MiniGuida

RACCOLTA DI PROCEDURE OPERATIVE: PIANO DI FORMAZIONE EFFICACE, USO VPN, TIPOLOGIE DI ATTACCHI, DATI SENSIBILI,REPORTISTICA, SICUREZZA ANCHE IN *SMART* WORKING.

DI ANDREA BRACCHI

PROCEDURE OPERATIVE

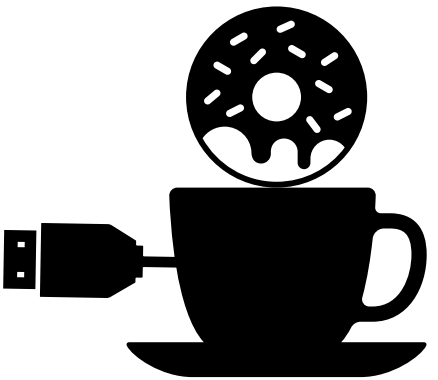
PIANO DI FORMAZIONE EFFICACE: SICUREZZA INFORMATICA

DI ANDREA BRACCHI

Verifica il mio profilo personale su Linkedin

StudioBracchi dal 2019
Sede Legale Via della pace n°27
Pontelagoscuro (Ferrara)

visita: **www.studiobracchi.org**
Info**: studiobracchi.info@gmail.com**



PROLOGO

Conoscenze minime di base, buone pratiche e piano di formazione, una MiniGuida per le aziende che vogliono fornire ai propri collaboratori gli strumenti e le conoscenze per svolgere il proprio lavoro anche in modalità smart working

UNA PROCEDURA DETTAGLIATA PER COSTRUIRE UNA FORMAZIONE EFFICACE SULLA SICUREZZA INFORMATICA IN AZIENDA:

1. **Identificare i destinatari:** Identificare i collaboratori e gli utenti che devono essere formati sulla sicurezza informatica, ad esempio personale che utilizza dati sensibili o che lavora da remoto.
2. **Definire gli obiettivi della formazione:** Definire gli obiettivi specifici della formazione sulla sicurezza informatica, ad esempio aumentare la consapevolezza sui rischi di sicurezza, migliorare la conoscenza delle pratiche di sicurezza informatica e rafforzare le politiche di sicurezza dell'organizzazione.
3. **Selezionare il contenuto della formazione:** Selezione il contenuto della formazione, tenendo presente gli obiettivi della formazione e le esigenze dei destinatari. Il contenuto potrebbe includere le seguenti tematiche: password sicure, phishing, malware, attacchi informatici, gestione dei dati sensibili, connessioni sicure e politiche di sicurezza dell'organizzazione.

4. **Scegliere la modalità di formazione:** Scegliere la modalità di formazione più adatta alle esigenze dei destinatari. Ad esempio, la formazione potrebbe essere fornita attraverso corsi in aula, corsi online, webinar, video tutorial, manuali di formazione, ecc.
5. **Pianificare la formazione:** Pianificare la formazione, definendo il calendario della formazione, la durata delle sessioni di formazione, il numero di partecipanti per sessione e i requisiti tecnologici per partecipare alla formazione.
6. **Erogare la formazione:** Erogare la formazione secondo il piano stabilito, assicurandosi che i destinatari partecipino attivamente alla formazione e che siano in grado di acquisire le competenze necessarie.
7. **Valutare l'efficacia della formazione:** Valutare l'efficacia della formazione, raccogliendo feedback dai partecipanti e misurando l'impatto della formazione sulla sicurezza informatica dell'organizzazione.
8. **Aggiornare la formazione:** Aggiornare la formazione sulla sicurezza informatica regolarmente, tenendo conto dei nuovi rischi di sicurezza e delle nuove tecnologie disponibili.

9. **Comunicare la formazione a tutta l'organizzazione:** Comunicare la formazione sulla sicurezza informatica a tutta l'organizzazione, in modo che tutti gli utenti siano consapevoli dei rischi di sicurezza e delle pratiche di sicurezza informatica adottate dall'organizzazione.

DEFINIRE LE CONOSCENZE MINIME DI BASE DEL COLLABORATORE: *LA SICUREZZA INFORMATICA*

1. **Password sicure:** Il collaboratore deve sapere come creare una password sicura e come utilizzare password differenti per gli account di lavoro e personali. Deve anche sapere come proteggere le sue password e come cambiarle regolarmente.
2. **Phishing:** deve conoscere i segni di phishing e come evitarli. Ad esempio, deve sapere come verificare l'autenticità di un'email o di una pagina web, come non cliccare sui link sospetti e come non fornire informazioni sensibili.
3. **Malware:** deve sapere come proteggere il suo computer e la rete da malware, ad esempio attraverso l'installazione di un antivirus e l'aggiornamento regolare del sistema operativo.
4. **Attacchi informatici:** deve conoscere i tipi di attacchi informatici e come evitarli, ad esempio attraverso l'installazione di un firewall, l'utilizzo di connessioni sicure e la limitazione degli accessi alle informazioni sensibili.

5. **Gestione dei dati sensibili:** Il collaboratore deve comprendere come gestire in modo sicuro i dati sensibili, ad esempio utilizzando la crittografia, il backup regolare e la distruzione sicura dei dati obsoleti.
6. **Connessioni sicure:** deve sapere come utilizzare le connessioni sicure per evitare la perdita di dati e l'accesso non autorizzato. Ad esempio, deve sapere come utilizzare una rete VPN e come non connettersi a reti Wi-Fi pubbliche non sicure.
7. **Politiche di sicurezza dell'organizzazione:** Il collaboratore deve conoscere le politiche di sicurezza dell'organizzazione e come rispettarle. Ad esempio, deve sapere come utilizzare i sistemi di sicurezza dell'organizzazione, come gestire le password e come evitare la divulgazione di informazioni sensibili.
8. **Reportistica:** deve sapere come segnalare eventuali violazioni della sicurezza o sospette attività malevole al personale incaricato della sicurezza informatica dell'organizzazione.
9. **Aggiornamento delle conoscenze:** Il collaboratore deve essere consapevole della necessità di aggiornare le sue conoscenze di sicurezza informatica in base alle nuove minacce e alle nuove tecnologie disponibili.

10. **Formazione continua:** Il collaboratore deve essere disposto a partecipare a corsi di formazione sulla sicurezza informatica e ad attivarsi per migliorare la sicurezza informatica dell'organizzazione.

UNA PROCEDURA OPERATIVA PER CREARE E GESTIRE *PASSWORD SICURE:*

1. **Utilizzare una combinazione di lettere, numeri e caratteri speciali:** la password dovrebbe essere composta da almeno otto caratteri che includono lettere maiuscole e minuscole, numeri e caratteri speciali come ! @#$%^&*.
2. **Non utilizzare parole di uso comune:** Evitare di utilizzare parole di uso comune come "password", "123456" o il nome dell'azienda. Queste password sono facilmente prevedibili e non sicure.
3. **Non utilizzare informazioni personali:** Non utilizzare informazioni personali come la data di nascita, il nome dei propri figli o il proprio indirizzo come parte della password. Queste informazioni sono facilmente accessibili e possono essere utilizzate per indovinare la password.
4. **Utilizzare frasi complesse:** Una buona pratica è utilizzare una frase complessa come password, utilizzando maiuscole, minuscole e caratteri speciali. Ad esempio, "il mio cane si chiama Pippo! " potrebbe essere trasformato in “!lIMiOcAnEsIcHiAmApIpPo#".

5. **Utilizzare un password manager:** Utilizzare un password manager per gestire tutte le password, in modo da avere una password diversa per ogni account. Il password manager genererà una password sicura e la salverà in modo sicuro.
6. **Cambiare la password regolarmente:** Cambiare la password regolarmente, ad esempio ogni 30 giorni, per evitare che le password vengano compromesse.
7. **Non condividere la password:** Non condividere mai la password con altri dipendenti o persone esterne all'organizzazione.
8. **Proteggere la password:** Proteggere la password, ad esempio memorizzarla in un posto sicuro o utilizzare la tecnologia di biometria, come l'impronta digitale o la scansione del volto.
9. **Utilizzare la verifica in due passaggi:** Utilizzare la verifica in due passaggi per proteggere l'account. Questa funzione richiederà un codice aggiuntivo generato da un'app o inviato via SMS per accedere all'account, anche se la password è stata compromessa.

10. **Monitorare le violazioni di sicurezza:** Monitorare regolarmente i siti web di violazioni di sicurezza per verificare se le proprie password sono state compromesse. In caso di compromissione della password, cambiare immediatamente la password.

ECCO UNA PROCEDURA OPERATIVA PER PREVENIRE GLI *ATTACCHI DI PHISHING*

1. **Verificare l'autenticità del mittente:** Verificare sempre l'indirizzo email del mittente, anche se sembra affidabile. Controllare se l'indirizzo email è legittimo e appartiene all'organizzazione o alla persona che dice di essere.
2. **Prestare attenzione all'oggetto dell'email:** Leggere attentamente l'oggetto dell'email e verificare se sembra legittimo e pertinente.
3. **Controllare l'ortografia e la grammatica:** Controllare l'ortografia e la grammatica dell'email. Le email di phishing spesso contengono errori grammaticali e di ortografia.
4. **Non fornire informazioni personali:** Non fornire mai informazioni personali come il numero di carta di credito, password o altre informazioni sensibili. Le organizzazioni legittime non chiederanno mai queste informazioni tramite email.
5. **Non cliccare sui link sospetti:** Non cliccare mai su link sospetti o non richiesti. Prima di cliccare su un link, passare il cursore del mouse sopra di esso per verificare l'URL. Se l'URL sembra sospetto, non cliccare.

6. **Non scaricare allegati sospetti:** Non scaricare mai allegati sospetti o non richiesti. Gli allegati possono contenere malware o virus che possono compromettere la sicurezza del computer.
7. **Utilizzare un filtro anti-spam:** Utilizzare un filtro anti-spam per bloccare le email di phishing. Questi filtri possono aiutare a identificare e bloccare le email di phishing prima che arrivino nella casella di posta in arrivo.
8. **Utilizzare il doppio fattore di autenticazione:** Utilizzare il doppio fattore di autenticazione per proteggere gli account. Questo sistema richiederà un codice aggiuntivo generato da un'app o inviato via SMS per accedere all'account, anche se la password è stata compromessa.
9. **Verificare l'autenticità di una pagina web:** Verificare sempre l'URL di una pagina web e controllare se è protetto da un certificato SSL. Inoltre, verificare se la pagina web richiede informazioni sensibili e se sembra legittimo.

10. **Segnalare l'email di phishing:** Segnalare sempre le email di phishing all'organizzazione o all'amministratore del sistema per aiutare a prevenire futuri attacchi di phishing.

UNA PROCEDURA OPERATIVA PER PROTEGGERE IL COMPUTER E LA RETE DA MALWARE:

1. **Installazione di un antivirus:** Installare un software antivirus sul computer e assicurarsi che sia aggiornato regolarmente per proteggere il sistema da eventuali minacce di malware.
2. **Verifica dei file scaricati:** Verificare sempre i file scaricati prima di aprirli. Assicurarsi che il file sia proveniente da una fonte affidabile e che sia stato scansionato dal software antivirus.
3. **Utilizzare solo software autorizzato:** Installare solo software autorizzato e proveniente da fonti affidabili.
4. **Aggiornamento del sistema operativo:** Assicurarsi di mantenere il sistema operativo e il software aggiornati regolarmente. Questi aggiornamenti includono spesso correzioni di sicurezza per le vulnerabilità del sistema.
5. **Utilizzo di password sicure:** Utilizzare password sicure e complesse per accedere al computer e ai dati sensibili. Cambiare regolarmente le password e non condividerle con nessuno.

6. **Utilizzare una rete sicura:** Utilizzare solo reti sicure e protette per accedere a Internet. Evitare di utilizzare reti pubbliche o non protette che possono essere facilmente compromesse.
7. **Verifica dell'indirizzo del sito web:** Verificare sempre l'indirizzo del sito web prima di inserire qualsiasi informazione personale o sensibile. Assicurarsi che l'URL inizi con "https" e che sia protetto da un certificato SSL.
8. **Utilizzare il doppio fattore di autenticazione:** Utilizzare il doppio fattore di autenticazione per accedere al computer e ai dati sensibili.
9. **Controllo dei messaggi di errore:** Non ignorare i messaggi di errore del sistema o del software. Questi messaggi possono indicare un problema di sicurezza o un'attività sospetta.
10. **Backup dei dati:** Effettuare regolarmente il backup dei dati importanti su un'unità esterna o sul cloud per proteggere i dati in caso di attacco di malware o di perdita di dati.

CONOSCERE LE TIPOLOGIE DI ATTACCHI INFORMATICI ANCHE IN *SMART* WORKING

UNA PROCEDURA OPERATIVA PER AIUTARE I COLLABORATORI A CONOSCERE I TIPI DI ATTACCHI INFORMATICI E COME EVITARLI:

1. **Conoscenza dei tipi di attacchi informatici:** Informare i collaboratori dei vari tipi di attacchi informatici più comuni, come phishing, malware, ransomware, attacchi di spoofing, attacchi DDoS, e così via. Fornire esempi concreti di casi in cui questi attacchi sono stati effettuati con successo, così che i dipendenti possano comprendere la loro pericolosità.
2. **Formazione sulla prevenzione degli attacchi informatici:** Offrire formazione su come prevenire gli attacchi informatici. Questo può includere l'utilizzo di software antivirus, l'installazione di aggiornamenti di sicurezza, l'adozione di buone pratiche di sicurezza informatica e la conoscenza delle tecniche di ingegneria sociale utilizzate dagli hacker.

3. **Monitoraggio delle attività sospette:** Informare i collaboratori sull'importanza di monitorare costantemente le attività sospette sul loro computer e sulla rete. Ciò include la segnalazione immediata di qualsiasi attività sospetta, come l'apertura di file o l'accesso a siti Web sospetti.
4. **Aggiornamento regolare dei software:** trasmettere ai collaboratori l'importanza di mantenere sempre aggiornati i software sui loro computer. Questo è particolarmente importante per il sistema operativo, il browser Web e il software antivirus, poiché questi sono i software più comunemente presi di mira dagli hacker.
5. **Backup dei dati:** Informare i collaboratori sull'importanza del backup dei dati. In caso di attacco informatico o di perdita di dati, il backup può essere utilizzato per ripristinare le informazioni crittografate o perse.
6. **Segnalazione degli incidenti di sicurezza:** Infine, è importante informare i collaboratori sull'importanza di segnalare tempestivamente qualsiasi incidente di sicurezza al proprio responsabile della sicurezza informatica.

DATI SENSIBILI

UNA PROCEDURA OPERATIVA PER UNA GESTIONE PIÙ SICURA DEI DATI SENSIBILI:

1. **Identificare i dati sensibili:** I collaboratori devono essere in grado di identificare i dati sensibili, come informazioni personali, finanziarie o di proprietà dell'azienda. Questi dati devono essere archiviati in modo sicuro e accessibili solo a chi ha bisogno di conoscerli.
2. **Utilizzo della crittografia:** La crittografia dei dati sensibili deve essere utilizzata per proteggere le informazioni durante il trasferimento o la conservazione. Gli addetti devono essere in grado di utilizzare la crittografia, come ad esempio la crittografia a chiave pubblica, per proteggere i dati sensibili.
3. **Backup regolare dei dati:** I dati sensibili devono essere salvati regolarmente in un sistema di backup sicuro. Gli addetti devono essere in grado di eseguire backup regolari dei dati sensibili e di verificare che il backup sia stato effettuato correttamente.

4. **Limitare l'accesso ai dati sensibili:** L'accesso ai dati sensibili deve essere limitato solo a coloro che hanno bisogno di conoscere tali informazioni per svolgere il loro lavoro. Gli addetti devono essere informati riguardo alla sensibilità dei dati e devono capire che la condivisione di queste informazioni con persone non autorizzate è una violazione della politica aziendale.
5. **Distruggere i dati obsoleti:** Quando i dati sensibili non sono più necessari, devono essere distrutti in modo sicuro. Gli addetti ai dati sensibili, devono essere in grado di identificare i dati obsoleti e di distruggerli in modo sicuro, ad esempio attraverso l'uso di software di cancellazione dei dati o la distruzione fisica dell'hardware.
6. **Monitoraggio dell'accesso ai dati sensibili:** Il monitoraggio dell'accesso ai dati sensibili è essenziale per garantire che solo gli addetti autorizzati abbiano accesso a tali informazioni. I collaboratori devono essere informati che l'accesso ai dati sensibili viene monitorato e registrato e che l'uso improprio di questi dati può comportare sanzioni disciplinari.

7. **Formazione continua:** I collaboratori devono ricevere una formazione specifica sulla gestione sicura dei dati sensibili per essere sempre aggiornati sulle nuove minacce informatiche e sulle migliori pratiche di sicurezza. La formazione continua può includere corsi di formazione online o seminari di formazione sul posto di lavoro.
8. **Verificare la conformità alle normative:** L'azienda deve verificare la conformità alle normative sulla protezione dei dati sensibili, come il GDPR (General Data Protection Regulation) dell'Unione Europea. I collaboratori devono essere informati riguardo alle normative in vigore e devono capire che la violazione delle normative può comportare sanzioni legali per l'azienda e per loro personalmente.

CONNESSIONI SICURE

UNA PROCEDURA SEMPLICE PASSO PER PASSO PER MANTENERE LE CONNESSIONI SICURE:

1. **Utilizzare una rete VPN:** La VPN (Virtual Private Network) è una tecnologia che consente di creare una connessione sicura tra il tuo dispositivo e la rete aziendale. *Seguire queste punti:*

➡ Installa il software VPN fornito dall'azienda sul tuo dispositivo.

➡ Accedi alla VPN utilizzando le credenziali fornite dall'azienda.

➡ Una volta connesso, tutte le tue attività online saranno crittografate e sicure.

2. **Evitare le reti Wi-Fi** pubbliche non sicure: Le reti Wi-Fi pubbliche, come quelle nei caffè o negli aeroporti, possono essere vulnerabili agli attacchi informatici. *Seguire queste istruzioni:*

➡ Evita di connetterti a reti Wi-Fi pubbliche non protette.

➡ Se devi utilizzare una rete Wi-Fi pubblica, utilizza una connessione VPN per crittografare i tuoi dati.

➡ Non accedere a informazioni sensibili, come conti bancari o password, quando sei connesso a una rete Wi-Fi pubblica.

3. **Utilizzare connessioni HTTPS:** HTTPS è un protocollo di sicurezza che crittografa i dati durante la trasmissione. *Seguire queste istruzioni:*

➡ Utilizza sempre connessioni HTTPS quando sei online.

➡ Verifica sempre che l'URL del sito web inizia con "https://" e che sia presente un lucchetto vicino all'URL.

➡ Non fornire mai informazioni sensibili su siti web non sicuri.

4. **Verificare l'autenticità dei siti web:** Gli hacker possono creare siti web falsi per rubare informazioni personali. *Seguire queste istruzioni:*

➡ Verifica sempre l'URL del sito web prima di fornire informazioni personali o sensibili.

➡ Non fornire mai informazioni personali o sensibili su siti web non verificati o non autentici.

➡ Utilizza strumenti di sicurezza come Safe Browsing di Google per verificare la sicurezza dei siti web.

LA CONOSCENZA DELLE POLITICHE DI SICUREZZA DELL'ORGANIZZAZIONE È FONDAMENTALE PER GARANTIRE LA SICUREZZA DELLE INFORMAZIONI AZIENDALI E DEI CLIENTI.

SENSIBILIZZARE E FAR COMPRENDERE L'APPLICAZIONE DELLE POLITICHE DI SICUREZZA DELL'ORGANIZZAZIONE:

1. **Comunicazione delle politiche di sicurezza:** l'organizzazione deve fornire ai collaboratori le politiche di sicurezza in modo chiaro e completo. Queste politiche devono essere accessibili e comprensibili per tutti.
2. **Formazione sui requisiti di sicurezza:** l'organizzazione deve fornire formazione sui requisiti di sicurezza delle politiche dell'organizzazione. La formazione dovrebbe comprendere le politiche di sicurezza dell'organizzazione, le modalità di protezione delle informazioni aziendali e dei clienti, le procedure per la gestione dei dati sensibili e le conseguenze in caso di violazione delle politiche di sicurezza.
3. **Implementazione delle politiche di sicurezza:** l'organizzazione deve implementare le politiche di sicurezza attraverso l'uso di tecnologie, software e strumenti di sicurezza appropriati. Inoltre, i collaboratori devono essere informati sui sistemi di sicurezza dell'organizzazione e sulle loro funzionalità.

4. **Responsabilità dei Collaboratori:** i collaboratori devono essere consapevoli delle proprie responsabilità per garantire la sicurezza delle informazioni aziendali e dei clienti. Essi devono conoscere e rispettare le politiche di sicurezza dell'organizzazione, utilizzando i sistemi di sicurezza dell'organizzazione come prescritto e segnalando eventuali violazioni o problemi di sicurezza.
5. **Monitoraggio delle politiche di sicurezza:** l'organizzazione deve monitorare costantemente le politiche di sicurezza per identificare eventuali violazioni o problemi di sicurezza. I collaboratori devono essere informati sul monitoraggio e sulla necessità di rispettare le politiche di sicurezza dell'organizzazione.
6. **Aggiornamenti delle politiche di sicurezza:** l'organizzazione deve aggiornare periodicamente le proprie politiche di sicurezza per mantenere al passo con le minacce emergenti e le tecnologie disponibili.

REPORTISTICA

LA SEGNALAZIONE DI VIOLAZIONI DELLA SICUREZZA O SOSPETTE ATTIVITÀ MALEVOLI

1. **Identificazione della violazione o attività sospetta:** il collaboratore deve essere in grado di riconoscere le violazioni della sicurezza o le attività sospette che possono verificarsi durante l'utilizzo dei sistemi informatici dell'organizzazione. Ciò può includere, ad esempio, accessi non autorizzati, tentativi di phishing o di attacchi informatici, furti di dati, comportamenti inappropriati di altri utenti, perdita di dispositivi mobili contenenti dati sensibili, e così via.
2. **Segnalazione immediata:** una volta identificata una violazione della sicurezza o un'attività sospetta, il collaboratore deve segnalarla immediatamente al personale incaricato della sicurezza informatica dell'organizzazione. Ciò può essere fatto immediatamente attraverso un numero di telefono o una e-mail dedicati, o attraverso un sistema di ticketing appositamente creato per la segnalazione di tali eventi.

3. **Descrizione dettagliata dell'evento:** il collaboratore deve fornire una descrizione dettagliata dell'evento o della violazione della sicurezza, comprensiva di tutte le informazioni rilevanti, come la data e l'ora dell'evento, il tipo di violazione o attività sospetta, i nomi degli utenti coinvolti, gli eventuali errori commessi e così via.
4. **Supporto all'investigazione:** deve fornire tutte le informazioni e il supporto necessari al personale incaricato della sicurezza informatica per condurre l'investigazione sulla violazione della sicurezza o sull'attività sospetta. Ciò può includere, ad esempio, la possibilità di accedere al sistema informatico per verificare le informazioni o la partecipazione a interviste per chiarire la situazione.
5. **Rispetto della privacy e delle politiche dell'organizzazione:** il collaboratore deve rispettare le politiche dell'organizzazione in merito alla sicurezza informatica e alla privacy dei dati. Ciò significa che tutte le informazioni relative alla violazione della sicurezza o all'attività sospetta devono essere gestite con riservatezza e nel rispetto della normativa sulla privacy.

6. **Azioni correttive:** una volta identificata la violazione della sicurezza o l'attività sospetta, l'organizzazione deve prendere le necessarie azioni correttive per risolvere il problema e prevenire futuri eventi simili. Il collaboratore può essere coinvolto in questo processo fornendo suggerimenti o suggerendo soluzioni per migliorare la sicurezza informatica dell'organizzazione.

AGGIORNAMENTO DELLE CONOSCENZE

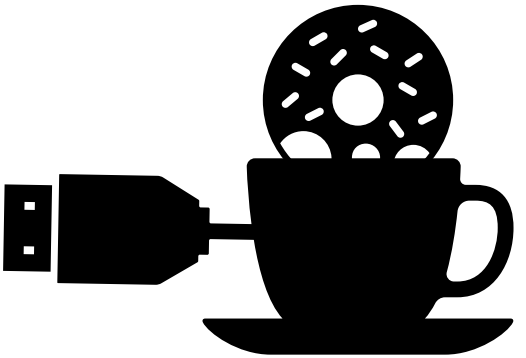
UNA PROCEDURA OPERATIVA PER GARANTIRE L'EFFICACIA DELLA FORMAZIONE CONTINUA DEI COLLABORATORI.

1. **Pianificazione:** La direzione dell'organizzazione deve pianificare la formazione continua dei collaboratori sulla sicurezza informatica come parte del piano di sviluppo delle risorse umane.
2. **Identificazione delle esigenze di formazione:** L'organizzazione deve identificare le esigenze di formazione in base alle funzioni e alle competenze di sicurezza informatica necessarie per svolgere il loro lavoro in modo sicuro.
3. **Selezione dei corsi di formazione:** L'organizzazione deve selezionare corsi di formazione sulla sicurezza informatica appropriati in base alle esigenze di formazione identificate. La selezione dei corsi dovrebbe essere fatta in base alla qualità dei corsi, all'esperienza del formatore, alla loro disponibilità e alla loro aderenza alle politiche di sicurezza dell'organizzazione.*(evitate i*

“discount” tutto compreso, con formazione solo di base)

4. **Programmazione della formazione:** L'organizzazione deve programmare la formazione in base alle esigenze di formazione identificate e alla disponibilità dei corsi di formazione selezionati.
5. **Comunicazione ai Collaboratori:** L'organizzazione deve trasmettere l'importanza della formazione continua sulla sicurezza informatica e come i corsi selezionati aiuteranno a migliorare la loro consapevolezza sulla sicurezza informatica.
6. **Coinvolgimento dei Collaboratori:** L'organizzazione deve coinvolgere i collaboratori nell'attività di formazione, incoraggiandoli a partecipare attivamente ai corsi di formazione e a condividere le loro conoscenze con i colleghi.
7. **Valutazione dell'efficacia:** L'organizzazione deve valutare l'efficacia della formazione continua sulla sicurezza informatica, ad esempio attraverso la verifica del miglioramento delle competenze di sicurezza informatica, il numero di violazioni della sicurezza informatica evitate e il feedback dei dipendenti.

8. **Aggiornamento delle politiche di sicurezza:** L'organizzazione deve aggiornare le politiche di sicurezza in base alle nuove minacce e alle nuove tecnologie disponibili e garantire che i collaboratori siano informati su tali aggiornamenti attraverso la formazione continua sulla sicurezza informatica.



BIOGRAFIA

Da una esperienza di 17 anni in campo, di realizzazione di Procedure a norme ISO, Istruzioni Operative e analisi di Risk management, in ambito di sicurezza sul lavoro nel ruolo di Supervisore, la passione per le nuove discipline che regolano la comunicazione di internet e in ambito web, mi portano ad accostarmi al Diritto informatico.
Lavorando da 4 anni come libero professionista, come consulente privacy, sempre in continuo aggiornamento sia in ambito informatico che in quello giuridico, partecipando a numerosi webinar, workshop, corsi di alta formazione, analisi delle sentenze e certificazioni, approfondisco gli studi iscrivendomi ad un Master in diritto di informatica e certificandomi come DPO.
Gli studi sulla Privacy comparata mi portano ad analizzare più aspetti della materia, quali i reati e crimini informatici, approdando anche alle discipline della Digital Forensics, Cybersecurity, Ingegneria Sociale e Osint.
sono convinto che ogni professione è esercitata da uomini ed è rivolta ad altri uomini.
L'attività lavorativa ha una ricaduta diretta sulla vita dell'uomo e assume quindi, inevitabilmente, un risvolto Etico.