Curriculum - Italiano

Unità di apprendimento per conoscenze, abilità e competenze per la sicurezza delle informazioni e la protezione dei dati nelle PMI

Funded by the
Erasmus+ Programme
of the European Union

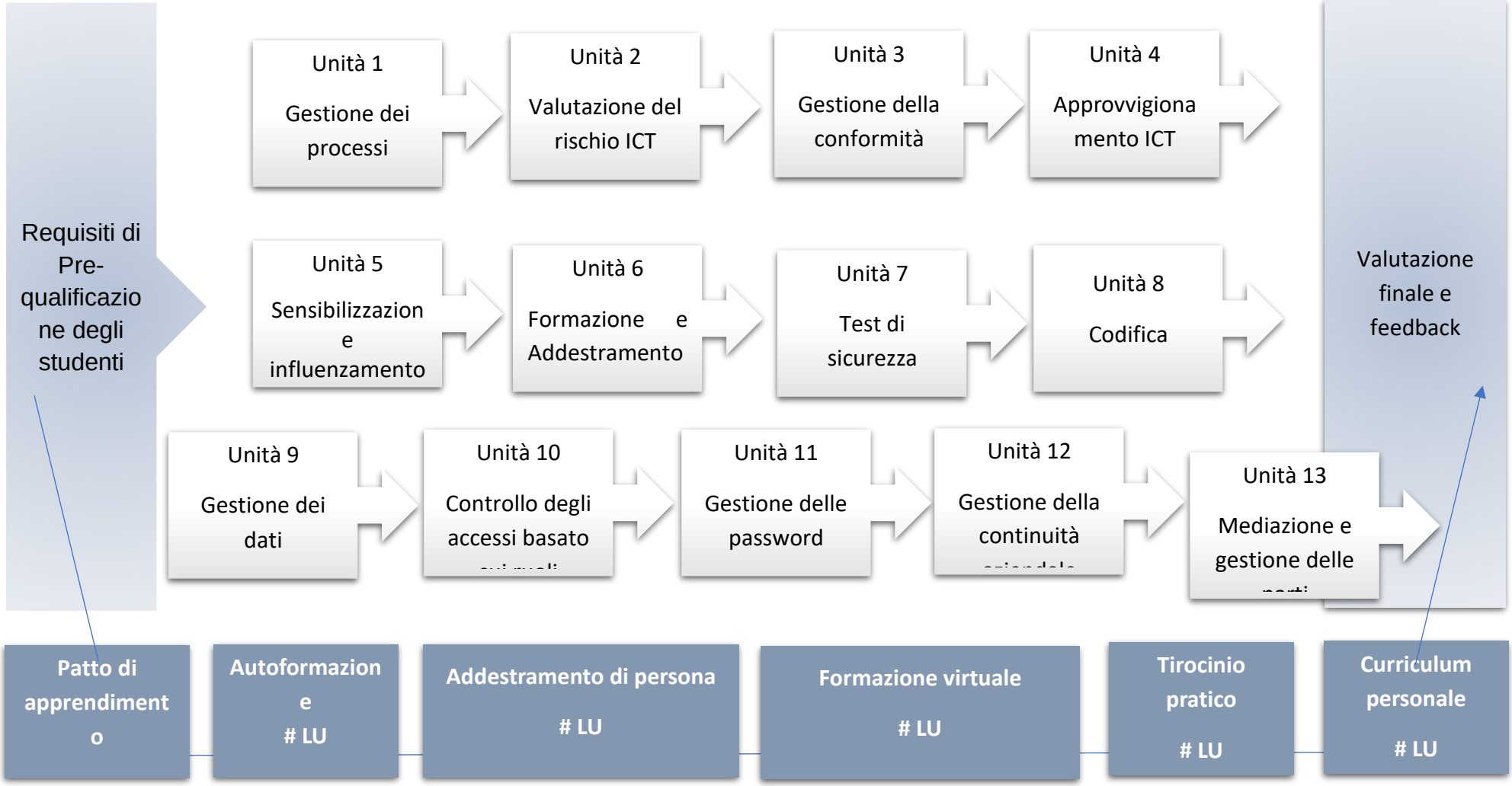
Funded by the
Erasmus+ Programme
of the European Union

Questo documento è stato prodotto nell'ambito del progetto ERASMUS+ "Teilzertifizierung im Berufsfeld Informationssicherheit - TeBeiSi", Project ID: 2018-1-EN02-KA202-005218.

Contenuti

Funded by the Erasmus+ Programme of the European Union

Curriculum TeBeISi (basato sui criteri ECVET)



Unità 1 - 6: Azioni a carattere

Unità 7 - 13: Azioni in itinere

1.1 Learning Units – sintesi e breve descrizione

#	5.2 Unità di apprendimento	panoramica e breve descrizione
LU1	**Gestione dei processi**	Analizzare i processi aziendali e produrre un rapporto strategico sulla protezione dei dati e la sicurezza delle informazioni.
LU2	**Valutazione del rischio ICT**	Seguire i cambiamenti all'interno e all'esterno dell'azienda che hanno un impatto sulla strategia di sicurezza dell'azienda e produrre segnalazioni per i dipendenti.
LU3	**Gestione della conformità**	Scrivere linee guida aziendali su come trattare informazioni e dati specifici
LU4	**Approvvigionamento ICT**	Produrre raccomandazioni riguardo agli articoli da acquistare considerando i requisiti di sicurezza delle informazioni e di protezione dei dati dell'azienda
LU5	**Sensibilizzazione ed influenzamento**	Condurre attività (informative) per sensibilizzare i dipendenti sui rischi di sicurezza nella loro routine lavorativa e per diffondere la consapevolezza tra I lavoratori.
LU6	**Formazione ed addestramento**	Creare piani di formazione per l'azienda al fine di poter formare regolarmente i dipendenti in materia di sicurezza delle informazioni e protezione dei dati.
LU7	**Test di sicurezza**	Installare un firewall e un software antivirus. Eseguire aggiornamenti e applicare metodi di base per testare la sicurezza del software utilizzato nell'azienda e produrre una normativa di sicurezza.
LU8	**Codifica**	Lavorare sulla messa in sicurezza dei dispositivi mobili, dei canali di comunicazione e delle unità di memorizzazione dei dati tramite password o altri mezzi di autenticazione.
LU9	**Gestione dei dati**	Eseguire back-up di routine dei dati e applicare i metodi di condotta corretta secondo il GDPR per il trattamento dei dati in azienda.
LU10	**Controllo degli accessi basato sui ruoli**	Stabilire account di amministratore e limitare i diritti di accesso tra gli impiegati secondo i livelli di sicurezza definiti.
LU11	**Gestione delle password**	Stabilire delle password per l'accesso individuale tra i dipendenti e permettere un processo di archiviazione e recupero sicuro.
LU12	**Gestione della continuità aziendale**	Stabilire linee guida e procedure per affrontare eventuali imprevisti.
LU13	**Mediazione e gestione delle parti interessate**	Coordinare le esigenze dei dirigenti e dei dipendenti dell'azienda, fornendo a entrambe le parti informazioni e approfondimenti dall'interno dell'azienda.

2 Descrizione dettagliata delle unità di apprendimento (basata su ECVET)

2.1 LU1 – Gestione dei processi

Unità di apprendimento 1	Gestione dei processi
Descrizione generale / Output	Analizzare i processi aziendali e produrre un rapporto strategico sulla protezione dei dati e la sicurezza delle informazioni.
Numero di codice	LU 1
Tipo	Obbligatorio - da definire
Volume	Ore - da definire
Competenze da acquisire	I partecipanti imparano a capire l'importanza di un'analisi strutturata dei processi in un'azienda. Sono capaci di riconoscere i processi che evocano la necessità di ulteriori analisi considerando la loro esposizione alla sicurezza dei dati e delle informazioni. I partecipanti hanno familiarità con la documentazione dei processi e sono capaci di monitorare i cambiamenti nella routine di lavoro. Sono capaci di preparare la documentazione che permette la formulazione di proposte di intervento. Tradotto con www.DeepL.com/Translator (versione gratuita)
Risultati di apprendimento	- **I partecipanti** - - **Imparano** - - come applicare le linee guida del GDPR e le buone pratiche di sicurezza delle informazioni. - - come identificare, documentare, progettare, implementare, governare e ottimizzare i processi aziendali. - - come pianificare strategicamente la documentazione dei processi. - - su tecniche e canali di comunicazione. - - **Possono** - - implementare la documentazione utilizzando sistemi EDP. - - riassumere le informazioni originali senza perdere il messaggio originale. - - comunicare efficacemente con i colleghi per adattare i flussi di lavoro. - - reagire in modo appropriato alle affermazioni degli altri, ad esempio, accettare critiche costruttive e ascoltare attivamente per trovare le migliori soluzioni. - - trovare informazioni legali e tecniche rilevanti e le corrispondenti raccomandazioni per l'azione da fonti affidabili. - - - **Competenza personale** - - **I partecipanti sono in grado di** -

	- - organizzare autonomamente il processo di documentazione, lavorando in modo strutturato con attenzione ai dettagli. - - comunicare autonomamente con i colleghi ed essere sicuri nelle interazioni. - - Riconoscere la responsabilità che appartiene al compito ed essere fiduciosi nell'interazione con gli altri. - - - Tradotto con www.DeepL.com/Translator (versione gratuita)
Raccomandazioni per l'apprendimento e l'insegnamento	Documentazione dei processi con l'aiuto di esempi reali. Esercizi sulla documentazione nel sistema EDP in forma libera e con l'aiuto di moduli di testo.
Letteratura e ulteriori fonti	Nguyen, B. T., Lee, G. M., Sun, K., & Guo, Y. (2019). GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. *IEEE Transactions on Information Forensics and Security,* 15, 1-13. EU-GDPR. (2019). *EU GDPR portal*. [Online]. Available: https://eugdpr.org. General data protection regulation (2018). Official Journal of the European Union [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/uri=CELEX:32016R0679. Gellert, R. (2015). Understanding data protection as risk regulation. *Journal of Internet Law*, 18 (11), 3-15.

2.2 LU2 – Gestione del Rischio ICT

Unità di apprendimento 2	Gestione del rischio ICT
Descrizione generale / Output	Seguire i cambiamenti all'interno e all'esterno dell'azienda che hanno un impatto sulla strategia di sicurezza dell'azienda e produrre rapporti per i dipendenti.
Numero di codice	LU 2
Tipo	Obbligatorio – da definire
Volume	Ore - da definire
Competenze da acquisire	I partecipanti imparano a capire le dinamiche del cambiamento tecnologico e la loro influenza sulla strategia aziendale per mitigare i rischi. Sono in grado di decidere l'urgenza di intervenire su questi rischi. I partecipanti saranno in grado di seguire gli sviluppi tecnologici all'interno e all'esterno dell'azienda e di fornire valutazioni sull'esposizione al rischio dell'azienda.
Risultati di apprendimento	**Competenze Tecniche** I partecipanti **Imparano** - sulla valutazione dell'esposizione al rischio dell'azienda e sull'adeguatezza delle misure attuali per far fronte ai rischi correlati. - come monitorare gli sviluppi tecnologici all'interno e all'esterno dell'azienda e i cambiamenti del personale. - come determinare il volume e lo scopo dei dati personali trattati. **Possono** - trovare informazioni sugli sviluppi tecnologici consultando fonti di notizie rilevanti e informazioni da autorità pubbliche o private del settore. - rilevare i rischi nonostante la ritrosia teorica dei dipendenti a ri-velare errori o debolezze. - fornire raccomandazioni per azioni basate sulle informazioni ottenute. - valutare e mitigare i rischi relativi alla protezione dei dati. - identificare le operazioni di archiviazione/processo dei dati personali all'interno delle organizzazioni e valutare il loro contesto. - intraprendere azioni sugli obiettivi fissati a livello di strategia al fine di mobilitare le risorse e i dipendenti per rafforzare la collaborazione. **Competenze Personali** **I partecipanti sono in grado di** - - mostrare resilienza di fronte alla non volontà dei colleghi di coo-perare. - - rimanere flessibili per trovare soluzioni e creare un ambiente di supporto. - - eseguire i compiti in modo strategico e organizzato.

	-
Raccomandazioni per l'apprendimento e l'insegnamento	Documentazione dei processi con l'aiuto di esempi reali. Esercizi sulla documentazione nel sistema EDP in forma libera e con l'aiuto di moduli di testo.
Letteratura & Altre Fonti	European Banking Authority (2019). Final Report: EBA Guidelines on ICT and security risk management [Online]. Available: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020. NZ Digital Government (2021). ICT Risk Management Guidance [Online]. Available: www.digital.govt.nz/dmsdocument/130-ict-risk-management-guidance/html. Commission de Surveillance du Secteur Financier (CSSF) (2020). ICT Risk [Online]. Available: www.cssf.lu/en/ict-risk/. Rothman, T. (2020). Valuations of Early-Stage Companies and Disruptive Technologies: How to Value Life Science, Cybersecurity and ICT Start-ups, and their Technologies. Berlin: Springer.

2.3 LU3 – Gestione della conformità

Unità di apprendimento 3	Gestione della conformità
Descrizione Generale / Output	Scrivere linee guida aziendali su come trattare informazioni e dati specifici.
Numero di codice	LU 3
Tipo	Obbligatorio – da definire
Volume	ore – da definire
Competenze da acquisire	The participants learn to understand the importance of codifying company behavioural guidelines in order to establish proper conduct with data and information. They learn how to set guidelines which establish compliance among employees. They understand the importance of preparing for foreseen and unforeseen contingencies and setting out companywide rules how to behave and measured to be taken in critical situations.
Risultati di apprendimento	**Competenze Tecniche** I partecipanti **Imparano** - sui regolamenti GDPR e sui documenti legali nazionali che regolano la sicurezza delle informazioni e la protezione dei dati. - sull'architettura dell'informazione e sui canali di comunicazione interna dell'organizzazione - come analizzare, mappare e documentare i processi che potrebbero causare un potenziale conflitto con le politiche di conformità. - come preparare le linee guida della politica di conformità. - come raccogliere, gestire e valutare le tecniche di elaborazione dei dati. - come pensare analiticamente nel processo di sintesi delle informazioni, sviluppare soluzioni e prendere decisioni relative alla gestione della conformità. **Possono** - implementare le procedure descritte nei documenti legali. - identificare i dati critici e le unità di informazione che richiedono una protezione o un trattamento speciale - Analizzare e mappare i processi relativi al flusso di informazioni nell'organizzazione. - Riconoscere i rischi potenziali e le minacce alla sicurezza delle informazioni e alla protezione dei dati nei processi interni dell'organizzazione. - sviluppare soluzioni relative alla gestione della conformità a problemi pratici, operativi o concettuali in un'ampia gamma di routine lavorative quotidiane. - comprendere lo scopo delle linee guida della politica di conformità e aggiornarle in situazioni di emergenza. - applicare le abilità analitiche e di pensiero critico nell'identificare i punti di forza e di debolezza delle potenziali soluzioni ai problemi relativi alla gestione della conformità.

	- riassumere le informazioni in modo conveniente e significativo **Competenze Personali** **I partecipanti sono in grado di** - lavorare in modo strutturato con attenzione ai dettagli - Riconoscere le responsabilità legate ai compiti ed essere sicuri nell'interazione con gli altri. - gestire i compiti in modo indipendente e dimostrare la volontà di imparare. -
Raccomandazioni per l'apprendimento e l'insegnamento	Documentazione dei processi con l'aiuto di esempi reali. Esercizi sulla documentazione nel sistema EDP in forma libera e con l'aiuto di moduli di testo.
Letteratura & Altre Fonti	Agostinelli S., Maggi F.M., Marrella A., & Sapio F. (2019) Achieving GDPR Compliance of BPMN Process Models. In: Cappiello C., Ruiz M. (eds) Information Systems Engineering in Responsible Information Systems. CAiSE 2019. Lecture Notes in Business Information Processing, 350, 10–22. Springer, Cham. https://doi.org/10.1007/978-3-030-21297-1_2 Basin, D., Debois, S., & Hildebrandt, T. (2018). On purpose and by necessity: compliance under the GDPR. In Proceedings Financial Cryptography and Data Security, 18 [Online]. Available: https://pure.itu.dk/ws/files/84212312/On_Purpose_and_ny_Necessity.pdf Besik, S. I., & Freytag, J. C. (2020). Managing Consent in Workflows under GDPR. In J. Manner, S. Haarmann, S. Kolb, O. Kopp (Eds.): 12th ZEUS Workshop, ZEUS 2020, Potsdam,Germany, 20-21 February 2020, (pp. 18-25). Blanco-Lainé, G., Sottet, J. S., & Dupuy-Chessa, S. (2019, November). Using an enterprise architecture model for GDPR compliance principles. In IFIP Working Conference on The Practice of Enterprise Modeling (pp. 199-214). Springer, Cham. EU-GDPR. (2019). EU GDPR portal. [Online]. Available: https://eugdpr.org. Kammüller, F., Ogunyanwo, O.O., & Probst, C.W. (2019). Designing data protection for GDPR compliance into IoT healthcare systems. Computer Science. arXiv:1901.02426. Torre, D., Soltana, G., Sabetzadeh, M., Briand, L. C., Auffinger, Y., & Goes, P. (2019). Using Models to Enable Compliance Checking Against the GDPR: An Experience Report. In 2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS), Munich, Germany, 2019, (pp. 1-11). doi: 10.1109/MODELS.2019.00-20. Wichmann, J., Sandkuhl, K., Shilov, N., Smirnov, A., Timm, F., & Wißotzki, M. (2020). Enterprise Architecture Frameworks as Support for Implementation of Regulations: Approach and Experiences from

	GDPR. Complex Systems Informatics and Modeling Quarterly, (24), 31-48.

2.4 LU4 – Approvvigionamento ICT

Unità di apprendimento 4	Approvvigionamento ICT
Description Generale / Output	Produrre raccomandazioni riguardo agli articoli da acquistare considerando i requisiti di sicurezza delle informazioni e di protezione dei dati dell'azienda.
Number di codice	LU 4
Tipo	Obbligatorio – da definire
Volume	Ore – da definire
Competenze da acquisire	I partecipanti imparano a capire l'importanza del sistema di approvvigionamento per sostenere l'implementazione della sicurezza delle informazioni e della protezione dei dati. Imparano come mettere le proprie competenze a disposizione del processo di approvvigionamento dell'azienda. I partecipanti sono in grado di esercitare un'influenza sull'acquisto di nuove tecnologie e macchinari e di valutare l'adeguatezza e l'utilizzo in termini di protezione dei dati e linee guida di sicurezza delle informazioni dell'azienda.
Risultati di apprendimento	**Competenze Tecniche** **I partecipanti** **Imparano** - sui requisiti di sicurezza e sulle specifiche dell'azienda per quanto riguarda le nuove attrezzature. - sulle specifiche dell'hardware esistente e l'urgenza di al-terle con la nuova tecnologia. - sull'inganno dei fornitori di servizi e delle attrezzature per le vio-lazioni del GDPR. **Possono** - . comunicare efficacemente con gli altri. - preparare e presentare una breve presentazione (relazione/procedura/processo/strategia) dedicata alla valutazione della tecnologia o dei macchinari che devono essere acquistati. - trasferire informazioni da diversi impiegati/reparti sulle loro necessità e poi dare la raccomandazione sull'acquisto. - raccogliere informazioni complete sulla tecnologia/macchinari acquistati. - trovare informazioni legali e tecniche rilevanti e prendere decisioni basate su questa indagine. - intraprendere azioni sugli obiettivi e le procedure definite a livello strategico per mobilitare le risorse e perseguire le strategie stabilite.

	- pianificare e gestire le risorse sotto vincoli di budget e di tempo e raggiungere gli obiettivi stabiliti facendo uso del monitoraggio dell'avanzamento del progetto e dei controlli di qualità **Competenze Personali** **I partecipanto sono in grado di** - conoscere le soluzioni di mercato esistenti per il problema dell'azienda. - dedicarsi ai dettagli (legali e tecnici). - mostrare fiducia e responsabilità nella comunicazione con le parti interessate.
Raccomandazioni per formazione ed addestramento	. Documentazione dei processi con l'aiuto di esempi reali. Esercizi sulla documentazione nel sistema EDP in forma libera e con l'aiuto di moduli di testo.
Letteratura & altre fonti	Australian Government: Digital Transformation Agency (2021). ICT procurement [Online]. Available: www.dta.gov.au/help-and-advice/ict-procurement. Moses, M. (2019). Procurement Process and ICT. Zerite Network [Online]. Available: http://zeritenetwork.com/procurement-process-and-ict/. European Commission (2016). Best practices for ICT procurement based on standards in order to promote efficiency and reduce lock-in: 2-year project completed [Online]. Available: ec.europa.eu/digital-single-market/en/news/. Dovgalenko, S. (2020). The Technology Procurement Handbook: A Practical Guide to Digital Buying. London: Kogan Page.

2.5 LU5 – Sensibilizzazione ed influenzamento

Unità di apprendimento 5	Sensibilizzazione ed influenzamento
Description Generale / Output	Condurre attività (informative) per sensibilizzare i dipendenti sui rischi di sicurezza nella loro routine lavorativa e per diffondere la consapevolezza tra la forza lavoro.
Numero di codice	LU 5
Tipo	Obbligatorio – da definire
Volume	Ore – da definire
Competenze da acquisire	Il partecipante impara a capire l'importanza di sensibilizzare i dipendenti e i membri del consiglio di amministrazione riguardo alla protezione dei dati e alla sicurezza delle informazioni. Impareranno ad aumentare la consapevolezza per le minacce comuni e a sviluppare le capacità nel personale per rilevare le probabili minacce nella loro routine lavorativa quotidiana. I partecipanti saranno in grado di condurre un'analisi sul livello di consapevolezza nell'azienda e di implementare la corrispondente sensibilizzazione
Risultati di apprendimento	**Competenze Tecniche** I partecipanti **Imparano** - sulle linee guida di base del GDPR. - Come gestire i processi e il personale potenzialmente vulnerabili agli attacchi o alla perdita di informazioni e dati sensibili. - come si possono implementare misure di auditing. - sulle tecniche e i canali di comunicazione. - come implementare strategie di cambiamento. **Possono** trovare la fonte pertinente di conoscenza giuridica. - cooperare con gli altri nel senso più ampio del termine per identificare il bisogno di cambiamento, ispirare e istruire e assistere nella sua attuazione. - comunicare efficacemente con gli altri scegliendo non solo il tipo di messaggio ma anche la sua portata e l'importanza per le circostanze. **Competenze Personali** **I partecipanti sono in grado di** - adattarsi a condizioni e circostanze mutevoli lavorando in modo organizzato e mantenendo una distanza che permetta un'adeguata autovalutazione. - essere un esempio per gli altri dipendenti seguendo il loro codice etico di condotta e mostrare responsabilità.

Raccomandazioni per formazione ed addestramento	Combina la conoscenza teorica e l'approccio con esempi pratici come misure di buon controllo e come gestire le situazioni, per esempio: - USB false- -Caso di manipolazione umana - Invio di false e-mail Applicare metodi di insegnamento interattivi (es. lavori di gruppo, discussioni, analisi di casi, simulazioni di ruolo, ecc.)
Letteratura & altre fonti	IT Governance Privacy Team (2020). EU General Data Protection Regulation (GDPR) – An implementation and compliance guide (4th ed.). Clarke, N., Furnell, S. (2020). Human Aspects of Information Security & Assurance (14th ed.). Plymouth: Centre for Security, Communication & Network Research. i-scoop (o.J.). GDPR awareness: a matter of people, culture, leadership and acting now [Online]. Available: https://www.i-scoop.eu/gdpr/gdpr-awareness/. Kefron - The Information Management People (o.J.). Why Maximizing Staff Awareness Is The Key To A Smooth GDPR Transition [Online]. Available: https://www.kefron.com/blog/why-maximizing-staff-awareness-is-the-key-to-a-smooth-gdpr-transition/. European Union Agency for Cybersecurity (2017). Handbook on Security of Personal Data Processing [Online]. Available: www.enisa.europa.eu General Data Protection Regulation (2021). Complete guide to GDPR compliance [Online]. Available: https://gdpr.eu/

2.6 LU6 – Formazione ed addestramento

Approvvigionamento ICT 6	Formazione ed addestramento
Descrizione Generale / Output	Creare piani di formazione per l'azienda al fine di poter formare regolarmente i dipendenti in materia di sicurezza delle informazioni e protezione dei dati.
Numero di codice	LU 6
Tipo	Obbligatorio – da definire
Volume	Ore – da definire
Competenze da acquisire	I partecipanti imparano a capire l'importanza della formazione per quanto riguarda la protezione dei dati e i requisiti di sicurezza delle informazioni. Imparano a educare sia se stessi che i dipendenti dell'azienda. I partecipanti saranno in grado di consultare fonti affidabili e di individuare i bisogni formativi in base alla consultazione o all'interazione con i dipendenti. I partecipanti imparano a preparare il materiale di formazione e a formare i dipendenti per inserire procedure di lavoro appropriate nel loro modo di lavorare quotidiano.
Risultati di apprendimento	**Competenze Tecniche** I partecipanti **Imparano** - dove trovare i materiali legali nazionali che regolano la sicurezza delle informazioni e la protezione dei dati (basi del GDPR). - come preparare il materiale di formazione e come fornire la formazione a procedure di lavoro adeguate all'interno dell'azienda. - come fare da mentore ai singoli dipendenti. **Possono** - Presentare ai dipendenti come applicare praticamente i dispositivi legali nazionali nel campo della sicurezza delle informazioni e della protezione dei dati seguendo le linee guida del GDPR. - convincere i dipendenti dell'importanza della formazione continua in entrambi i settori attraverso una sensibilizzazione attiva. - fare da mentore e sostenere i singoli dipendenti per quanto riguarda le esigenze di formazione identificate. - sviluppare soluzioni a problemi pratici, operativi o concettuali che si presentano nell'esecuzione del lavoro nei contesti più disparati. **Competenze Personali** **I partecipanti sono in grado di** - - organizzare autonomamente sessioni di formazione all'interno dell'azienda in modo strutturato con attenzione alle esigenze attuali. - - Comunicare autonomamente con i colleghi e con la direzione avendo fiducia nelle interazioni. - - riconoscere la responsabilità che appartiene al compito e motivare i dipendenti ad apprendere.

Raccomandazioni per formazione ed addestramento	Documentare le difficoltà di sicurezza dell'informazione e di protezione dei dati incontrate nell'attività quotidiana per pianificare e attuare misure di formazione adeguate.
Letteratura ed altre fonti	Pipkin, D. (2000). Information security: Protecting the global enterprise. New York: Hewlett-Packard Company. Da Veiga, A., Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. Computers & Security, (49), 162–176. doi: 10.1016/j.cose.2014.12.006. Peacock, M., Steward, E. B., & Belcourt, M. (2019). Understanding Human Resources Management. Nelson: Nelson College Indigenous. Ryan, L. (2010). Corporate Education: A Practical Guide to Effective Corporate Learning. Salisbury: Griffin Press. Osborne, B. (2020). 10 Benefits of Security Awareness Training [Online]. Available: https://resources.infosecinstitute.com/topic/10-benefits-of-security-awareness-training/. GDPR informer (2017). Data Protection Training: 10 Tips for Your Staff [Online]. Available: https://gdprinformer.com/gdpr-articles/data-protection-training-10-tips-staff.

2.7 LU7 – Test di sicurezza

Unità formativa 7	Test di sicurezza
Description Generale / Output	Installare un firewall e un software antivirus. Eseguire aggiornamenti e applicare metodi di base per testare la sicurezza del software utilizzato nell'azienda e produrre una documentazione appropriata.
Numero di codice	LU 7
tipo	Obbligatoria – Da definire
Volume	Ore – da definire
Competenze da acquisire	I partecipanti imparano a capire l'importanza di testare le infrastrutture ICT esistenti per la loro vulnerabilità di fronte agli sviluppi tecnologici. Imparano a usare (o a capire con un supporto esterno) strumenti di penetration testing per garantire la sicurezza dei firewall e dei canali di comunicazione. C'è un numero infinito di modi per violare un'applicazione. E i test di sicurezza, da soli, non sono l'unica (o la migliore) misura di quanto sia sicura un'applicazione. Ma è altamente raccomandato che i test di sicurezza siano inclusi come parte del software standard
Risultati di apprendimento	**Competenze Tecniche** I partecipanti Imparano - sulla sicurezza della rete: Si tratta di cercare vulnerabilità nell'infrastruttura di rete (risorse e politiche). - sulla sicurezza del software di sistema: Si tratta di valutare le debolezze nei vari software (sistema operativo, sistema di database e altri software) da cui dipende l'applicazione. - sulla sicurezza delle applicazioni lato client: Si tratta di assicurare che il client (browser o qualsiasi altro strumento simile) non possa essere manipolato. - sulla sicurezza delle applicazioni lato server: Si tratta di assicurarsi che il codice del server e le sue tecnologie siano abbastanza robuste da respingere qualsiasi intrusione. **Possono** **- costruire test per determinare la sicurezza del prodotto software.** **- adattare il quadro esistente.** **- accedere al sistema informatico o alla rete con autorizzazione.** **- garantire i sistemi per evitare di rubare o distruggere i dati.** **- eseguire la maggior parte delle attività di violazione con l'autorizzazione del proprietario.** **Competenze Personali** **I partecipanti sono in grado di** - riconoscere la documentazione dei processi come punto di partenza per ulteriori fasi di lavoro.

	- Lavorare in modo strutturato con attenzione ai dettagli. - Riconoscere la responsabilità che appartiene al compito ed essere sicuri nell'interazione con gli altri. -
Raccomandazione per formazione ed addestramento	La maggior parte dei tipi di test di sicurezza comportano passi complessi e un comportamento fuori dagli schemi, ma a volte, si tratta di test semplici che aiutano a smascherare i rischi di sicurezza più gravi.
Letteratura ed altre fonti	Dekkers, C., McCurley, J., & Zubrow, D. (2013). Measures and Measurement for Secure Software Development. Pittsburgh: Carnegie Mellon University. Dowd, M., McDonald, J., & Schuh, J. (2007). The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. Boston: Addison-Wesley.

2.8 LU8 - Codifica

Unità Didattica 8	Codifica
Descrizione Generale / Output	Lavorare sulla messa in sicurezza dei dispositivi mobili, dei canali di comunicazione e delle unità di memorizzazione dei dati tramite password o altri mezzi di autenticazione.
Numero di codice	LU 8
Tipo	Obbligatorio – da definire
Volume	Ore – da definire
Competenze da acquisire	I partecipanti imparano a capire l'importanza della codifica delle password per la loro vulnerabilità di fronte agli sviluppi tecnologici. Imparano a usare (o a capire con un supporto esterno) gli strumenti di codifica delle password per garantire la sicurezza dei firewall e dei canali di comunicazione. La codifica delle password è il processo in cui una password viene convertita da un formato di testo letterale in una sequenza di caratteri umanamente illeggibile. Se fatto correttamente, è molto difficile tornare alla password originale e quindi aiuta a proteggere le credenziali dell'utente e a prevenire l'accesso non autorizzato a un sito web.
Risultati di apprendimento	Competenze Tecniche I partecipanti Imparano - sui valori letterali: Le password erano memorizzate in formato testo letterale nei database senza alcuna codifica o hashing. Poiché i database hanno bisogno di autenticazione, che nessuno tranne gli amministratori e l'applicazione aveva, questo era considerato sicuro. - sulla crittografia: È un'alternativa più sicura e il primo passo verso la sicurezza delle password. - Hashing: Per combattere questi attacchi, gli sviluppatori hanno dovuto trovare un modo per proteggere le password in un database in modo tale che non possano essere decifrate. - sul Salting: Per combattere la comparsa di tabelle arcobaleno, gli sviluppatori hanno iniziato ad aggiungere una sequenza casuale di caratteri all'inizio delle password hash. - circa i codificatori di password: Fornisce molteplici implementazioni di codifica delle password tra cui scegliere. Ognuna ha i suoi vantaggi e svantaggi, e uno sviluppatore può scegliere quale usare a seconda del requisito di autenticazione della sua applicazione. **Possono** - istruire il team sulle migliori pratiche di codifica delle password. - educare il team sulla sicurezza informatica. - decidere quali tipi di password non usare. - definire il modo giusto per generare processi di codifica.

	- eliminare le password complesse. - ridurre fortemente il rischio di copiare una password. - garantire la verifica e la responsabilità delle password. **Competenze Personali** **I partecipanti sono in grado di** - riconoscere la documentazione dei processi come punto di partenza per ulteriori fasi di lavoro. - Lavorare in modo strutturato con attenzione ai dettagli. - Riconoscere la responsabilità che appartiene al compito ed essere si-curo nell'interazione con gli altri. - gestire i principali compiti richiesti con un buon livello di autono-mia. - enfatizzare le loro competenze sociali (soft skills, empatia e comunica-zione in particolare).
Raccomandazioni per apprendimento e insegnamento	La maggior parte dei tipi di processi di codifica comportano passi complessi e un pensiero fuori dagli schemi, ma, a volte, sono semplici test che aiutano ad esporre i rischi di codifica più gravi.
Letteratura & altre fonti	Kaliski, B. (2000). Password-Based Cryptography Specification Version 2.0. RFC Editor, US. https://doi.org/10.17487/RFC2898. Mourouzis, T., Pavlou, K. E., & Kampakis, S. (2018). The Evolution of User-Selected Passwords: A Quantitative Analysis of Publicly Available Datasets. Computer Science. arXiv:1804.03946. Barbero, G., Trasselli, F. (2015). Manus OnLine and the Text Encoding Initiative Schema. Journal of the Text Encoding Initiative, (8), 1-16. doi: 10.4000/jtei.1054.

2.9 LU9 – Gestione dei dati

Unità di apprendimento 9	Gestione dei dati
Descrizione Generale / Output	Eseguire back-up di routine dei dati e applicare i metodi di condotta corretta secondo il GDPR al trattamento dei dati in azienda.
Numero di codice	LU 9
Tipo	Obbligatorio – da definire
Volume	ore – da definire
Competenze da acquisire	I partecipanti imparano a capire l'importanza di conservare ed elaborare dati e informazioni secondo le linee guida concordate. Imparano la corretta condotta con i dati in considerazione del GDPR. I partecipanti saranno in grado di valutare l'archiviazione e l'elaborazione dei dati fisici ed elettronici nell'azienda e di identificare potenziali comportamenti scorretti. I partecipanti imparano a suggerire modifiche nei processi aziendali al fine di mitigare questi rischi.
Risultati di apprendimento	**Competenze Tecniche** I partecipanti **Imparano** - come definire le esigenze di informazione necessarie per il successo del processo: che tipo di dati vengono trattati all'interno dell'organizzazione e quali tecniche di archiviazione dovrebbero essere conformi alle norme vigenti. - regole, come determinare il volume e lo scopo delle operazioni di archiviazione e trattamento dei dati personali. - come organizzare e applicare la gestione dei dati nell'azienda: adattarsi al cambiamento; applicare il pensiero analitico; sviluppare soluzioni; eseguire compiti di gestione del progetto in modo indipendente. - diverse tecniche e stili di comunicazione per ottenere le informazioni necessarie per la conservazione. **Possono** - determinare il volume e lo scopo dei dati personali che vengono conservati/elaborati all'interno dell'organizzazione. - Creare backup regolari per ridurre al minimo il rischio di perdere dati e informazioni preziose. - Lavorare all'interno del gruppo per estrarre in modo efficiente le informazioni per migliorare i processi. - Pianificare e gestire varie risorse e monitorare il processo di gestione dei dati per raggiungere un obiettivo specifico. **Competenze Personali** **I partecipanti sono in grado di** - lavorare in modo strutturato con attenzione ai dettagli

	- Riconoscere la responsabilità che appartiene al compito ed essere sicuro nell'interazione con gli altri. - gestire i compiti in modo indipendente e dimostrare la volontà di imparare
Raccomandazioni per apprendimento ed insegnamento	Combinare la conoscenza teorica e l'approccio con esempi pratici. Applicare metodi di insegnamento interattivi (es. lavori di gruppo, discussioni, analisi di casi, simulazioni di ruolo, ecc.)
Letteratura & altre fonti	Calabro, A., Daoudagh, S., & Marchetti, E. (2020). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. Information Systems (91) [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306437919305216. Guide on Good Data Protection Practice in Research (2019) [Online]. Available: https://www.eui.eu/documents/servicesadmin/deanofstudies/researchethics/guide-data-protection-research.pdf. EU-GDPR. (2019). EU GDPR portal. [Online]. Available: https://eugdpr.org. General data protection regulation (2018). Official Journal of the European Union [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

2.10 LU10 - Controllo degli accessi basato sui ruoli

Unità di apprendimento 10	Controllo degli accessi basato sui ruoli
Descrizione Generale / Output	Stabilire account di amministratore e limitare i diritti di accesso tra gli impiegati secondo i livelli di sicurezza definiti.
Numero di codice	LU 10
Tipo	Obbligatorio – da definire
Volume	Ore – da definire
Competenze da acquisire	I partecipanti imparano a capire l'importanza di limitare l'accessibilità a dati, informazioni o infrastrutture fisiche quando possibile, e di concedere l'accesso solo a un gruppo di dipendenti pertinenti. Imparano a stabilire restrizioni appropriate secondo un livello di sicurezza definito. I partecipanti saranno in grado di assegnare i ruoli all'interno dell'azienda ai livelli di autorizzazione e di rendere tracciabile l'accesso a specifiche informazioni, se necessario.
Risultati di apprendimento	**Competenze Tecniche** I partecipanti **Imparano** - come identificare le operazioni chiave con dati personali che vengono eseguite all'interno di un'organizzazione. - come stabilire l'accessibilità delle informazioni a gruppi specifici di dipendenti. - come stabilire le restrizioni appropriate secondo i livelli di sicurezza definiti e concordati quando ritenuto necessario. Può **Possono** - distinguere i ruoli dei singoli impiegati e dei gruppi per definire le loro esigenze per i vari livelli di sicurezza (in base ai livelli di sicurezza assegnati concordati con la direzione). - trovare soluzioni appropriate per i singoli dipendenti o gruppi in termini di accesso o restrizioni ed è in grado di giustificarle. - gestire i diritti dei singoli utenti, che diventa una questione di semplice assegnazione di ruoli appropriati all'account dell'utente, quando i ruoli sono chiaramente definiti (dalla direzione). **Competenze Personali** **I partecipanti sono in grado di** - assegnare autonomamente ruoli appropriati secondo le specifiche della direzione (livelli di sicurezza assegnati). - Comunicare in modo autonomo con i colleghi e con la direzione avendo sicurezza nell' interazione. - riconoscere autonomamente la responsabilità che appartiene al compito e rispettare le esigenze degli altri.

Raccomandazioni per apprendimento ed insegnamento	Imparare/insegnare le tre regole principali definite per RBAC: 1) Assegnazione dei ruoli, 2) Autorizzazione dei ruoli, 3) Autorizzazione dei permessi. Pensare all'importanza della sensibilizzazione nell'attribuzione dei ruoli e prendere accordi chiari con la direzione.
Letteratura ed altre fonti	Blokdyk, G., (2017). Role-based Access Control: A Successful Design Process. D Ferraiolo, DR Kuhn, R Chandramouli, (2003), Role-based access control. Benantar, M., (2006)., Access Control Systems: Security, Identity Management and Trust Models. New York: Springer. Zhang, E. (2020). What is Role-Based Access Control (RBAC)? Examples, Benefits, and More [Online]. Available: https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more.

2.11 LU11 – Gestione delle Password

Unità di apprendimento 11	Gestione delle Password
Description Generale / Output	Stabilire delle password per l'accesso individuale dei dipendenti e permettere un processo di archiviazione e recupero sicuro.
Numero di codice	LU 11
Tipo	Obbligatorio – da definire
Volume	ore – da definire
Competenze da acquisire	I partecipanti imparano a capire l'importanza di centralizzare la gestione dell'utilizzo delle password all'interno dell'azienda. Impareranno come definire le password che garantiscono l'autenticazione (dei dipendenti) e come resettare le stesse. I partecipanti imparano come creare strutturalmente, usare/gestire, memorizzare e cambiare le password dei dipendenti.
Risultati di apprendimento	**Competenze Tecniche** I partecipanti **Imparano** - sulla memorizzazione della password. - sulla trasmissione della password. - Informazioni su come indovinare una password. - Informazioni sul furto tramite cracking della password. - sulla sostituzione della password. **Possono** - educare il team sulle migliori pratiche per le password. - educare il team sulla sicurezza informatica. - decidere quali tipi di password non usare. - generare password complesse. - sfruttare il potenziale dell'automazione. - eliminare le password complesse. - eliminare la necessità di reimpostare le password. - garantire la verifica e la tracciabilità delle password. **Competenze Personali** **I partecipanti sono in grado di** - riconoscere la documentazione dei processi come punto di partenza per ulteriori fasi di lavoro. - Lavorare in modo strutturato con attenzione ai dettagli. - Riconoscere la responsabilità del compito ed essere sicuro nell'interazione con gli altri. - gestire i principali compiti richiesti con un buon livello di autono-mia. - enfatizzare le loro competenze sociali (soft skills, empatia e comunicazione in particolare).

Raccomandazioni per apprendimento ed insegnamento	Gestione delle password con l'aiuto di esempi reali. Esercizi sulla documentazione in forma libera e con l'aiuto di moduli di testo.
Letteratura & altre fonti	Luca, M. (2008). Password Management for Distributed Environments. Saarbrücken: VDM Verlag Dr. Müller. Smith, S. B. (2017). Password Manager: Keep Record of Internet User ID and Passwords in the Password Manage. Keep your internet login info in a safe offline location. CreateSpace: North Charleston.

2.12 LU12 – Gestione della contunità aziendale

Unità di apprendimento 12	Gestione della continuità aziendale
Descrizione Generale / Output	Stabilire linee guida e procedure per affrontare eventuali imprevisti.
Numero di codice	LU 12
Tipo	Obbligatorio – da definire
Volume	Ore - da definire
Competenze da acquisire	I partecipanti imparano a capire l'importanza di considerare scenari "what if". Imparano ad analizzare le emergenze teoriche e a preparare linee guida strategiche di conseguenza. I partecipanti saranno in grado di stabilire linee guida e di predefinire misure per essere preparati e rispondere in modo coordinato a nuove situazioni quando si presentano.
Risultati di apprendimento	**Competenze Tecniche** I partecipanti **Imparano** come trovare documenti nazionali e come cercare la competenza nei documenti legali nazionali che regolano la sicurezza e la protezione dei dati. - tecniche di simulazione per prevedere potenziali violazioni di dati. - come gestire le regole per la valutazione del rischio. **Possono** - identificare i rischi usando diverse tecniche e stili di comunicazione. - implementare le regole di valutazione dei rischi agendo con l'approvazione della direzione. - pianificare e sviluppare soluzioni adattandosi alle circostanze e ai cambiamenti su scala organizzativa e implementarle agendo con l'approvazione della direzione. - trovare nuove soluzioni basate sull'analisi di eventi precedenti. CompetenzaPersonale **I partecipanti sono in grado di** - lavorare in circostanze sfavorevoli pur essendo legati ai dettagli. - adattarsi facilmente a nuove circostanze. - essere un esempio per gli altri impiegati seguendo il loro codice etico di condotta e mostrare responsabilità.
Raccomandazioni per apprendimento ed insegnamento	Pratica teorica di scenari di diverse minacce e situazioni di rischio. Lavorare con esempi di situazioni reali.
Letteratura & altre fonti	Irwin, L. (2019). Why risk assessments are essential for GDPR compliance [Online]. Available:

https://www.itgovernance.co.uk/blog/why-risk-assessments-are-essential-for-gdpr-compliance.

European Data Protection Board (2021). Guidelines 01/2021 on Examples regarding Data Breach Notification [Online]. Available: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf.

European Union Agency for Cybersecurity (2017). Handbook on Security of Personal Data Processing [Online]. Available: www.enisa.europa.eu.

Green, A. (2020). GDPR Data Breach Guidelines - COMPLIANCE & REGULATION [Online]. Available: https://www.varonis.com/blog/guide-eu-gdpr-breach-notification-rule/.

General data protection regulation (2021). Complete guide to GDPR compliance [Online]. Available: https://gdpr.eu/.

2.13 LU13 – Negoziazione e gestione delle parti interessate

Unità didattica 13	Negoziazione e gestione delle parti interessate
Descrizione Generale / Output	Coordinare i bisogni dei dirigenti e dei dipendenti dell'azienda, fornendo a entrambe le parti informazioni e approfondimenti dall'interno dell'azienda.
Numero di codice	LU 13
Tipo	Obbligatorio – da definire
Volume	ore - da definire
Competenze da acquisire	I partecipanti imparano a capire l'importanza di coordinarsi con tutte le parti interessate nell'azienda per quanto riguarda il loro ruolo e il loro impatto sulla protezione dei dati e la sicurezza delle informazioni. Imparano a comunicare efficacemente con i diversi livelli gerarchici (dipendenti e management) e ad armonizzare i loro bisogni e interessi quando si verificano cambiamenti nelle routine organizzative. I partecipanti saranno in grado di interagire con le parti interessate in modo diplomatico e di affrontare possibili resistenze verso la propria azione.
Risultati di apprendimento	**Competenze Tecniche** I partecipanti **Imparano** . - come trovare i documenti legali nazionali che regolano la sicurezza delle informazioni e la protezione dei dati e come reperire le competenze. - Quali canali di comunicazione interna ed esterna si possono applicare agendo con l'approvazione della direzione e quali rischi sono associati ad essi. - quali misure possono essere applicate per osservare, testare e valutare i processi nell'organizzazione. - Quali misure possono essere applicate per valutare i rischi e come gestire la valutazione dei rischi. **Possono** - implementare misure di auditing interno (con l'approvazione della direzione). - pianificare e sviluppare soluzioni strategiche e poi implementarle agendo con l'approvazione della direzione. - sviluppare una cultura della prevenzione con l'appoggio della direzione. - identificare, valutare e dare priorità ai rischi. - creare regolamenti interni su scala organizzativa e implementarli (con l'approvazione della direzione). **Competenze Personali** **I partecipanti sono in grado di** - affrontare il cambiamento e l'adattamento. - essere creativi e cercare di crescere ulteriormente.

	- fare leva sul proprio codice etico in modo che gli altri possano seguire il loro esempio.
Raccomandazioni per Apprendimento ed insegnamento	Fondere la conoscenza teorica e l'approccio con esempi pratici. Applicare metodi di insegnamento interattivi (per esempio: lavori di gruppo, discussioni, analisi di casi, simulazioni di ruolo, ecc.)
Letteratura & altre fonti	IT Governance Privacy Team (2020). EU General Data Protection Regulation (GDPR) – An implementation and compliance guide (4th ed.). General data protection regulation (2021). Complete guide to GDPR compliance [Online]. Available: https://gdpr.eu/. Gorondutse, A. H., & Hilman, H. (2016). Mediation effect of organizational culture on the relationship between perceived ethics and SMEs. Journal of Industrial Engineering and Management 2016, 9(2), 505-529. Straight, J. (2018). GDPR compliance: Identifying an organization's unique profile [Online]. Available: https://www.helpnetsecurity.com/2018/05/14/gdpr-compliance-profile/