazione continua del personale per diffondere la consapevolezza sull'importanza della sicurezza informatica e sui suoi impatti sull'organizzazione (conformemente all'art. 13 del CAD), e infine, considerare nell'ambito dei contratti ICT specifiche garanzie da parte dei fornitori per garantire il rispetto dei requisiti minimi di sicurezza.

L'Unione delle Terre d'Argine propone la buona pratica di un approccio integrato alla cybersecurity, mirato a mitigare le vulnerabilità sia legate alle tecnologie sia alle azioni umane. Questo approccio strategico è finalizzato a garantire un ambiente digitale sicuro e resiliente per l'amministrazione, affrontando in modo integrato le sfide legate alla sicurezza informatica.

Le modalità dello scambio

Modalità del trasferimento *(descrive l'attività che viene proposta nel corso dello scambio: una sorta di bozza di programma della/e giornata/e di scambio)*

Programma del Corso

Il trasferimento delle competenze potrà avvenire attraverso incontri sincroni nei quali affrontare le seguenti tematiche:

1. Misure di Sicurezza ICT per le PA:

- Approfondimento del documento sulle Misure di Sicurezza ICT dell'Unione delle Terre d'Argine.
- Analisi delle azioni pratiche implementate per garantire la sicurezza delle informazioni.

2. Criteri di sicurezza CIS-CVS ver. 8:

- Studio dettagliato del documento relativo ai criteri di sicurezza CIS-CVS ver. 8.
- Implementazione pratica di tali criteri per migliorare la sicurezza informatica.

3. Backup e Business Continuity:

- Approfondimento del piano di Backup e di Business Continuity dell'Unione delle Terre d'Argine.
- Simulazioni pratiche per garantire un rapido recupero in caso di incidenti o interruzioni.

4. Disaster e Incident Recovery:

- Analisi dettagliata del piano di Disaster e Incident Recovery dell'Unione delle Terre d'Argine.
- Esercitazioni pratiche per gestire situazioni di emergenza e ripristinare rapidamente le operazioni.

5. Linee guida per l'utilizzo degli strumenti informatici:

- Approfondimento delle linee guida per un utilizzo sicuro degli strumenti informatici dell'Unione delle Terre d'Argine.
- Sessioni pratiche per applicare correttamente tali linee guida.

6. Linee guida contratti ICT:

- Studio delle linee guida da considerare nell'ambito dei contratti ICT.
- Analisi dei requisiti di sicurezza contrattuali e delle garanzie fornite dai fornitori.

7. Abilitazione allo IaaS Qualificato:

- Analisi del piano di abilitazione allo IaaS Qualificato nell'ambito del finanziamento PNRR M1C1 Misura 1.2.
- Implementazione pratica delle tecniche di migrazione necessarie per l'IaaS Qualificato.

8. Progetto di innalzamento delle Misure di Sicurezza ICT:

- Esame del progetto di innalzamento delle Misure di Sicurezza ICT dell'Unione delle Terre d'Argine nell'ambito del finanziamento alle Unioni Avanzate.
- Implementazione delle nuove misure di sicurezza e valutazione dell'impatto sull'ambiente digitale dell'amministrazione.

Quanti partecipanti possono essere ospitati per ogni sessione *(se si ritiene utile, è possibile anche indicare che tipo di figure professionali possono maggiormente giovare di questo scambio)*

Massimo 5 persone, tra personale tecnico (preferibile) e/o amministrativo

Quanto tempo dura ogni sessione di attività di scambio *(indicare numero di giornate)*

Un approfondimento avrà durata di almeno 4 ore. Pertanto, l'attività di scambio per coprire l'intera pianificazione dei corsi potrà essere organizzata in un arco temporale di almeno 4 giornate.

Date disponibili

In quale periodo è possibile attivare lo scambio? *(indicare le date in cui si è disponibili per lo scambio. Scegliere se offrire un'alternativa indicando "O" precisando, di seguito, le date alternative; oppure scegliere se offrire più sessioni di scambio indicando "E" precisando, di seguito, le date disponibili per attivare gli scambi).*

Febbraio 2026 (17, 19, 24, 26)

Marzo 2026 (1, 3, 15, 17, 22, 24, 28)