Centro Formazione Professionale CFP COMO

Agenzia per la Formazione, l'Orientamento e il Lavoro

della Provincia di Como

Mappatura delle Attività

e

Analisi dei rischi *ex* d.lgs. 231/2001

Rev. 2 - 2024

LFA

Luigi Fagetti & Associati

22100 COMO - Via Volta, 66- Tel. 031/278800 - Fax 031/2749023
info@studiolegalefagetti.com - www.studiolegalefagetti.com

Approvato dall'Amministratore Unico

con Delibera n°1473/2024 del 20.12.2024

Contenuti:

Ciclo Amministrazione – Mappatura
Ciclo Amministrazione – Sensibilità al rischio
Ciclo Amministrazione – Risk Control Matrix
Ciclo Amministrazione – Gap analysis e Piano d'Azione

Ciclo Direzione – Mappatura
Ciclo Direzione – Sensibilità al rischio
Ciclo Direzione – Risk Control Matrix
Ciclo Direzione – Gap analysis e Piano d'Azione

Ciclo Formazione – Mappatura
Ciclo Formazione – Sensibilità al rischio
Ciclo Formazione – Risk Control Matrix
Ciclo Formazione – Gap analysis e Piano d'Azione

Ciclo Orientamento e Lavoro – Mappatura
Ciclo Orientamento e Lavoro – Sensibilità al rischio
Ciclo Orientamento e Lavoro – Risk Control Matrix
Ciclo Orientamento e Lavoro – Gap analysis e Piano d'Azione

Ciclo Segreteria – Mappatura
Ciclo Segreteria – Sensibilità al rischio
Ciclo Segreteria – Risk Control Matrix
Ciclo Segreteria – Gap analysis e Piano d'Azione

Ciclo Sostegno – Mappatura
Ciclo Sostegno – Sensibilità al rischio
Ciclo Sostegno – Risk Control Matrix
Ciclo Sostegno – Gap analysis e Piano d'Azione

Ciclo Amministrazione – Mappatura

GESTIONE ACQUISTI (BENI E MATERIALI)	La richiesta di acquisto viene effettuata dai richiedenti sulla base del Mod.40 del MQ (Modulo Qualità), che prende il nome di "Richiesta di materiale/servizi" e consegnata al Referente Fornitori/Acqusti che compila il Mod.42 DEL MQ, definito "Ordine di acquisto". Il Referente ufficio acquisti/magazzino/mautenzione predispone l'istruttoria utilizzando l'elenco dei fornitori, cioè il Mod.18 del MQ denominato "Elenco Fornitori Abituali" oppure selezionando l'azienda fornitrice nel rispetto del Regolamento e del Codice degli Appalti. Alla ricezione del materiale, l'incaricato sottopone la merce ad un primo controllo di qualità, e segnala al Referente Fornitori/Acquisto/Magazzino l'idoneità o meno del materiale con relativa motivazione. In caso di inidoneità, il Referente lo segnala sul Mod.42 Ordine di Acqusito e invia la segnalazione al fornitore. Per quanto riguarda l'effettuazione di opere di manutenzione, l'Operatore Tecnico della Logistica ne controlla la qualità e, in caso di inidoneità, lo segnala al Responsabile Ufficio Manutenzioni che invia la segnalazione che al fornitore. In caso di acquisti per contanti, che prevedono quindi l'utilizzo della cassa contanti, IL Referente Fornitori/Acquisti/Magazzino predispone relativo mandato di cassa, autorizzato dal Direttore, e provvede a erogare la somma a chi effettua l'acquisto. Ulteriori dettagli sul processo sono descritti al capitolo 5 del MQ.	**RESPONSABILE AMMINISTRATIVO** **REFERENTE FORNITURE ACQUISTI MAGAZZINO - MANUTENZIONE** **DIRETTORE (VICE-DIRETTORE)**
GESTIONE FORNITORI	L'Agenzia si avvale di fornitori abituali presenti nel Mod.18 del MQ denominato "Elenco Fornitori Abituali", che abbiano garantito prestazioni, sia in termini di qualità, sia di puntualità nelle consegne che di rapporto qualità prezzo. La qualità nella consegna viene misurata come rapporto percentuale tra il numero di forniture non idonee e il numero delle forniture totali. Le non conformità vengono gestite secondo le modalità contenute nel capitolo settimo del MQ denominato "Misurazioni, Analisi, Miglioramento". I fornitori che non soddisfano le condizioni di qualità vengono esclusi dalla lista suddetta. Per l'individuazione dei nuovi fornitori l'Agenzia aggiorna il Mod.18 MQ "Elenco Fornitori Abituali" mediante un'indagine di mercato tra le Aziende in possesso di idonea qualificazione economico, finanziaria e tecnico organizzativa per assicurare la fornitura di beni e servizi richiesti. Per la fornitura di beni e servizi utilizzati per lo svolgimento delle attività dell'Agenzia soggette a finanziamento pubblico dovranno essere rispettate le norme e le procedure meglio definite dai diversi Enti finanziatori, al fine di garantirne la relativa rendicontazione. Ulteriori dettagli sul processo sono descritti nel capitolo 5 del MQ.	**RESPONSABILE AMMINISTRATIVO** **REFERENTE FORNITURE ACQUISTI MAGAZZINO - MANUTENZIONE**
FATTURAZIONE (ATTIVA/PASSIVA)	La fatturazione passiva segue iter differenti a seconda dell'oggetto: beni e servizi (tra cui le manutenzioni) o prestatori intellettuali. Nel primo caso si applica quanto previsto dal MQ capitolo 5: addetto ufficio acquisti effettua una verifica di coerenza fattura/ordine/contratto, se il controllo è positivo la fattura viene registrata in contabilità gestionale e successivamente contabilizzata. Successivamente passa in pagamento secondo i termini contrattuali previsti. Nel caso dei prestatori intellettuali è Responsabile Amministrativo che verifica la coerenza con il contratto in essere, con i registri tramite gestionale (GRS) e con i timesheet compilati dai docenti per le attività diverse dalla docenza. Fatturazione Attiva --> attività residuale per servizi forniti (es. catering, affitto sale, organizzazione eventi o corsi non finanziati, attività finanziate per disoccupati, donne vittime di violenza, detenuti, ecc.). La fattura viene emessa sulla base della scheda d'iscrizione (ad esempio per corsi effettuati) o del relativo contratto/preventivo/bando.	**RESPONSABILE AMMINISTRATIVO** **REFERENTE FORNITURE ACQUISTI MAGAZZINO - MANUTENZIONE**
TESORERIA (ATTIVA/PASSIVA)	Ogni pagamento è subordinato all'emissione di un apposito mandato di pagamento (predisposto dall' Ufficio Amministrativo). I pagamenti avvengono principalmente tramite bonifico bancario con firma congiunta del Direttore e dell'Amministratore Unico. Il pagamento tramite assegni segue lo stesso iter e prevede anch'esso la firma congiunta. I mandati di pagamento per cassa sono a firma singola del Direttore. Gli incassi di bar/ristorante (aperto esclusivamente a clienti istituzionali: docenti, genitori, fornitori, ecc.) vengono registrati quotidianamente (pos/contanti). I contanti vengono versati con cadenza generalmente trimestrale. La cassa viene anche utilizzata per gli acquisti per contanti. Non c'è home banking dispositivo ma solo informativo: si effettua un monitoraggio delle prime note e la comparazione quotidiana con l'estratto conto. A seguito del check i movimenti vengono registrati in contabilità.	**RESPONSABILE AMMINISTRATIVO** **REFERENTE FORNITURE ACQUISTI MAGAZZINO - MANUTENZIONE** **DIRETTORE** **AMMINISTRATORE UNICO**

CONTABILITA'/FORMAZIONE BILANCIO	Il Referente Contabilità cura la registrazione in contabilità gestionale e l'esportazione dei dati in contabilità ordinaria (in automatico tramite sistema informatico). Le rettifiche vengono registrate manualmente così come i fuori campo IVA. Il Responsabile Amministrativo, col supporto di commercialista esterno, predispone i dati per la stesura del fascicolo di bilancio. Il commercialista esterno predispone il fascicolo. Trimestralmente, il Direttore, l'Amministratore Unico, il Responsabile Amministrativo, il Commercialista esterno e il Revisore dei Conti effettuano l'analisi dello stato di avanzamento con la previsione. Il Direttore controlla e verifica il processo di formazione del bilancio.	**DIRETTORE** **RESPONSABILE AMMINISTRATIVO** **COMMERCIALISTA ESTERNO / REVISORE DEI CONTI**
GESTIONE RISORSE UMANE	La gestione delle risorse umane si applica relativamente a: -ricerca, selezione ed assegnazione incarichi; -inserimento dei neo-assunti; -informazione, formazione monitoraggio e aggiornamento del personale. Le richieste di candidature vengono formalizzate attraverso il portale dell'Agenzia. Una Commissione (interna, se del caso integrata da componenti esterni tecnici) nominata dall'Amministratore Unico provvede ad esaminare le candidature e al relativo giudizio di idoneità, che viene pubblicizzato sul portale dell'Agenzia. I colloqui vengono tenuti dal Direttore, affiancato dai responsabili d'area (formazione e orientamento/lavoro). Il numero di colloqui può variare a seconda della complessità dell'incarico/assunzione. La formalizzazione dell'incarico spetta al Direttore, che agisce congiuntamente con l'Amministratore Unico. Per quanto concerne la prassi rimandiamo al capitolo secondo del MQ.	**DIRETTORE** **AMMINISTRATORE UNICO** **RESPONSABILE AMMINISTRATIVO** **RESPONSABILE RISORSE UMANE** **VICE-DIRETTORE** **RESPONSABILI AREA FORMAZIONE E ORIENTAMENTO/LAVORO**
RENDICONTAZIONE	L'attività di rendicontazione viene ricoperta dal Responsabile Amministrativo, con l'ausilio del Referente Ufficio Acquisti/Magazzino e con il ViceDirettore che è anche il Responsabile dell'Area Progettazione. I termini, le modalità, le regole sono differenti in relazione ai diversi bandi in funzione dei quali sono stati elaborati i progetti, e possono essere coinvolti anche i Responsabili d'Area. Tali regole seguono le direttive sancite dai progetti nei rispettivi bandi (Regione Lombardia, Progetto Erasmus, PNRR, ecc).	**RESPONSABILE AMMINISTRATIVO** **REFERENTE FORNITURE ACQUISTI MAGAZZINO - MANUTENZIONE** **VICE-DIRETTORE ED EVENTUALMENTE I RESPONSABILI D'AREA IN RELAZIONE AL PROGETTO/CORSO DA RENDICONTARE**
GESTIONE DEI SISTEMI INFORMATIVI - ARCHIVI FISICI	Lo stabile storico è situato a Como in via bellinzona 88, la struttura è delimitata esternamente da una muraglia con cancelli automatici chiusi L'ingresso principale è monitorato dalla Segreteria. La sala ced risiede al primo piano interrato, la porta d'accesso REI tagliafuoco risulta chiusa a chiave. L'accesso è monitorato da una telecamera di sorveglianza. La sala è utilizzata anche come magazzino di materiale informatico. Le chiavi della sala ced sono in segreteria, non presente un registro per gli accessi. All'interno della sala ced sono presenti due armadi rack, uno che ospita la parte server e l'altro per le apparecchiature di rete e fonia. Entrambi gli armadi sono protetti da un gruppo UPS per gestire gli sbalzi di tensione e interruzioni di corrente, l'Ups però non gestisce lo spegnimento automatizzato dei server. Attualmente non sono presenti sonde d'allarme, i server sono tarati per lo spegnimento in caso di alte temperature ma senza una procedura di sicurezza, sono presenti avvisi via mail ricevuti da cierre. La sala ced ha un sistema di raffrescamento interno. E' presente inventario degli asset interno gestito da Cierre che comprende hardware, software si tratta più che altro di un inventario operativo che di gestione Asset. Gli archivi cartacei sono stipati in Garage eterni sotto il parcheggio, gli archivi risultano chiusi a chiave le chiavi sono disponibiliti in segreteria.	**DIRETTORE, RESP. AMM.VO E REFERENTE UFFICIO ACQUISTI / MAGAZZINO / MANUTENZIONE E SEGRETERIA**

GESTIONE DEI SISTEMI INFORMATIVI - ANTIMALWARE	L'azienda si è dotata di vari sistemi di sicurezza per contrastare i malware; per la parte client server è installato l'antivirus Eset, l'antivirus comprende servizi di antiransomware, application control e webfiltering, la gestione è centralizzata su console cloud gestita da cierre. A Protezione dell'infrastruttura è presente un firewall zyxell usg300 (in fase sdi aggiornamento, il prodotto è a fine vita) con servizi attivi di content filtering e antivirus. I servizi mail sono divisi in due parti una parte on premise su server mdeamon che comprende anche un antivirus interno per la parte amministrativa con dominio cfpcomo.com; la parte didattica invece è configurata su servizi google apps con il dominio cfpcomo.education.com i sistemi di sicurezza sono proprietari di google. All'interno dell'infrastruttura non è presente un sistema di gestione delle patch di sicurezza, per la parte client i pc si aggiornano automaticamente e gli utenti decidono quando installare gli updates, per la parte server sono automatizzati. Il firewall si aggiorna ogni settimana in modo automatico, per gli altri apparati di rete come siwtch, access point, nas ecc. gli aggiornamenti sono manuali e non programmati. L'aggiornamento firmware dei server viene svolto all'occorrenza. I collaboratori sono formati e informati sull'utilizzo degli asset, viene svolta formazione attiva durante l'anno, le procedure d'utilizzo risultano documentate. Presente regolamento informatico con procedure documentate a disposizione degli incaricati e degli ADS.	**DIRETTORE, RESP. AMM.VO E REFERENTE UFFICIO ACQUISTI / MAGAZZINO / MANUTENZIONE E SEGRETERIA, DOCENTI E UTENTI**
GESTIONE DEI SISTEMI INFORMATIVI - AUTENTICAZIONE	L'accesso ai Vari PC e SERVER è gestito da credenziali univoche, presente password policy con le seguenti caratteristiche: 8 caratteri comprensivi di caratteri speciali, scadenza password ogni 3 mesi, history standard, blocco account a seguito di multipli tentitivi d'accesso falliti non attivo. Sono presente due domini separati uno utilizzato dalla parte amministrativa e uno per la parte di didattica. La revisione degli accessi viene svolta all'occorrenza in corrispondenza dell'off-boarding di un utente. Le Password della posta elettronica non scadono, non è presente MFA. L'accesso al gestionale amministrativo/didattica/magazzino e personale esterno avviene con la stessa password dell'utente di dominio. L'accesso al portale zucchetti per visualizzare le timbrature, richiesta permessi ecc. è gestito con credenziali univoche per ogni utente, la password scade regolarmente tramite procedura automatizzata, il personale interno ha l'accesso amministratore per gestire e forzare la scadenza password degli account.	**DIRETTORE, RESP. AMM.VO E REFERENTE UFFICIO ACQUISTI / MAGAZZINO / MANUTENZIONE E SEGRETERIA, DOCENTI E UTENTI**
GESTIONE DEI SISTEMI INFORMATIVI - SISTEMA DI AUTORIZZAZIONE	L'azienda usa i 2 server di dominio active directory di Microsoft per gestire le Autorizzazioni, uno per la parte amministrativa e uno per la parte Didattica. Non è presente procedura documentata di on-boarding e off-boarding, ma risulta esserci prassi consolidata tra la direzione e L'IT. (nella procedura di off-boarding e regolamento informatico sono specificati i dettagli della gestione degli account di dominio e e-mail) Presente riesame annuale degli accessi ai sistemi. Gli utenti sono amministratori della macchina.	**DIRETTORE, RESP. AMM.VO E REFERENTE UFFICIO ACQUISTI / MAGAZZINO / MANUTENZIONE E SEGRETERIA, DOCENTI E UTENTI**
GESTIONE DEI SISTEMI INFORMATIVI - BACKUP E DISASTER RECOVERY	Presente sistema di backup Veeam Backup & Replication che svolge il backup di tutte le macchine virtuali, i backup sono giornalieri e vengono svolti su NAS. È attivo un sistema di repliche gestito sempre da Veeam Backup & Replication, le repliche sono attive durante le ore di lavoroe vengono eseguite ogni ora. E' presente un backup aggiuntivo su disco USB che viene portato fuori sede, il disco viene cambiato ogni settimana da Denise, i backup su disco esterno sono Cifrati. I NAS sono presso la sala CED. È presente un Backup in cloud solo per la PEC istituzionale svolto su amazon S3. Presente procedura interna con la documentaizone dei backup e procedura di restore, manca procedura di disaster recovery. Durante l'anno sono stati fatti restore granulari all'occorrenza. Sono presenti alert di buon funzionamento.	**DIRETTORE, RESP. AMM.VO E REFERENTE UFFICIO ACQUISTI / MAGAZZINO / MANUTENZIONE E SEGRETERIA, DOCENTI E UTENTI**
GESTIONE DEI SISTEMI INFORMATIVI - INFRASTRUTTURA DI NETWORKING	Lq rete risulta segmentata, presente Vlan management e vlan backup. Presente rete wi-fi cfp_didattica che può essere utilizzata a fronte di registrazione del mac address del dispositivo e della password di accesso, la registrazione viene gestita da Moriani. La rete wifi è utilizzabile da chi ne fa richiesta, anche a titolo temporaneo come esterni che vengono ad operare al CFP per tempi contingentati. Il mac address viene registrato e poi rimosso al termine dell'attività. I dispositivi collegati a questa rete posson osolamente accedere alla parte relativa alla didattica su apposito server dedicato. La rete uffici amministrativi è separate da quella della Didattica, i sistemi di rete non sono ridondati, i server hanno la ridondanza con alimentatore, 'dischi e scheda di rete. Sono presenti servizi pubblicati tramite firewall drytek, come webmail di mdeamon e il sistema di videosorveglianza, il sistema di video sorveglianza è su una rete separata. Presente connettività dati che serve sia la parte di navigazione internet che la fonia, presente linea di backup con tecnologia wifi.	**DIRETTORE, RESP. AMM.VO E REFERENTE UFFICIO ACQUISTI / MAGAZZINO / MANUTENZIONE E SEGRETERIA, DOCENTI E UTENTI**
GESTIONE DEI SISTEMI INFOMRATIVI - RACCOLTA DI LOG E MONITORAGGIO	È in fase di introduzione un sistema di monitoraggio dei server e dei servizi di rete principali, nonché di un sistema di raccolta log ADS.	**DIRETTORE, RESP. AMM.VO E REFERENTE UFFICIO ACQUISTI / MAGAZZINO / MANUTENZIONE E SEGRETERIA**

CICLO AZIENDALE:	Amministrazione	
#	SEZIONI NUOVE DOPO AGGIORNAMENTO REATI PRESUPPOSTO 2024	CHECK
1	Violazioni del Codice Etico aziendale	Y
2	Reati in danno alla Pubblica Amministrazione	Y
3	Delitti informatici e trattamento illecito di dati	Y
4	Delitti di criminalità organizzata	Y
5	Reati in tema di falsità in moneta, carte di pubblico credito, valori di bollo e strumenti o segni di riconoscimento	Y
6	Delitti contro l'industria e il commercio	N/A
7	Reati societari	Y
10	Delitti contro la personalità individuale	N/A
13	Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro	N/A
14	Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio	Y
15	Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori	Y
16	Altre fattispecie in materia di strumenti di pagamento diversi dai contanti	N/A
17	Delitti in materia di violazione del diritto d'autore	N/A
18	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	N/A
19	Reati ambientali	Y
20	Impiego di cittadini di paesi terzi il cui soggiorno è irregolare	Y
21	Razzismo e xenofobia	N/A

Ciclo Amministrazione – Risk Control Matrix

CICLO AZIENDALE:	Amministrazione

RISK CONTROL MATRIX

SEZIONE PRIMA: Comportamenti non conformi al Codice Etico aziendale

VIOLAZIONE	DESCRIZIONE PRINCIPIO DI RIFERIMENTO	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Rispetto Privacy	*trattamento di dati personali e dati sensibili nel rispetto della normativa vigente.*	Diffusione non autorizzata dei dati al di fuori dell'ufficio.	**0,1**	**0,2**	Accettabile	Tutte le figure operanti nel ciclo.
Rispetto Privacy	*trattamento di dati personali e dati sensibili nel rispetto della normativa vigente.*	Archiviazione di dati in modo tale da consentire l'accesso anche da parte di persone non autorizzate.	**0,35**	**0,2**	Accettabile	Tutte le figure operanti nel ciclo.
Rispetto SGQ	*svolgimento delle attività regolamentate dal Sistema di Gestione della Qualità, adottato dall'azienda, nel pieno rispetto della politica per la Qualità aziendale, delle relative procedure e delle eventuali istruzioni operative applicabili.*	Non rispetto/ritardi degli adempimenti previsti dall'iter procedurale (con disallinaementi tra quanto effettivamente svolto e quanto formalizzato).	**0,4**	**0,2**	Accettabile	Tutte le figure operanti nell'Ente
Rispetto SGQ	*svolgimento delle attività regolamentate dal Sistema di Gestione della Qualità, adottato dall'azienda, nel pieno rispetto della politica per la Qualità aziendale, delle relative procedure e delle eventuali istruzioni operative applicabili.*	Non idoneità/non conformità rilevate in modo scorretto o intempestivo.	**0,2**	**0,05**	Accettabile	Tutte le figure operanti nel ciclo.

CICLO AZIENDALE:	Amministrazione

RISK CONTROL MATRIX

SEZIONE SECONDA: Reati in danno alla Pubblica Amministrazione

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Frode informatica	*Art. 640-ter c.p.*	Inserimento di dati alterati per ottenere finanziamenti più alti.	**0,3**	**0,3**	Rilevante	Resp. Amm.vo e Referente ufficio acquisti/magazzino/mautenzione
Frode informatica	*Art. 640-ter c.p.*	Potenziale alterazione del funzionamento di un sistema informatico o telematico della pubblica amministrazione, o potenziale accesso (senza averne diritto o formale autorizzazione) a dati, informazioni, programmi informatici o telematici al fine di ottenere finanziamenti più alti.	**0,3**	**0,3**	Rilevante	Resp. Amm.vo e Referente ufficio acquisti/magazzino/mautenzione
Truffa in danno dello Stato o di altro ente pubblico	*Art. 640, co. 2, n. 1, c.p.*	In tema di gestione delle risorse umane, alterazione della documentazione da fornire alla Pubblica Amministrazione all'atto del pagamento dei contributi, procurando per sé o altri un ingiusto profitto con altrui danno.	**0,3**	**0,3**	Rilevante	Resp. Amm.vo e Responsabile Risorse Umane
Truffa in danno dello Stato o di altro ente pubblico	*Art. 640, co. 2, n. 1, c.p.*	Si commette il reato di truffa in danno dello Stato o di altro ente pubblico e malversazione di erogazioni pubbliche nel momento in cui, in fase di rendicontazione delle attività svolte, il responsabile amministrativo dichiara il falso, modificando fraudolentemente i dati del corso di formazione, procurando per sé o altri un ingiusto profitto con altrui danno. A seguito della commissione dei precedente reato, l'Ente ottiene una indebita percezione di erogazioni a danno dello Stato.	**0,3**	**0,3**	Rilevante	Resp. Amm.vo, Referente ufficio acquisti/magazzino/mautenzione, Vice-Direttore ed eventualmente i Responsabili d'area in relazione al progetto/corso da rendicontare

Corruzione (varie forme)	*Artt. 317, 318, 319-bis, 319-quater, 320, 321, 322 c.p.*	Nella fase di valutazione e selezione del personale se si accetta di assumere un candidato segnalato da un pubblico ufficiale come favore per aver svolto il suo lavoro evitando di arrecare danno all'Ente o come ricompensa per aver omesso o ritardato un atto del suo ufficio. Il reato di induzione indebita a dare o promettere utilità si potrebbe configurare qualora il pubblico ufficiale o l'incaricato di pubblico servizio effettui pressioni su un esponente di AFOL Como, al fine di indurlo a selezionare docenti suoi parenti o congiunti, senza basarsi su criteri oggettivi e di merito) in cambio della non segnalazione di irregolarità (di carattere contributivo, previdenziale e assistenziale) realizzate da AFOL Como stessa. Qualora l'esponente dell'Ente cedesse alle pressioni del pubblico ufficiale/incaricato di pubblico servizio, per favorire l'Ente stesso, si ravviserebbe la fattispecie di reato ex art. 319-quater c.p.	**0,3**	**0,3**	Rilevante	Resp. Amm.vo e Responsabile Risorse Umane
Corruzione (varie forme)	*Artt. 317, 318, 319-bis, 319-quater, 320, 321, 322 c.p.*	La fattispecie di reato rappresentata dalla "concussione" può essere commessa se durante una verifica ispettiva da parte di pubblici funzionari, il referente interno di AFOL Como che ha il compito di interfacciarsi con il pubblico ufficiale accetta di sottostare alle richieste sia dirette che indirette dello stesso per non arrecare un danno all'Ente. Le fattispecie di "corruzione", invece, rappresentano il delitto commesso dal pubblico ufficiale che, per compiere un atto del suo ufficio, o per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, in denaro od altra utilità, una retribuzione che non gli è dovuta, o ne accetta la promessa. Gli accordi fraudolenti alla corruzione di pubblici ufficiali e/o incaricati di pubblico	**0,3**	**0,3**	Rilevante	Resp. Amm.vo, Amministratore Unico, Direttore, Vice-Direttore
Corruzione (varie forme)	*Artt. 317, 318, 319-bis, 319-quater, 320, 321, 322 c.p.*	L'Ente potrebbe procedere con il pagamento: - a favore di parenti o amici del Pubblico Funzionario/incaricato di pubblico servizio; - di fatture di fornitori indicati dal Pubblico Funzionario/incaricato di pubblico servizio, a fronte di servizi anche non necessari o mai erogati. Sono da considerare a rischio anche la stipula ed esecuzione di contratti di acquisto con soggetti privati che, pur non comportando contatti o rapporti diretti con la Pubblica Amministrazione, potrebbero assumere carattere strumentale e/o	**0,3**	**0,3**	Rilevante	Resp. Amm.vo, Direttore (Vice-Direttore), Referente forniture acquisti magazzino - Mannutenzione
Corruzione (varie forme)	*Artt. 317, 318, 319-bis, 319-quater, 320, 321, 322 c.p.*	La gestione delle risorse finanziarie (in ingresso e in uscita) rappresenta un'area a rischio "strumentale" in relazione ai reati contro la Pubblica Amministrazione nel cui ambito, in linea di principio, potrebbero crearsi le condizioni per commettere tali reati (es.: pagamenti finalizzati ad ottenere illeciti vantaggi in atti d'ufficio, trasferimento di risorse finanziarie a fronte di fatture sovrastimate o false, ricorso	**0,3**	**0,3**	Rilevante	Resp. Amm.vo, Amministratore Unico, Direttore (Vice-Direttore)

CICLO AZIENDALE:	Amministrazione
RISK CONTROL MATRIX	

SEZIONE TERZA - Delitti informatici e trattamento illecito di dati

RISCHIO REATO	***RIFERIMENTI NORMATIVI***	***CONDOTTA ERRATA***	***PROBABILITA***	***IMPATTO***	***VALUTAZIONE***	***FUNZIONI COINVOLTE***
Accesso abusivo a sistema informatico e danneggiamento di informazioni, dati, programmi e sistemi informatici, anche dello Stato o altro ente pubblico o comunque di pubblico interesse	*Art. 615-ter, 615-quater, 629, co. 3, 635-bis, 635-ter, 635-quater, 635-quater.1 c.p.*	Accesso di utenti non autorizzati a sistemi aziendali protetti da misure di sicurezza (es.: sistemi interbancari). Utilizzo abusivo di password di accesso a siti di soggetti terzi, pubblici o privati, al fine di acquisire informazioni riservate e conseguire vantaggi competitivi. Accesso a una postazione PC, a sistemi di gestione aziendali, a sistemi telematici (anche della Pubblica amministrazione) con password diverse dalle proprie o senza autorizzazione specifica, con codici di accesso ottenuti violando le regole stabilite dalle policy e procedure aziendali. Detenzione abusiva di codici di accesso a sistemi informatici dell'Amministrazione giudiziaria o finanziaria, al fine di acquisire informazioni riservate su procedimenti penali/amministrativi che coinvolgano la Società. Manomissione del sistema di sorveglianza interno al fine di cancellare le registrazioni di un incidente avvenuto ai danni di un lavoratore memorizzate sul dispositivo. Assenza o inadeguatezza di un sistema di protezione dei dati e di un costante monitoraggio dei dati all'interno della rete.	**0,3**	**0,3**	Rilevante	Direttore, Resp. Amm.vo e Referente ufficio acquisti/magazzino/mautenzione

CICLO AZIENDALE:	Amministrazione
RISK CONTROL MATRIX	

SEZIONE QUARTA: Delitti di criminalità organizzata

RISCHIO REATO	***RIFERIMENTI NORMATIVI***	***CONDOTTA ERRATA***	***PROBABILITA***	***IMPATTO***	***VALUTAZIONE***	***FUNZIONI COINVOLTE***
Associazione per delinquere (anche di tipo mafioso)	*Artt. 416 c.p. (ad eccezione del sesto comma), 416-bis c.p.*	I reati associativi, essendo per definizione costituiti dall'accordo volto alla commissione di qualunque delitto, estendono il novero dei reati presupposto ad un numero indeterminato di figure criminose, per cui qualsiasi attività svolta dall'Ente potrebbe potenzialmente comportare la commissione di un delitto - e la conseguente responsabilità ex d.lgs. 231/01 - "tramite" un'associazione per delinquere. Nello specifoc, l'Ente potrebbe instaurare, nell'ambito dei processi di acquisto (scelta del fornitore/consuelnte) e di selezione del personale, rapporti con soggetti di dubbia onorabilità.	**0,3**	**0,3**	Rilevante	Resp. Amm.vo e Responsabile Risorse Umane, Amministratore Unico, Direttore e Vice-Direttore

CICLO AZIENDALE: Amministrazione

RISK CONTROL MATRIX

SEZIONE QUINTA: Reati in tema di falsità in moneta, carte di pubblico credito, valori di bollo e strumenti o segni di riconoscimento

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Spendita e introduzione nello Stato di monete falsificate anche ricevute in buona fede	*Art. 453 co. 1 n. 3 c.p.* *Art. 455 c.p.* *Art. 457 c.p.*	Ricevimento di pagamenti con denaro falsificato non identificato e utilizzato.	**0,05**	**0,2**	Accettabile	Direttore e Ufficio Amministrativo

CICLO AZIENDALE: Amministrazione

RISK CONTROL MATRIX

SEZIONE SETTIMA: Reati Societari

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Ostacolo all'esercizio delle attività di controllo, revisione e delle funzioni delle autorità pubbliche di vigilanza	*Art. 2625 comma 2 c.c.* *Art. 2638 comma 1 e 2 c.c.*	Fornire documenti alterati	**0,3**	**0,5**	Rilevante	Ufficio Amministrativo
Reati di c.d. falso in bilancio	*Art. 2621 c.c.* *Art. 2621 bis c.c.* *Art. 2632 c.c.* *Art. 2626 c.c.* *Art. 2627 c.c.* *Art. 2636 c.c.* *Art. 2629 c.c.*	I reati di cui agli artt. 2621 c.c., 2621-bis c.c., 2632 c.c., 2626 c.c., 2627 c.c. possono essere commessi se gli operatori amministrativi o i dirigenti, nonché i collaboratori e consulenti di AFOL Como, durante la formazione del bilancio, redazione dei documenti contabili societari, relazioni o altre comunicazioni sociali, espongono fatti materiali non corrispondenti al vero o omettono informazioni imposte dalla legge sulla situazione economica, patrimoniale o finanziaria dell'Ente in modo da indurre in errore i destinatari, ovvero effettuano operazioni sul capitale in violazione delle disposizioni di legge previste in materia. Il reato di illecita influenza sull'assemblea si potrebbe realizzare qualora l'amministratore rappresentasse alle parti sociali prospettive improbabili nella loro attualità, allo scopo di ottenere dei voti per una rielezione o per la realizzazione di operazioni straordinarie. Il reato di operazioni in pregiudizio dei creditori si potrebbe consumare allorché i creditori dell'Ente subiscano un danno a causa di riduzioni del capitale o di operazioni straordinarie effettuate in violazione delle disposizioni di legge.	**0,3**	**0,3**	Rilevante	Resp. Amm.vo e Direttore
Reati di c.d. falso in bilancio	*Art. 2621 c.c.* *Art. 2621 bis c.c.*	I reati di cui agli artt. 2621 c.c. e 2621-bis c.c. possono essere commessi nell'ambito della gestione dei flussi finanziari (in entrata e in uscita) nel momento in cui tali movimentazioni si riflettono in un bilancio che espone fatti non corrispondenti al vero e pertanto una situazione economica, patrimoniale o finanziaria tale da indurre in errore i destinatari del bilancio stesso.	**0,3**	**0,3**	Rilevante	Resp. Amm.vo, Direttore e Amministratore Unico
Corruzione tra privati	*Art. 2635 c.c.* *Art. 2635-bis c.c.*	La gestione degli incassi e pagamenti è processo trasversale nel compimento dei reati di cui agli artt. 2635 e 2635-bis c.c. nelle ipotesi in cui la corruzione (potenzialmente realizzabile nei processi nel seguito esaminati) avvenga mediante utilizzo di denaro.	**0,3**	**0,3**	Rilevante	Resp. Amm.vo, Direttore e Amministratore Unico
Corruzione tra privati	*Art. 2635 c.c.* *Art. 2635-bis c.c.*	Il reato di cui all'art. 2625 c.c. potrebbe verificarsi mediante azioni (indisponibilità agli appuntamenti, ritardo o mancata consegna della documentazione richiesta) od omissioni (di informazioni, dati, documenti) che impediscono di fatto lo svolgimento dei controlli delle parti sociali e degli organi di controllo (Collegio Sindacale, Società di revisione).	**0,3**	**0,3**	Rilevante	Resp. Amm.vo e Direttore
Corruzione tra privati	*Art. 2635 c.c.* *Art. 2635-bis c.c.*	I reati relativi agli artt. 2635 c.c. e 2635-bis c.c. possono essere commessi se gli operatori amministrativi o i dirigenti, durante il processo di qualifica e monitoraggio dei fornitori, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per qualificare/mantenere qualificato un fornitore privo dei requisiti necessari o più in generale per favoritismi a fornitori specifici. Tali reati potrebbero altresì essere commessi qualora venisse offerto, agli esponenti di AFOL Como competenti nell'ambito della selezione di docenti per i corsi di formazione, denaro o altra utilità al fine di selezionare collaboratori senza basarsi su criteri oggettivi predefiniti e quindi in contrasto con le procedure operative interne.	**0,3**	**0,3**	Rilevante	Resp. Amm.vo e Direttore (Vice-Direttore), Referente forniture acquisti magazzino manutenzione
Corruzione tra privati	*Art. 2635 c.c.* *Art. 2635-bis c.c.*	I reati di cui agli artt. 2635 e 2635-bis c.c. potrebbero verificarsi qualora venisse offerto, agli esponenti di AFOL Como che operano nell'ambito dell'assunzione del personale, denaro o altra utilità al fine di selezionare dipendenti senza basarsi su criteri oggettivi predefiniti e quindi in contrasto con le procedure operative interne.	**0,3**	**0,3**	Rilevante	Resp. Amm.vo e Resp. Risorse Umane

CICLO AZIENDALE: Amministrazione

RISK CONTROL MATRIX

SEZIONE DECIMA: Delitti contro la personalità individuale

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Intermediazione illecita e sfruttamento del lavoro	*Art. 603-bis c.p.*	Il reato di cui all'art. 603-bis c.p. può essere astrattamente commesso qualora i referenti di AFOL Como competenti nell'ambito dell'assunzione e gestione del personale agiscano nel mancato rispetto della normativa prevista in materia, nonché delle procedure operative interne.	**0,3**	**0,3**	Rilevante	Direttore, Amministratore Unico, Resp. Ammv.vo, Resp. Risorse Umane

CICLO AZIENDALE:	Amministrazione					
RISK CONTROL MATRIX						
SEZIONE QUATTORDICESIMA: Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio						
RISCHIO REATO	**RIFERIMENTI NORMATIVI**	**CONDOTTA ERRATA**	**PROBABILITA**	**IMPATTO**	**VALUTAZIONE**	**FUNZIONI COINVOLTE**
Ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio	*Art. 648, 648-bis, 648-ter, 648-ter.1 c.p.*	I reati richiamati dall'art. 25-octies del Decreto possono essere commessi se la provvista illecita venisse costituita in capo all'Ente attraverso, ad esempio, la commissione di un delitto economico di riserve occulte o di fondi neri.	**0,3**	**0,3**	Rilevante	Resp. Amm.vo e Direttore
Ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio	*Art. 648, 648-bis, 648-ter, 648-ter.1 c.p.*	I reati richiamati dall'art. 25-octies del Decreto potrebbero essere potenzialmente commessi accettando incassi od effettuando pagamenti in contanti o con modalità al di fuori di quanto previsto dalla legge, dalle regole interne e dalle procedure di controllo adottate dall'Ente.	**0,3**	**0,3**	Rilevante	Resp. Amm.vo, Direttore e Amministratore Unico
Ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio	*Art. 648, 648-bis, 648-ter, 648-ter.1 c.p.*	I reati richiamati dall'art. 25-octies del Decreto possono essere potenzialmente commessi nelle ipotesi in cui l'Ente omettesse la verifica in merito all'attendibilità commerciale e professionale dei fornitori o non si allertasse in occasione di particolari indicatori di anomalia, quali: reticenza del fornitore a fornire documenti identificativi, comportamenti sospetti della controparte, etc.	**0,3**	**0,3**	Rilevante	Resp. Amm.vo e Direttore (Vice-Direttore), Referente forniture acquisti magazzino manutenzione
Ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio	*Art. 648, 648-bis, 648-ter, 648-ter.1 c.p.*	I reati richiamati dall'art. 25-octies del Decreto potrebbero essere potenzialmente commessi mediante il pagamento di premi ai dipendenti (in contanti o con modalità difformi rispetto a quanto previsto dalla legge, dalle regole e dalle procedure di controllo interne) al fine di riciclare denaro proveniente da attività illecite, commesse dagli esponenti dell'Ente o da terzi.	**0,3**	**0,3**	Rilevante	Resp. Amm.vo e Resp. Risorse Umane

CICLO AZIENDALE:	Amministrazione					
RISK CONTROL MATRIX						
SEZIONE QUINDICESIMA: Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori						
RISCHIO REATO	**RIFERIMENTI NORMATIVI**	**CONDOTTA ERRATA**	**PROBABILITA**	**IMPATTO**	**VALUTAZIONE**	**FUNZIONI COINVOLTE**
Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento	*Art. 493-ter, 493-quater, 515-bis, 640-ter c.p.*	I reati in oggetto potrebbero essere potenzialmente commessi mediante utilizzo indebito, falsificazione o alterazione di carte di credito o di pagamento per l'acquisto di beni o servizi.	**0,3**	**0,3**	Rilevante	Resp. Amm.vo e Direttore (Vice-Direttore), Amministratore Unico, Referente forniture acquisti magazzino manutenzione

CICLO AZIENDALE:	Amministrazione					
RISK CONTROL MATRIX						
SEZIONE DICIANNOVESIMA: Reati ambientali						
RISCHIO REATO	**RIFERIMENTI NORMATIVI**	**CONDOTTA ERRATA**	**PROBABILITA**	**IMPATTO**	**VALUTAZIONE**	**FUNZIONI COINVOLTE**
Inquinamento ambientale e delitti colposi contro l'ambiente	*Art. 452-bis, 452-quinquies c.p.*	Scorretto smaltimento dei toner delle stampanti esauriti	**0,1**	**0,7**	Accettabile	Resp. Amm.vo; Referente forniture acquisti magazzino manutenzione

CICLO AZIENDALE:	Amministrazione					
RISK CONTROL MATRIX						
SEZIONE VENTESTIMA: Impiego di cittadini di paesi terzi con permesso di soggiorno irregolare						
RISCHIO REATO	**RIFERIMENTI NORMATIVI**	**CONDOTTA ERRATA**	**PROBABILITA**	**IMPATTO**	**VALUTAZIONE**	**FUNZIONI COINVOLTE**
Disposizioni contro le immigrazioni clandestine e Impiego di dittadini di paesi terzi il cui soggiorno è irregolare	*Art. 22, comma 12-bis, D.lgs. n. 286/1998 Art. 12 commi 3, 3-bis, 3-ter e 5 D.lgs. n. 286/1998*	I reati di cui all'art. 22, c. 12-bis e all'art. 12, c. 3, 3-bis, 3-ter e 5 D.lgs. 286/1998, possono essere commessi se il datore di lavoro occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, ovvero il cui permesso sia scaduto, revocato o annullato.	**0,3**	**0,3**	Rilevante	Direttore, Amministratore Unico, Resp. Ammv.vo, Resp. Risorse Umane

QUASER CERTIFICAZIONI S.R.L.
UNI EN ISO 9001:2015
(EA 37, 38)
AGENZIA PER LA FORMAZIONE, L'ORIENTAMENTO E IL LAVORO DELLA PROVINCIA DI COMO
CENTRO DI FORMAZIONE PROFESSIONALE
dedicato a "Luigi Grisoni"
COMO Monteolimpino via Bellinzona, 88 tel. 031/571055 - 574000 fax 575047
C.F. 95092770130 P.Iva 03095420133 e-mail: info@cfpcomo.com www.cfpcomo.com

Centro Formazione Professionale CFP COMO

CICLO AZIENDALE:	AMMINISTRAZIONE				
Rischio	**Descrizione Rischio**	**Descrizione GAP**	**Priorità**	**Funzioni coinvolte**	**Action Plan**
Rispetto Privacy	Diffusione non autorizzata dei dati al di fuori dell'ufficio. Archiviazione di dati in modo tale da consentire l'accesso anche da parte di persone non autorizzate.	Modalità di archiviazione non ottimali a presidiare il rischio individuato.	Bassa	Tutte le figure operanti nel ciclo.	**Chiusura a chiave degli armadi dove sono archiviati dati personali e/o sensibili di qualsiasi natura (utenti, dipendenti, candidati,...).** **Il sistema della tutela dell'Ente sulla Privacy (adottato dall'Ente in seguito alla normativa Europea - GDPR) migliora ulteriormente questo GAP**
Rispetto SGQ	Non rispetto/ritardi degli adempimenti previsti dall'iter procedurale (con disallinaementi tra quanto effettivamente svolto e quanto formalizzato). Non idoneità/non conformità rilevate in modo scorretto o intempestivo.	Il SGQ adottato risulta poco interiorizzato dagli operatori.	Media	Tutte le figure operanti nel ciclo. Tutte le figure operanti nel ciclo.	**Svolte diversi seminari a partire dal 2010 sulla sensibilizzazione sulle Procedure, raccogliendo feedback operativi da parte di chi è chiamato ad applicare il SGQ. Sulla base di tali feedback andranno valutate eventuali revisioni future.** **Sensibilizzazione di tutti gli operatori coinvolti sull'importanza della tempestiva segnalazione di inidoneità e Non Conformità di qualsiasi livello.**
Frode Informatica	Accessi non autorizzati al sistema informatico.	I sistemi di controllo applicati in passato non risultavano pienamente idonei a prevenire il rischio individuato.	Media	Tutte le figure operanti nel ciclo.	**Formalizzazione di un contratto di mantuenzione hardware/software con assistenza continuativa e monitoraggio dei presidi di sicurezza informatica. Utilizzo Sistema Informativo interno:** **prevista la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password).** **SI regionali/provinciali: identificate e comunicate responsabilità in capo a chi opera coi SI regionali e provinciali. Laddove possibile richiedere e fornire possibilità di accesso a detti sistemi con differenti profilazioni a seconda delle attività da svolgere.** **Previsto inoltre un controllo da parte di un adeguato livello aziendale sulle attività svolte dall'utente (monitoraggio dei login e dei dati inseriti).**
Truffa in danno dello Stato o di altro ente pubblico	In tema di gestione delle risorse umane, alterazione della documentazione da fornire alla Pubblica Amministrazione all'atto del pagamento dei contributi, procurando per sé o altri un ingiusto profitto con altrui danno. Si commette il reato di truffa in danno dello Stato o di altro ente pubblico e malversazione di erogazioni pubbliche nel momento in cui, in fase di rendicontazione delle attività svolte, il responsabile amministrativo dichiara il falso, modificando fraudolentemente i dati del corso di formazione, procurando per sé o altri un ingiusto profitto con altrui danno.	Possibilità di alterazione dei dati dei registri utilizzati nei rapporti con la PA (registri scolastici, rendicontazione finanziamenti, selezione, appalti, ecc.)	Media	Resp. Amm.vo e Responsabile Risorse Umane Resp. Amm.vo, Referente ufficio acquisti/magazzino/manutenzione, Vice-Direttore ed eventualmente i Responsabili d'area in relazione al progetto/corso da rendicontare	**Utilizzo Sistema Informativo interno: prevista la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password).** **SI regionali/provinciali: identificate e comunicate responsabilità in capo a chi opera coi SI regionali e provinciali. Laddove possibile richiedere e fornire possibilità di accesso a detti sistemi con differenti profilazioni a seconda delle attività da svolgere.** **Previsto inoltre un controllo da parte di un adeguato livello aziendale sulle attività svolte dall'utente (monitoraggio dei login e dei dati inseriti).**

Corruzione (varie forme)	Nella fase di valutazione e selezione del personale se si accetta di assumere un candidato segnalato da un pubblico ufficiale come favore per aver svolto il suo lavoro evitando di arrecare danno all'Ente o come ricompensa per aver omesso o ritardato un atto del suo ufficio. Il reato di induzione indebita a dare o promettere utilità si potrebbe configurare qualora il pubblico ufficiale o l'incaricato di pubblico servizio effettui pressioni su un esponente di AFOL Como, al fine di indurlo a selezionare docenti suoi parenti o congiunti, senza basarsi su criteri oggettivi e di merito) in cambio della non segnalazione di irregolarità (di carattere contributivo, previdenziale e assistenziale) realizzate da AFOL Como stessa. Qualora l'esponente dell'Ente cedesse alle pressioni del pubblico ufficiale/incaricato di pubblico servizio, per favorire	Possibilità di comportamenti illeciti personali	Media	Tutte le figure operanti nel ciclo.	**Precipua diffusione ed attuazione del Piano Triennale di Prevenzione della Corruzione e Trasparenza** **Formazione permanente** **Istituzione di Commissioni di Gara che sottraggano le decisioni al singolo**
	La fattispecie di reato rappresentata dalla "concussione" può essere commessa se durante una verifica ispettiva da parte di pubblici funzionari, il referente interno di AFOL Como che ha il compito di interfacciarsi con il pubblico ufficiale accetta di sottostare alle richieste sia dirette che indirette dello stesso per non arrecare un danno all'Ente. Le fattispecie di "corruzione", invece, rappresentano il delitto commesso dal pubblico ufficiale che, per compiere un atto del suo ufficio, o per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, in denaro od altra utilità, una retribuzione che non gli è dovuta, o ne accetta la promessa. Gli accordi funzionali alla corruzione di pubblici ufficiali e/o incaricati di pubblico servizio, prodromici alla corruzione			Tutte le figure operanti nel ciclo.	
	L'Ente potrebbe procedere con il pagamento: - a favore di parenti o amici del Pubblico Funzionario/incaricato di pubblico servizio; - di fatture di fornitori indicati dal Pubblico Funzionario/incaricato di pubblico servizio, a fronte di servizi anche non necessari o mai erogati. Sono da considerare a rischio anche la stipula ed esecuzione di contratti di acquisto con soggetti privati che, pur non comportando contatti o rapporti diretti con la Pubblica Amministrazione, potrebbero assumere carattere strumentale e/o di supporto ai fini della commissione dei reati di corruzione e di induzione indebita a dare o promettere utilità, in quanto strumentali alla creazione di una "provvista" da impiegarsi per			Tutte le figure operanti nel ciclo.	
	La gestione delle risorse finanziarie (in ingresso e in uscita) rappresenta un'area a rischio "strumentale" in relazione ai reati contro la Pubblica Amministrazione nel cui ambito, in linea di principio, potrebbero crearsi le condizioni per commettere tali reati (es.: pagamenti finalizzati ad ottenere illeciti vantaggi in atti d'ufficio, trasferimento di risorse finanziarie a fronte di fatture sovrastimate o false, ricorso sistematico a mezzi di pagamento non conformi alle modalità previste da policy interne).			Tutte le figure operanti nel ciclo.	

Associazione per delinquere (anche di tipo mafioso)	I reati associativi, essendo per definizione costituiti dall'accordo volto alla commissione di qualunque delitto, estendono il novero dei reati presupposto ad un numero indeterminato di figure criminose, per cui qualsiasi attività svolta dall'Ente potrebbe potenzialmente comportare la commissione di un delitto - e la conseguente responsabilità ex d.lgs. 231/01 - "tramite" un'associazione per delinquere. Nello specifoc, l'Ente potrebbe instaurare, nell'ambito dei processi di acquisto (scelta del fornitore/consuelnte) e di selezione del personale, rapporti con soggetti di dubbia onorabilità.	Possibilità di comportamenti illeciti personali	Media	Resp. Amm.vo e Responsabile Risorse Umane, Amministratore Unico, Direttore e Vice-Direttore	
Spendita denaro falso ricevuto in buona fede	Ricevimento di denaro contante non verificato presso il bar aziendale.	I sistemi di controllo applicati in passato non risultavano pienamente idonei a prevenire il rischio individuato.	Bassa (accettabile in seguito ad intervento)	Direttore e Ufficio Amministrativo	**Fornito alle aree interessate da movimenti in contanti (ad es. bar e uff. amministrazione) un rilevatore di banconote false.**
Ostacolo all'esercizio delle attività di controllo, revisione e delle funzioni delle autorità pubbliche di vigilanza	Fornire dati alterati	I sistemi di controllo sulla corretta tenuta della documentazione a supporto delle attività svolte non prevengono pienamente il rischio individuato.	Medio-Alta	Ufficio Amministrativo	**Formalizzazione all'interno del proprio SGQ di un'apposita procedura riguardante la Rendicontazione dei progetti finanziati.** **Sensibilizzazione dei docenti circa l'importanza della rendicontazione e del ruolo che ha la corretta e puntuale tenuta dei documenti a supporto.** **Prevista a conclusione delle attività (in particolare per quelle legate a progetti finanziati) una check list di verifica della relativa documentazione (effettuando un controllo sulla presenza del documento e un controllo sulla completezza/corretta tenuta del documento). Tale controllo potrà essere effettuato dalla Segreteria didattica in coordinamento con amministrazione e responsabili di area.** **A seguito del controllo la documentazione non dovrà più essere liberamente accessibile agli operatori.**
Reati di c.d. falso in bilancio	I reati di cui agli artt. 2621 c.c., 2621-bis c.c., 2632 c.c., 2626 c.c., 2627 c.c. possono essere commessi se gli operatori amministrativi o i dirigenti, nonché i collaboratori e consulenti di AFOL Como, durante la formazione del bilancio, redazione dei documenti contabili societari, relazioni o altre comunicazioni sociali, espongono fatti materiali non corrispondenti al vero o omettono informazioni imposte dalla legge sulla situazione economica, patrimoniale o finanziaria dell'Ente in modo da indurre in errore i destinatari, ovvero effettuano operazioni sul capitale in violazione delle disposizioni di legge previste in materia. Il reato di illecita influenza sull'assemblea si potrebbe realizzare qualora l'amministratore rappresentasse alle parti sociali prospettive improbabili nella loro attualità, allo scopo di ottenere dei voti per una rielezione o per la	Inserimento in bilancio di dati non veritieri	Bassa	Resp. Amm.vo e Direttore	**Il processo di formazione del bilancio deve essere condiviso tra i soggetti preposti (Amministrazione, Direttore, Commercialista Esterno, Revisore)**
	I reati di cui agli artt. 2621 c.c. e 2621-bis c.c. possono essere commessi nell'ambito della gestione dei flussi finanziari (in entrata e in uscita) nel momento in cui tali movimentazioni si riflettono in un bilancio che espone fatti non corrispondenti al vero e pertanto una situazione economica, patrimoniale o finanziaria tale da indurre in errore i destinatari del bilancio stesso.	Rappresentazione in bilancio di fatti non veritieri		Resp. Amm.vo, Direttore e Amministratore Unico	**Il processo di formazione del bilancio deve essere condiviso tra i soggetti preposti (Amministrazione, Direttore, Commercialista Esterno, Revisore)**

	La gestione degli incassi e pagamenti è processo trasversale nel compimento dei reati di cui agli artt. 2635 e 2635-bis c.c. nelle ipotesi in cui la corruzione (potenzialmente realizzabile nei processi nel seguito esaminati) avvenga mediante utilizzo di denaro.	Possibilità di pagamenti indebiti	Media	Resp. Amm.vo, Direttore e Amministratore Unico	**I pagamenti devono avvenire a firma congiunta**
	Il reato di cui all'art. 2625 c.c. potrebbe verificarsi mediante azioni (indisponibilità agli appuntamenti, ritardo o mancata consegna della documentazione richiesta) od omissioni (di informazioni, dati, documenti) che impediscono di fatto lo svolgimento dei controlli delle parti sociali e degli organi di controllo (Collegio Sindacale, Società di revisione).	Azioni personali di interferenza	Media	Tutte le figure operanti nel ciclo.	**Diffusione del PTCPT e massima condivisione del processo decisionale**
Corruzione tra privati	I reati relativi agli artt. 2635 c.c. e 2635-bis c.c. possono essere commessi se gli operatori amministrativi o i dirigenti, durante il processo di qualifica e monitoraggio dei fornitori, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per qualificare/mantenere qualificato un fornitore privo dei requisiti necessari o più in generale per favoritismi a fornitori specifici. Tali reati potrebbero altresì essere commessi qualora venisse offerto, agli esponenti di AFOL Como competenti nell'ambito della selezione di docenti per i corsi di formazione, denaro o altra utilità al fine di selezionare collaboratori senza basarsi su criteri oggettivi predefiniti e quindi in contrasto con le procedure operative interne.	Comportamenti illeciti personali	Media	Resp. Amm.vo e Direttore (Vice-Direttore), Referente forniture acquisti magazzino manutenzione	**Diffusione del PTCPT e massima condivisione del processo decisionale**
	I reati di cui agli artt. 2635 e 2635-bis c.c. potrebbero verificarsi qualora venisse offerto, agli esponenti di AFOL Como che operano nell'ambito dell'assunzione del personale, denaro o altra utilità al fine di selezionare dipendenti senza basarsi su criteri oggettivi predefiniti e quindi in contrasto con le procedure operative interne.	Comportamenti illeciti personali	Media	Resp. Amm.vo e Resp. Risorse Umane	**Diffusione del PTCPT e massima condivisione del processo decisionale**
Intermediazione illecita e sfruttamento del lavoro	Il reato di cui all'art. 603-bis c.p. può essere astrattamente commesso qualora i referenti di AFOL Como competenti nell'ambito dell'assunzione e gestione del personale agiscano nel mancato rispetto della normativa prevista in materia, nonché delle procedure operative interne.	Possibilità di utilizzo di manodopera non in regola	Bassa	Direttore, Amministratore Unico, Resp. Ammv.vo, Resp. Risorse Umane	**Contrattualizzazione di tutte le figure operanti in AFOL.**

	I reati richiamati dall'art. 25-octies del Decreto possono essere commessi se la provvista illecita venisse costituita in capo all'Ente attraverso, ad esempio, la commissione di un delitto economico di riserve occulte o di fondi neri.	Possibilità di costituzione di riserve occulte in bilancio	Bassa	Resp. Amm.vo e Direttore	**Il processo di formazione del bilancio deve essere condiviso tra i soggetti preposti (Amministrazione, Direttore, Commercialista Esterno, Revisore)**
Ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio	I reati richiamati dall'art. 25-octies del Decreto potrebbero essere potenzialmente commessi accettando incassi od effettuando pagamenti in contanti o con modalità al di fuori di quanto previsto dalla legge, dalle regole interne e dalle procedure di controllo adottate dall'Ente.	Possibilità di pagamenti indebiti in contanti	Bassa	Resp. Amm.vo, Direttore e Amministratore Unico	**Controllo della gestione in contanti dell'attività del bar, rendicontazione, versamento senza dilazioni delle somme in c/c bancario**
	I reati richiamati dall'art. 25-octies del Decreto possono essere potenzialmente commessi nelle ipotesi in cui l'Ente omettesse la verifica in merito all'attendibilità commerciale e professionale dei fornitori o non si allertasse in occasione di particolari indicatori di anomalia, quali: reticenza del fornitore a fornire documenti identificativi, comportamenti sospetti della controparte, etc.	Possibilità di operare con soggetti a rischio	Media	Resp. Amm.vo e Direttore (Vice-Direttore), Referente forniture acquisti magazzino manutenzione	**Selezione e aggiornamento della Lista Fornitori**
	I reati richiamati dall'art. 25-octies del Decreto potrebbero essere potenzialmente commessi mediante il pagamento di premi ai dipendenti (in contanti o con modalità difformi rispetto a quanto previsto dalla legge, dalle regole e dalle procedure di controllo interne) al fine di riciclare denaro proveniente da attività illecite, commesse dagli esponenti dell'Ente o da terzi.	Possibilità di pagamenti indebiti in contanti	Bassa	Resp. Amm.vo e Resp. Risorse Umane	**Controllo della gestione in contanti dell'attività del bar, rendicontazione, versamento senza dilazioni delle somme in c/c bancario**
Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento	I reati in oggetto potrebbero essere potenzialmente commessi mediante utilizzo indebito, falsificazione o alterazione di carte di credito o di pagamento per l'acquisto di beni o servizi.	Possibilità di utilizzo personale di carte aziendali	Bassa	Resp. Amm.vo e Direttore (Vice-Direttore), Amministratore Unico, Referente forniture acquisti magazzino manutenzione	**Prevedere che i pagamenti, anche di entità modesta, vengano effettuati a mezzo bonifico a seguito di autorizzazione del Direttore.**
Inquinamento ambientale e delitti colposi contro l'ambiente	Scorretto smaltimento dei toner delle stampanti esauriti	Possibilità di un illecito smaltimento	Bassa	Resp. Amm.vo; Referente forniture acquisti magazzino manutenzione	**Contratto di manutenzione e smaltimento dei toner usati**
Disposizioni contro le immigrazioni clandestine e Impiego di dittadini di paesi terzi il cui soggiorno è irregolare	I reati di cui all'art. 22, c. 12-bis e all'art. 12, c. 3, 3-bis, 3-ter e 5 D.lgs. 286/1998, possono essere commessi se il datore di lavoro occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, ovvero il cui permesso sia scaduto, revocato o annullato.	Possibilità di utilizzo di manodopera non in regola	Bassa	Direttore, Amministratore Unico, Resp. Ammv.vo, Resp. Risorse Umane	**Contrattualizzazione di tutte le figure operanti in AFOL.**
Frode Informatica	Potenziale alterazione del funzionamento di un sistema informatico o telematico della pubblica amministrazione, o potenziale accesso (senza averne diritto o formale autorizzazione) a dati, informazioni, programmi informatici o telematici al fine di ottenere finanziamenti più alti.	Possibilità di accesso di personale non autorizzato alla sala server; possibilità di installazione di software malevoli e/o non autoirzzati da parte degli utenti sulle proprie macchine; dischi di backup vulnerabili e a rischio di perdita di dati	Medio-Alta	Direttore, Resp. Amm.vo e Referente ufficio acquisti/magazzino/manutenzione e Segreteria	**ARCHIVI FISICI: Introdurre registro per gli accessi alla sala ced. introdurre sistema di spegnimento automatizzato e sicuro dell'infrastruttura server in caso di prolungata assenza di corrente. ANTIMALWARE: integrare la esistente con la parte di Cyber Secuirty per essere aggiornati sulle nuove minacce. AUTENTICAZIONE: definire il passaggio al nuovo sistema di posta con entrambi i domini ed attivare una password policy efficace e doppio fattore di autenticazione (MFA). Rafforzare la password policy attiva aumentando i caratteri delle password portandoli almeno a 12, aumentare la history delle password almeno a 15/20, inserire blocco degli account dopo 10 tentativi sbagliati (può andare bene anche un bocco temporizzato). SISTEMA DI AUTORIZZAZIONE: Rendere gli utenti delle postazioni di lavoro non amministratori della propria macchina se possibile così da diminuire la possibilità di installazione di software malevolo e/o non autorizzato. BACKUP E DISASTER RECOVERY: Valutare il Backup in cloud o immutabile in sostituzione del backup su dischi usb. INFRASTRUTTURA DI NETWORKING: Ridondare i dispositivi critici di rete principali come switch e firewall. RACCOLTA DI LOG E MONITORAGGIO: introdurre sistema di monitoraggio dei server e servizi di rete principali; introdurre sistema di raccolta log ADS.**
Accesso abusivo a sistema informatico e danneggiamento di informazioni, dati, programmi e sistemi informatici, anche dello Stato o altro ente pubblico o comunque di pubblico interesse	Accesso di utenti non autorizzati a sistemi aziendali protetti da misure di sicurezza (es.: sistemi interbancari). Utilizzo abusivo di password di accesso a siti di soggetti terzi, pubblici o privati, al fine di acquisire informazioni riservate e conseguire vantaggi competitivi. Accesso a una postazione PC, a sistemi di gestione aziendali, a sistemi telematici (anche della Pubblica amministrazione) con password diverse dalle proprie o senza autorizzazione specifica, con codici di accesso ottenuti violando le regole stabilite dalle policy e procedure aziendali. Detenzione abusiva di codici di accesso a sistemi informatici dell'Amministrazione giudiziaria o finanziaria, al fine di acquisire informazioni riservate su procedimenti penali/amministrativi che coinvolgano la Società. Manomissione del sistema di sorveglianza interno al fine di cancellare le registrazioni di un incidente avvenuto ai danni di un lavoratore memorizzate sul dispositivo. Assenza o inadeguatezza di un sistema di protezione dei dati e di un				

MAPPATURA ATTIVITA

CICLO AZIENDALE:	***Direzione***
RESPONSABILE	***Direttore***

ATTIVITA SVOLTE	***DESCRIZIONE***	***FUNZIONI COINVOLTE***
DIREZIONE GENERALE DELL'ENTE	Il Direttore è nominato dall'Amministratore Unico con un incarico triennale, rinnovabile. Il Direttore svolge il suo operato, in stretto raccordo con l'Amministratore Unico, con riferimento all'art. 6 dello Statuto ed al Titolo IV punto 3 del Regolamento interno relativo al funzionamento dell'Azienda/Agenzia, nel rispetto del Regolamento di contabilità dell'Agenzia stessa. "Attua gli indirizzi strategici definiti dall'Amministratore Unico ed è responsabile di tutta la gestione e del buon andamento amministrativo, contabile e finanziario dell'Agenzia. In particolare, il Direttore, in base al mandato ricevuto dall'Amministratore Unico, definisce i programmi di lavoro e le iniziative volte al conseguimento degli scopi istituzionali dell'Agenzia" (art. 6 dello Statuto). Predispone il Piano-programma ed i progetti di Bilancio preventivo e consuntivo da sottoporre all'approvazione dell'Amministratore Unico e del Revisore Unico per approvazione.	**DIRETTORE** **AMMINISTRATORE UNICO**
STIPULAZIONE DI ATTI/ CONTRATTI	Tutti gli atti relativi alla gestione dei finanziamenti pubblici e privati che pervengono all'Agenzia vengono predisposti dall'ufficio amministrazione secondo format aziendali e vengono successivamente verificati e firmati dal Direttore (in quanto delegato dall'Amministratore Unico). Gli atti/contratti che presuppongono un impegno di spesa vengono invece sottoscritti con duplice firma (Direttore e Amministratore Unico). I contratti di acquisto inferiore a 3.000,00 possono essere sottoscritti direttamente dall'Amministratore Unico. La legale rappresentanza dell'Ente è in capo all'Amministratore Unico (Soggetto con potere di firma). Il Direttore ha funzione di RUP unico.	**DIRETTORE** **RESPONSABILE AMMINISTRATIVO**
DEFINIZIONE E CONTROLLO DEGLI INDICATORI/OBIETTIVI	Il Direttore definisce gli indicatori di processi/obiettivi nell'ambito delle aree di progettazione, formazione DDIF, Apprendistato duale e orientamento/lavoro, secondo quanto previsto dal Sistema Gestione Qualità e ne verifica il raggiungimento, sulla base di quanto indicato nel Piano Programma, elaborato dal Direttore e sottoposto all'approvazione dell'Amministratore Unico e approvato anche dal Consiglio Provinciale. Il Direttore è Responsabile della Prevenzione della Corruzione e Trasparenza nonché Responsabile Trattamento Dati. Inoltre è delegato dall'Amministratore Unico per il d.lgs. 81/08.	**DIRETTORE** **RESPONSABILI AREE (PROGETTAZIONE, FORMAZIONE E ORIENTAMENTO/LAVORO)** **RESPONSABILE AMMINISTRATIVO**
GESTIONE DEI SISTEMI INFORMATIVI - ARCHIVI FISICI	Lo stabile storico è situato a Como in via bellinzona 88, la struttura è delimitata esternamente da una muraglia con cancelli automatici chiusi L'ingresso principale è monitorato dalla Segreteria. La sala ced risiede al primo piano interrato, la porta d'accesso REI tagliafuoco risulta chiusa a chiave. L'accesso è monitorato da una telecamera di sorveglianza. La sala è utilizzata anche come magazzino di materiale informatico. Le chiavi della sala ced sono in segreteria, non presente un registro per gli accessi. All'interno della sala ced sono presenti due armadi rack, uno che ospita la parte server e l'altro per le apparecchiature di rete e fonia. Entrambi gli armadi sono protetti da un gruppo UPS per gestire gli sbalzi di tensione e interruzioni di corrente, l'Ups però non gestisce lo spegnimento automatizzato dei server. Attualmente non sono presenti sonde d'allarme, i server sono tarati per lo spegnimento in caso di alte temperature ma senza una procedura di sicurezza, sono presenti avvisi via mail ricevuti da cierre. La sala ced ha un sistema di raffrescamento interno. E' presente inventario degli asset interno gestito da Cierre che comprende hardware, software si tratta più che altro di un inventario operativo che di gestione Asset. Gli archivi cartacei sono stipati in Garage eterni sotto il parcheggio, gli archivi risultano chiusi a chiave le chiavi sono disponibiliti in segreteria.	**DIRETTORE, RESP. AMM.VO E REFERENTE UFFICIO ACQUISTI / MAGAZZINO / MANUTENZIONE E SEGRETERIA**

GESTIONE DEI SISTEMI INFORMATIVI - ANTIMALWARE	L'azienda si è dotata di vari sistemi di sicurezza per contrastare i malware; per la parte client server è installato l'antivirus Eset, l'antivirus comprende servizi di antiransomware, application control e webfiltering, la gestione è centralizzata su console cloud gestita da cierre. A Protezione dell'infrastruttura è presente un firewall zyxell usg300 (in fase sdi aggiornamento, il prodotto è a fine vita) con servizi attivi di content filtering e antivirus. I servizi mail sono divisi in due parti una parte on premise su server mdeamon che comprende anche un antivirus interno per la parte amministrativa con dominio cfpcomo.com; la parte didattica invece è configurata su servizi google apps con il dominio cfpcomo.education.com i sistemi di sicurezza sono proprietari di google. All'interno dell'infrastruttura non è presente un sistema di gestione delle patch di sicurezza, per la parte client i pc si aggiornano automaticamente e gli utenti decidono quando installare gli updates, per la parte server sono automatizzati. Il firewall si aggiorna ogni settimana in modo automatico, per gli altri apparati di rete come siwtch, access point, nas ecc. gli aggiornamenti sono manuali e non programmati. L'aggiornamento firmware dei server viene svolto all'occorrenza. I collaboratori sono formati e informati sull'utilizzo degli asset, viene svolta formazione attiva durante l'anno, le procedure d'utilizzo risultano documentate. Presente regolamento informatico con procedure documentate a disposizione degli incaricati e degli ADS.	**DIRETTORE, RESP. AMM.VO E REFERENTE UFFICIO ACQUISTI / MAGAZZINO / MANUTENZIONE E SEGRETERIA, DOCENTI E UTENTI**
GESTIONE DEI SISTEMI INFORMATIVI - AUTENTICAZIONE	L'accesso ai Vari PC e SERVER è gestito da credenziali univoche, presente password policy con le seguenti caratteristiche: 8 caratteri comprensivi di caratteri speciali, scadenza password ogni 3 mesi, history standard, blocco account a seguito di multipli tentitivi d'accesso falliti non attivo. Sono presente due domini separati uno utilizzato dalla parte amministrativa e uno per la parte di didattica. La revisione degli accessi viene svolta all'occorrenza in corrispondenza dell'off-boarding di un utente. Le Password della posta elettronica non scadono, non è presente MFA. L'accesso al gestionale amministrativo/didattica/magazzino e personale esterno avviene con la stessa password dell'utente di dominio. L'accesso al portale zucchetti per visualizzare le timbrature, richiesta permessi ecc. è gestito con credenziali univoche per ogni utente, la password scade regolarmente tramite procedura automatizzata, il personale interno ha l'accesso amministratore per gestire e forzare la scadenza password degli account.	**DIRETTORE, RESP. AMM.VO E REFERENTE UFFICIO ACQUISTI / MAGAZZINO / MANUTENZIONE E SEGRETERIA, DOCENTI E UTENTI**
GESTIONE DEI SISTEMI INFORMATIVI - SISTEMA DI AUTORIZZAZIONE	L'azienda usa i 2 server di dominio active directory di Microsoft per gestire le Autorizzazioni, uno per la parte amministrativa e uno per la parte Didattica. Non è presente procedura documentata di on-boarding e off-boarding, ma risulta esserci prassi consolidata tra la direzione e L'IT. (nella procedura di off-boarding e regolamento informatico sono specificati i dettagli della gestione degli account di dominio e e-mail) Presente riesame annuale degli accessi ai sistemi. Gli utenti sono amministratori della macchina.	**DIRETTORE, RESP. AMM.VO E REFERENTE UFFICIO ACQUISTI / MAGAZZINO / MANUTENZIONE E SEGRETERIA, DOCENTI E UTENTI**
GESTIONE DEI SISTEMI INFORMATIVI - BACKUP E DISASTER RECOVERY	Presente sistema di backup Veeam Backup & Replication che svolge il backup di tutte le macchine virtuali, i backup sono giornalieri e vengono svolti su NAS. È attivo un sistema di repliche gestito sempre da Veeam Backup & Replication, le repliche sono attive durante le ore di lavoroe vengono eseguite ogni ora. E' presente un backup aggiuntivo su disco USB che viene portato fuori sede, il disco viene cambiato ogni settimana da Denise, i backup su disco esterno sono Cifrati. I NAS sono presso la sala CED. È presente un Backup in cloud solo per la PEC istituzionale svolto su amazon S3. Presente procedura interna con la documentaizone dei backup e procedura di restore, manca procedura di disaster recovery. Durante l'anno sono stati fatti restore granulari all'occorrenza. Sono presenti alert di buon funzionamento.	**DIRETTORE, RESP. AMM.VO E REFERENTE UFFICIO ACQUISTI / MAGAZZINO / MANUTENZIONE E SEGRETERIA, DOCENTI E UTENTI**
GESTIONE DEI SISTEMI INFORMATIVI - INFRASTRUTTURA DI NETWORKING	Lq rete risulta segmentata, presente Vlan management e vlan backup. Presente rete wi-fi cfp_didattica che può essere utilizzata a fronte di registrazione del mac address del dispositivo e della password di accesso, la registrazione viene gestita da Moriani. La rete wifi è utilizzabile da chi ne fa richiesta, anche a titolo temporaneo come esterni che vengono ad operare al CFP per tempi contingentati. Il mac address viene registrato e poi rimosso al termine dell'attività. I dispositivi collegati a questa rete posson osolamente accedere alla parte relativa alla didattica su apposito server dedicato. La rete uffici amministrativi è separate da quella della Didattica, i sistemi di rete non sono ridondati, i server hanno la ridondanza con alimentatore, 'dischi e scheda di rete. Sono presenti servizi pubblicati tramite firewall drytek, come webmail di mdeamon e il sistema di videosorveglianza, il sistema di video sorveglianza è su una rete separata. Presente connettività dati che serve sia la parte di navigazione internet che la fonia, presente linea di backup con tecnologia wifi.	**DIRETTORE, RESP. AMM.VO E REFERENTE UFFICIO ACQUISTI / MAGAZZINO / MANUTENZIONE E SEGRETERIA, DOCENTI E UTENTI**
GESTIONE DEI SISTEMI INFOMRATIVI - RACCOLTA DI LOG E MONITORAGGIO	È in fase di introduzione un sistema di monitoraggio dei server e dei servizi di rete principali, nonché di un sistema di raccolta log ADS.	**DIRETTORE, RESP. AMM.VO E REFERENTE UFFICIO ACQUISTI / MAGAZZINO / MANUTENZIONE E SEGRETERIA**

CICLO AZIENDALE:	Direzione	
#	SEZIONI NUOVE DOPO AGGIORNAMENTO REATI PRESUPPOSTO 2020	CHECK
1	Violazioni del Codice Etico aziendale	Y
2	Reati in danno alla Pubblica Amministrazione	Y
3	Delitti informatici e trattamento illecito di dati	Y
4	Delitti di criminalità organizzata	N/A
5	Reati in tema di falsità in moneta, carte di pubblico credito, valori di bollo e strumenti o segni di riconoscimento	N/A
6	Delitti contro l'industria e il commercio	N/A
7	Reati societari	Y
10	Delitti contro la personalità individuale	N/A
13	Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro	N/A
14	Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio	N/A
15	Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori	N/A
16	Altre fattispecie in materia di strumenti di pagamento diversi dai contanti	N/A
17	Delitti in materia di violazione del diritto d'autore	N/A
18	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	Y
19	Reati ambientali	N/A
20	Impiego di cittadini di paesi terzi il cui soggiorno è irregolare	N/A
21	Razzismo e xenofobia	N/A

Ciclo Direzione – Risk Control Matrix

CICLO AZIENDALE: Direzione

RISK CONTROL MATRIX

SEZIONE PRIMA: Comportamenti non conformi al Codice Etico aziendale

VIOLAZIONE	DESCRIZIONE PRINCIPIO DI RIFERIMENTO	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Rispetto SGQ	*svolgimento delle attività regolamentate dal Sistema di Gestione della Qualità, adottato dall'azienda, nel pieno rispetto della politica per la Qualità aziendale, delle relative procedure e delle eventuali istruzioni operative applicabili.*	Adempimenti richiesti da SGQ sono vissuti come un aggravio delle attività degli operatori (burocratizzazione delle attività).	**0,25**	**0,05**	Accettabile	Tutte le figure operanti nel ciclo.

CICLO AZIENDALE: Direzione

RISK CONTROL MATRIX

SEZIONE SECONDA: Reati in danno alla Pubblica Amministrazione

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Frode informatica	*Art. 640-ter c.p.*	Inserimento di dati falsificati al fine di ottenere più finanziamenti o rendicontare costi di fatto non sostenuti.	**0,3**	**0,8**	Rilevante	Resp. Amministrativo, Responsabile Segreteria, Vicedirettore, Responsabili d'Area (Coordinatori per ciascun corso/bando)
Frode informatica	*Art. 640-ter c.p.*	Potenziale alterazione del funzionamento di un sistema informatico o telematico della pubblica amministrazione, o potenziale accesso (senza averne diritto o formale autorizzazione) a dati, informazioni, programmi informatici o telematici al fine di ottenere finanziamenti più alti.	**0,3**	**0,3**	Rilevante	Resp. Amm.vo e Referente ufficio acquisti/magazzino/mautenzione
Truffa in danno dello Stato o di altro ente pubblico	*Art. 640, co. 2, n. 1, c.p.*	Inserimento di dati falsificati al fine di ottenere più finanziamenti o rendicontare costi di fatto non sostenuti.	**0,3**	**0,3**	Rilevante	Direttore e Resp. Amm.vo
Corruzione (varie forme)	*Artt. 317, 318, 319-bis, 319-quater, 320, 321, 322 c.p.*	La fattispecie di reato rappresentata dalla "concussione" può essere commessa se durante una verifica ispettiva da parte di pubblici funzionari, il referente interno di AFOL Como che ha il compito di interfacciarsi con il pubblico ufficiale accetta di sottostare alle richieste sia dirette che indirette dello stesso per non arrecare un danno all'Ente. Le fattispecie di "corruzione", invece, rappresentano il delitto commesso dal pubblico ufficiale che, per compiere un atto del suo ufficio, o per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, in denaro od altra utilità, una retribuzione che non gli è dovuta, o ne accetta la promessa. Gli accordi funzionali alla corruzione di pubblici ufficiali e/o incaricati di pubblico servizio, prodromici alla corruzione, integrano il reato ex art. 346-bis, il quale punisce tutte le condotte che risultino anche solo potenzialmente idonee a ledere l'imparzialità e il buon andamento dell'amministrazione pubblica.	**0,3**	**0,3**	Rilevante	Direttore e Vice-Direttore, nonché altri eventuali soggetti che gestitscono rapporti con pubblici funzionari in occasione di visite ispettive o accertamenti
Corruzione in atti giudiziari	*Artt. 319-ter c.p.*	L'Ente potrebbe indurre il giudice a pronunciarsi in senso favorevole ovvero a considerare la documentazione prodotta in ritardo nel corso di un procedimento, o comunque, a favorire l'Ente a svantaggio della controparte. La corruzione potrebbe avvenire mediante: - il pagamento in denaro; - la scelta di avvalersi in futuro di un fornitore indicato dallo stesso funzionario pubblico; - regalie ed omaggi; - la promessa di assunzione di un parente o amico del funzionario pubblico; - il trasferimento di risorse finanziarie allo Studio Legale che gestisce il contenzioso (parcelle gonfiate).	**0,3**	**0,3**	Rilevante	Direttore e Vice-Direttore

CICLO AZIENDALE: Direzione

RISK CONTROL MATRIX

SEZIONE TERZA: Delitti informatici e trattamento illecito di dati

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Accesso abusivo a sistema informatico e danneggiamento di informazioni, dati, programmi e sistemi informatici, anche dello Stato o altro ente pubblico o comunque di pubblico interesse	*Art. 615-ter, 615-quater, 629, co. 3, 635-bis, 635-ter, 635-quater, 635-quater.1 c.p.*	Accesso di utenti non autorizzati a sistemi aziendali protetti da misure di sicurezza (es.: sistemi interbancari). Utilizzo abusivo di password di accesso a siti di soggetti terzi, pubblici o privati, al fine di acquisire informazioni riservate e conseguire vantaggi competitivi. Accesso a una postazione PC, a sistemi di gestione aziendali, a sistemi telematici (anche della Pubblica amministrazione) con password diverse dalle proprie o senza autorizzazione specifica, con codici di accesso ottenuti violando le regole stabilite dalle policy e procedure aziendali. Detenzione abusiva di codici di accesso a sistemi informatici dell'Amministrazione giudiziaria o finanziaria, al fine di acquisire informazioni riservate su procedimenti penali/amministrativi che coinvolgano la Società. Manomissione del sistema di sorveglianza interno al fine di cancellare le registrazioni di un incidente avvenuto ai danni di un lavoratore memorizzate sul dispositivo. Assenza o inadeguatezza di un sistema di protezione dei dati e di un costante monitoraggio dei dati all'interno della rete.	**0,3**	**0,3**	Rilevante	Direttore, Resp. Amm.vo e Referente ufficio acquisti/magazzino/mautenzione

CICLO AZIENDALE: Direzione

RISK CONTROL MATRIX

SEZIONE SETTIMA: Reati societari

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Ostacolo all'esercizio delle attività di controllo, revisione e delle funzioni delle autorità pubbliche di vigilanza	*Art. 2625 comma 2 c.c.* *Art. 2638 comma 1 e 2 c.c.*	A seguito delle richieste da parte dell'ente di controllo vengono forniti dati fasulli e/o alterati.	**0,05**	**0,1**	Accettabile	Funzionari regionali coinvolte nella verifica ispettiva
Corruzione tra privati	*Art. 2635 c.c.* *Art. 2635-bis c.c.*	I reati di cui agli artt. 2635 e 2635-bis potrebbero realizzarsi mediante la promessa o offerta da parte dell'Ente di denaro o altre utilità non dovute agli organi di controllo, al fine di omettere rilievi emersi nel corso delle verifiche da parte degli organi di controllo.	**0,05**	**0,1**	Accettabile	Direttore, Vice-Direttore e Resp. Amm.vo

CICLO AZIENDALE: Direzione

RISK CONTROL MATRIX

SEZIONE DICIOTTESIMA: Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	*Art. 377-bis c.p.*	Soggetti apicali di AFOL Como potrebbero potenzialmente indurre, con minaccia, la persona chiamata davanti all'autorità giudiziaria a non rendere dichiarazioni utilizzabili in un procedimento penale, ovvero a rendere dichiarazioni mendaci.	**0,3**	**0,3**	Rilevante	Direttore e Vice-Direttore

Gap Analysis e Piano di Azione

CICLO AZIENDALE: DIREZIONE

Rischio	Descrizione Rischio	Descrizione GAP	Priorità	Funzioni coinvolte	Action Plan
Rispetto SGQ	Burocratizzazione delle attività	Il SGQ adottato risulta poco interiorizzato dagli operatori.	Media	Tutte le figure operanti nel ciclo.	**Impostata e svolta attività di sensibilizzazione sulle Procedure, raccogliendo feedback operativi da parte di chi è chiamato ad applicare il SGQ. Sulla base di tali feedback andranno valutate eventuali revisioni future.** **Adottata check-list al fine di verificare le attività e i controlli sui Responsabili d'Area in merito ai progetti/corsi finanziati**
Frode informatica	Inserimento di dati falsificati al fine di ottenere più finanziamenti o rendicontare costi di fatto non sostenuti.	I sistemi di controllo applicati in passato non risultavano pienamente idonei a prevenire il rischio individuato.	Media	Resp. Amministrativo, Responsabile Segreteria, Vicedirettore, Responsabili d'Area (Coordinatori per ciascun corso/bando)	**Utilizzo Sistema Informativo interno: prevista la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password).** **SI regionali/provinciali:** **identificate e comunicate responsabilità in capo a chi opera coi SI regionali e provinciali. Laddove possibile richiedere e fornire possibilità di accesso a detti sistemi con differenti profilazioni a seconda delle attività da svolgere.** **Previsto inoltre un controllo da parte di un adeguato livello aziendale sulle attività svolte dall'utente (monitoraggio dei login e dei dati inseriti).**
Truffa in danno dello Stato o di altro ente pubblico	Inserimento di dati falsificati al fine di ottenere più finanziamenti o rendicontare costi di fatto non sostenuti.	Possibilità di alterazione dei dati dei registri utilizzati nei rapporti con la PA (registri scolastici, rendicontazione finanziamenti, selezione, appalti, ecc.)	Media	Direttore e Resp. Amm.vo	**Utilizzo Sistema Informativo interno: prevista la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password).** **SI regionali/provinciali: identificate e comunicate responsabilità in capo a chi opera coi SI regionali e provinciali. Laddove possibile richiedere e fornire possibilità di accesso a detti sistemi con differenti profilazioni a seconda delle attività da svolgere.** **Previsto inoltre un controllo da parte di un adeguato livello aziendale sulle attività svolte dall'utente (monitoraggio dei login e dei dati inseriti).**
Corruzione (varie forme)	La fattispecie di reato rappresentata dalla "concussione" può essere commessa se durante una verifica ispettiva da parte di pubblici funzionari, il referente interno di AFOL Como che ha il compito di interfacciarsi con il pubblico ufficiale accetta di sottostare alle richieste sia dirette che indirette dello stesso per non arrecare un danno all'Ente. Le fattispecie di "corruzione", invece, rappresentano il delitto commesso dal pubblico ufficiale che, per compiere un atto del suo ufficio, o per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, owero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, in denaro od altra utilità, una retribuzione che non gli è dovuta, o ne accetta la promessa. Gli accordi funzionali alla corruzione di pubblici ufficiali e/o incaricati di pubblico servizio, prodromici alla corruzione, integrano il reato ex art. 346-bis, il quale punisce tutte le condotte	Possibilità di comportamenti illeciti personali		Direttore e Vice-Direttore, nonché altri eventuali soggetti che gestitscono rapporti con pubblici funzionari in occasione di visite ispettive o accertamenti	**Precipua diffusione ed attuazione del Piano Triennale di Prevenzione della Corruzione e Trasparenza Formazione permanente Istituzione di Commissioni di Gara che sottraggano le decisioni al singolo**

Corruzione in atti giudiziari	L'Ente potrebbe indurre il giudice a pronunciarsi in senso favorevole owero a considerare la documentazione prodotta in ritardo nel corso di un procedimento, o comunque, a favorire l'Ente a svantaggio della controparte. La corruzione potrebbe avvenire mediante: - il pagamento in denaro; - la scelta di avvalersi in futuro di un fornitore indicato dallo stesso funzionario pubblico; - regalie ed omaggi; - la promessa di assunzione di un parente o amico del funzionario pubblico; - il trasferimento di risorse finanziarie allo Studio Legale che gestisce il contenzioso (parcelle gonfiate).	Comportamenti illeciti personali	Bassa	Direttore e Vice-Direttore	**Diffusione del PTCPT e massima condivisione del processo decisionale, puntuale rendicontazione delle attività di vigilanza e controllo**
Ostacolo all'esercizio delle attività di controllo, revisione e delle funzioni delle autorità pubbliche di vigilanza	Fornire dati fasulli.	I sistemi di controllo sulla corretta tenuta della documentazione a supporto delle attività svolte non prevengono pienamente il rischio individuato.	Medio-Alta	Funzionari regionali coinvolte nella verifica ispettiva	**Formalizzazione all'interno del proprio SGQ di un'apposita procedura riguardante la Rendicontazione dei progetti finanziati.** **Sensibilizzazione dei docenti circa l'importanza della rendicontazione e del ruolo che ha la corretta e puntuale tenuta dei documenti a supporto.** **Prevista a conclusione delle attività (in particolare per quelle legate a progetti finanziati) una check list di verifica della relativa documentazione (effettuando un controllo sulla presenza del documento e un controllo sulla completezza/corretta tenuta del documento). Tale controllo potrà essere effettuato dalla Segreteria didattica in coordinamento con amministrazione e responsabili di area.** **A seguito del controllo la documentazione non dovrà più essere liberamente accessibile agli operatori.**
Corruzione tra privati	I reati di cui agli artt. 2635 e 2635-bis potrebbero realizzarsi mediante la promessa o offerta da parte dell'Ente di denaro o altre utilità non dovute agli organi di controllo, al fine di omettere rilievi emersi nel corso delle verifiche da parte degli organi di controllo.	Comportamenti illeciti personali	Media	Direttore, Vice-Direttore e Resp. Amm.vo	**Diffusione del PTCPT e massima condivisione del processo decisionale, puntuale rendicontazione delle attività di vigilanza e controllo**
Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	Soggetti apicali di AFOL Como potrebbero potenzialmente indurre, con minaccia, la persona chiamata davanti all'autorità giudiziaria a non rendere dichiarazioni utilizzabili in un procedimento penale, owero a rendere dichiarazioni mendaci.	Possibilità di comportamenti illeciti personali	Bassa	Direttore e Vice-Direttore	**Diffusione del PTCPT e massima condivisione del processo decisionale, puntuale rendicontazione delle attività di vigilanza e controllo**
Frode Informatica	Potenziale alterazione del funzionamento di un sistema informatico o telematico della pubblica amministrazione, o potenziale accesso (senza averne diritto o formale autorizzazione) a dati, informazioni, programmi informatici o telematici al fine di ottenere finanziamenti più alti.	Possibilità di accesso di personale non autorizzato alla sala server; possibilità di installazione di software malevoli e/o non autoirzzati da parte degli utenti sulle proprie macchine; dischi di backup vulnerabili e a rischio di perdita di dati	Medio-Alta	Tutte le figure operanti nel ciclo.	**ARCHIVI FISICI: Introdurre registro per gli accessi alla sala ced. introdurre sistema di spegnimento automatizzato e sicuro dell'infrastruttura server in caso di prolungata assenza di corrente.** **ANTIMALWARE: integrare la esistente con la parte di Cyber Secuirty per essere aggiornati sulle nuove minacce.** **AUTENTICAZIONE: definire il passaggio al nuovo sistema di posta con entrambi i domini ed attivare una password policy efficace e doppio fattore di autenticazione (MFA). Rafforzare la password policy attiva aumentando i caratteri delle password portandoli almeno a 12, aumentare la history delle password almeno a 15/20, inserire blocco degli account dopo 10 tentativi sbagliati (può andare bene anche un bocco temporizzato). SISTEMA DI AUTORIZZAZIONE: Rendere gli utenti delle postazioni di lavoro non amministratori della propria macchina se possibile così da diminuire la possibilità di installazione di software malevolo e/o non autorizzato. BACKUP E DISASTER RECOVERY: Valutare il Backup in cloud o immutabile in sostituzione del backup su dischi usb. INFRASTRUTTURA DI NETWORKING: Ridondare i dispositivi critici di rete principali come switch e firewall. RACCOLTA DI LOG E MONITORAGGIO: introdurre sistema di monitoraggio dei server e servizi di rete principali; introdurre sistema di raccolta log ADS.**
Accesso abusivo a sistema informatico e danneggiamento di informazioni, dati, programmi e sistemi informatici, anche dello Stato o altro ente pubblico o comunque di pubblico interesse	Accesso di utenti non autorizzati a sistemi aziendali protetti da misure di sicurezza (es.: sistemi interbancari). Utilizzo abusivo di password di accesso a siti di soggetti terzi, pubblici o privati, al fine di acquisire informazioni riservate e conseguire vantaggi competitivi. Accesso a una postazione PC, a sistemi di gestione aziendali, a sistemi telematici (anche della Pubblica amministrazione) con password diverse dalle proprie o senza autorizzazione specifica, con codici di accesso ottenuti violando le regole stabilite dalle policy e procedure aziendali. Detenzione abusiva di codici di accesso a sistemi informatici dell'Amministrazione giudiziaria o finanziaria, al fine di acquisire informazioni riservate su procedimenti penali/amministrativi che coinvolgano la Società. Manomissione del sistema di sorveglianza interno al fine di cancellare le registrazioni di un incidente awenuto ai danni di un lavoratore memorizzate sul dispositivo. Assenza o inadeguatezza di un				

MAPPATURA ATTIVITA

CICLO AZIENDALE: ***Formazione (DDIF, Apprendistato, Duale)***

RESPONSABILE ***Responsabile Area Formazione***

ATTIVITA SVOLTE	***DESCRIZIONE***	***FUNZIONI COINVOLTE***
ANALISI E RELAZIONI CON IL TERRITORIO	Analisi delle opportunità offerte dai diversi Bandi/Avvisi (provinciali, regionali, nazionali e UE) dei fabbisogni specifici espressi dai diversi committenti pubblici e privati abbinata allo studio dei fabbisogni di formazione in ambito territoriale attraverso le informazioni recepite da: -relazioni con il sistema istituzionale e sociale locale; -relazioni con il sistema produttivo; -relazioni con il sistema scolastico; -relazioni con le famiglie degli allievi; - relazione con i servizi di riferimento per gli allievi con BES.	**DIRETTORE** **VICE-DIRETTORE** **RESPONSABILE AREA FORMAZIONE (DDIF, APPRENDISTATO, DUALE)** **RESPONSABILE AREA PROGETTAZIONE, ORIENTAMENTO/LAVORO**
GESTIONE BUDGET	Gestione dei budget di progetto in base ai diversi interventi proposti in collaborazione con la Direzione e il Responsabile Amministrativo dell'Agenzia.	**DIRETTORE** **VICE-DIRETTORE** **RESPONSABILE AREA PROGETTAZIONE, ORIENTAMENTO/LAVORO** **RESPONSABILE AMMINISTRATIVO**
PROGETTAZIONE	Sulla base degli indirizzi del Piano Programma il responsabile di area procede all'elaborazione dei singoli progetti (secondo vincoli e risorse dei singoli dispositivi e/o contratti di servizio). Ogni singolo progetto viene sottoposto al riesame della Direzione e ad una verifica formale prima della presentazione. I Responsabili dell'Area PROGETTAZIONE, ORIENTAMENTO/LAVORO, FORMAZIONE (DDIF, APPRENDISTATO, DUALE), prima dell'attivazione del progetto, effettuano i necessari controlli per l'accertamento dei requisiti richiesti dai singoli bandi di riferimento. La progettazione rivolta ad allievi con BES è concertata anche con i servizi di riferimento, le famiglie, i consigli di classe e i coordinatori del corso. Ciascun Responsabile individua dunque le risorse e le modalità organizzative necessarie alla realizzazione dei progetti/corsi assegnati. Viene progettata ed erogata l'attività di orientamento sia in ingresso (relazionandosi con gli istituti secondari di primo grado) sia in uscita per l'orientamento post qualifica/diploma (inserimento lavorativo).	**DIRETTORE** **VICE-DIRETTORE** **RESPONSABILE AREA PROGETTAZIONE, ORIENTAMENTO/LAVORO** **RESPONSABILE AREA FORMAZIONE (DDIF, APPRENDISTATO, DUALE)**
EROGAZIONE	Il processo di erogazione del servizio formativo si articola in servizi erogati all'interno dell'Agenzia e servizi e attività realizzate fuori dall'edificio scolastico. I processi vengono descritti nell'allegato al capitolo quinto del MQ e prevedono: accoglienza, lezioni frontali, lezioni erogate individualmente o a piccolo gruppo a supporto delle lezioni di classe (allievi BES), attività laboratoriali, verifiche finali e in itinere (supporto alle verifiche per allievi con BES), stage (compresi stage interni e esterni protetti per allievi con BES), visite guidate e gite scolastiche (con supporto per allievi con BES).	**RESPONSABILE AREA FORMAZIONE (DDIF, APPRENDISTATO, DUALE)** **TUTOR** **DOCENTI**
CONCLUSIONE E RENDICONTAZIONE	Vengono effettuati i controlli necessari (in avvio, in itinere e a conclusione dell'erogazione) su aspetti logistici, didattici e di apprendimento. I dettagli sono descritti al capitolo quinto del MQ. La rintracciabilità del servizio portato a termine è garantito dalla tenuta dei documenti di supporto (registri, calendari, questionari, ecc...) in ogni fase dell'erogazione. I dati vengono registrati sul sistema GRS direttamente dai singoli docenti, e quotidianamente inviati a Regione Lombardia. Tutta la documentazione a supporto permette di ripercorrere a ritroso l'iter formativo al fine di evidenziare eventuali criticità sopraggiunte durante l'erogazione del servizio e costituisce il punto di partenza per il processo di rendicontazione.	**RESPONSABILE AREA FORMAZIONE (DDIF, APPRENDISTATO, DUALE)** **TUTOR** **DOCENTI**

GESTIONE DEI SISTEMI INFORMATIVI - ANTIMALWARE	L'azienda si è dotata di vari sistemi di sicurezza per contrastare i malware; per la parte client server è installato l'antivirus Eset, l'antivirus comprende servizi di antiransomware, application control e webfiltering, la gestione è centralizzata su console cloud gestita da cierre. A Protezione dell'infrastruttura è presente un firewall zyxell usg300 (in fase sdi aggiornamento, il prodotto è a fine vita) con servizi attivi di content filtering e antivirus. I servizi mail sono divisi in due parti una parte on premise su server mdeamon che comprende anche un antivirus interno per la parte amministrativa con dominio cfpcomo.com; la parte didattica invece è configurata su servizi google apps con il dominio cfpcomo.education.com i sistemi di sicurezza sono proprietari di google. All'interno dell'infrastruttura non è presente un sistema di gestione delle patch di sicurezza, per la parte client i pc si aggiornano automaticamente e gli utenti decidono quando installare gli updates, per la parte server sono automatizzati. Il firewall si aggiorna ogni settimana in modo automatico, per gli altri apparati di rete come siwtch, access point, nas ecc. gli aggiornamenti sono manuali e non programmati. L'aggiornamento firmware dei server viene svolto all'occorrenza. I collaboratori sono formati e informati sull'utilizzo degli asset, viene svolta formazione attiva durante l'anno, le procedure d'utilizzo risultano documentate. Presente regolamento informatico con procedure documentate a disposizione degli incaricati e degli ADS.	**RESPONSABILE AREA FORMAZIONE (DDIF, APPRENDISTATO, DUALE)** **TUTOR** **DOCENTI**
GESTIONE DEI SISTEMI INFORMATIVI - AUTENTICAZIONE	"L'accesso ai Vari PC e SERVER è gestito da credenziali univoche, presente password policy con le seguenti caratteristiche: 8 caratteri comprensivi di caratteri speciali, scadenza password ogni 3 mesi, history standard, blocco account a seguito di multipli tentitivi d'accesso falliti non attivo. Sono presente due domini separati uno utilizzato dalla parte amministrativa e uno per la parte di didattica. La revisione degli accessi viene svolta all'occorrenza in corrispondenza dell'off-boarding di un utente. Le Password della posta elettronica non scadono, non è presente MFA. L'accesso al gestionale amministrativo/didattica/magazzino e personale esterno avviene con la stessa password dell'utente di dominio. L'accesso al portale zucchetti per visualizzare le timbrature, richiesta permessi ecc. è gestito con credenziali univoche per ogni utente, la password scade regolarmente tramite procedura automatizzata, il personale interno ha l'accesso amministratore per gestire e forzare la scadenza password degli account."	**RESPONSABILE AREA FORMAZIONE (DDIF, APPRENDISTATO, DUALE)** **TUTOR** **DOCENTI**
GESTIONE DEI SISTEMI INFORMATIVI - SISTEMA DI AUTORIZZAZIONE	L'azienda usa i 2 server di dominio active directory di Microsoft per gestire le Autorizzazioni, uno per la parte amministrativa e uno per la parte Didattica. Non è presente procedura documentata di on-boarding e off-boarding, ma risulta esserci prassi consolidata tra la direzione e L'IT. (nella procedura di off-boarding e regolamento informatico sono specificati i dettagli della gestione degli account di dominio e e-mail) Presente riesame annuale degli accessi ai sistemi. Gli utenti sono amministratori della macchina.	**RESPONSABILE AREA FORMAZIONE (DDIF, APPRENDISTATO, DUALE)** **TUTOR** **DOCENTI**
GESTIONE DEI SISTEMI INFORMATIVI - BACKUP E DISASTER RECOVERY	Presente sistema di backup Veeam Backup & Replication che svolge il backup di tutte le macchine virtuali, i backup sono giornalieri e vengono svolti su NAS. È attivo un sistema di repliche gestito sempre da Veeam Backup & Replication, le repliche sono attive durante le ore di lavoroe vengono eseguite ogni ora. E' presente un backup aggiuntivo su disco USB che viene portato fuori sede, il disco viene cambiato ogni settimana da Denise, i backup su disco esterno sono Cifrati. I NAS sono presso la sala CED. È presente un Backup in cloud solo per la PEC istituzionale svolto su amazon S3. Presente procedura interna con la documentaizone dei backup e procedura di restore, manca procedura di disaster recovery. Durante l'anno sono stati fatti restore granulari all'occorrenza. Sono presenti alert di buon funzionamento.	**RESPONSABILE AREA FORMAZIONE (DDIF, APPRENDISTATO, DUALE)** **TUTOR** **DOCENTI**
GESTIONE DEI SISTEMI INFORMATIVI - INFRASTRUTTURA DI NETWORKING	Lq rete risulta segmentata, presente Vlan management e vlan backup. Presente rete wi-fi cfp_didattica che può essere utilizzata a fronte di registrazione del mac address del dispositivo e della password di accesso, la registrazione viene gestita da Moriani. La rete wifi è utilizzabile da chi ne fa richiesta, anche a titolo temporaneo come esterni che vengono ad operare al CFP per tempi contingentati. Il mac address viene registrato e poi rimosso al termine dell'attività. I dispositivi collegati a questa rete posson osolamente accedere alla parte relativa alla didattica su apposito server dedicato. La rete uffici amministrativi è separate da quella della Didattica, i sistemi di rete non sono ridondati, i server hanno la ridondanza con alimentatore, 'dischi e scheda di rete. Sono presenti servizi pubblicati tramite firewall drytek, come webmail di mdeamon e il sistema di videosorveglianza, il sistema di video sorveglianza è su una rete separata. Presente connettività dati che serve sia la parte di navigazione internet che la fonia, presente linea di backup con tecnologia wifi.	**RESPONSABILE AREA FORMAZIONE (DDIF, APPRENDISTATO, DUALE)** **TUTOR** **DOCENTI**
GESTIONE DEI SISTEMI INFOMRATIVI - RACCOLTA DI LOG E MONITORAGGIO	È in fase di introduzione un sistema di monitoraggio dei server e dei servizi di rete principali, nonché di un sistema di raccolta log ADS.	**RESPONSABILE AREA FORMAZIONE (DDIF, APPRENDISTATO, DUALE)** **TUTOR** **DOCENTI**

UNI EN ISO 9001:2015
(EA 37, 38)

AGENZIA PER LA FORMAZIONE, L'ORIENTAMENTO E IL LAVORO DELLA PROVINCIA DI COMO
CENTRO DI FORMAZIONE PROFESSIONALE
dedicato a "Luigi Grisoni"
COMO Monteolimpino via Bellinzona, 88 tel. 031/571055 - 574000 fax 575047
C.F. 95092770130 P.Iva 03095420133 e-mail: info@cfpcomo.com www.cfpcomo.com

CICLO AZIENDALE:	Formazione (DDIF, Apprendistato, Duale)	
#	SEZIONI NUOVE DOPO AGGIORNAMENTO REATI PRESUPPOSTO 2024	CHECK
1	Violazioni del Codice Etico aziendale	Y
2	Reati in danno alla Pubblica Amministrazione	Y
3	Delitti informatici e trattamento illecito di dati	Y
4	Delitti di criminalità organizzata	N/A
5	Reati in tema di falsità in moneta, carte di pubblico credito, valori di bollo e strumenti o segni di riconoscimento	Y
6	Delitti contro l'industria e il commercio	Y
7	Reati societari	Y
10	Delitti contro la personalità individuale	Y
13	Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro	Y
14	Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio	N/A
15	Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori	N/A
16	Altre fattispecie in materia di strumenti di pagamento diversi dai contanti	N/A
17	Delitti in materia di violazione del diritto d'autore	Y
18	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	N/A
19	Reati ambientali	Y
20	Impiego di cittadini di paesi terzi il cui soggiorno è irregolare	Y
21	Razzismo e xenofobia	Y

UNI EN ISO 9001:2015
(EA 37, 38)
AGENZIA PER LA FORMAZIONE, L'ORIENTAMENTO E IL LAVORO DELLA PROVINCIA DI COMO
CENTRO DI FORMAZIONE PROFESSIONALE
dedicato a "Luigi Grisoni"
COMO Monteolimpino via Bellinzona, 88 tel. 031/571055 - 574000 fax 575047
C.F. 95092770130 P.Iva 03095420133 e-mail: info@cfpcomo.com www.cfpcomo.com

CICLO AZIENDALE: Formazione (DDIF, Apprendistato, Duale)

RISK CONTROL MATRIX

SEZIONE PRIMA: Comportamenti non conformi al Codice Etico aziendale

VIOLAZIONE	DESCRIZIONE PRINCIPIO DI RIFERIMENTO	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Verificabilità	*tutte le attività dell'AZIENDA vengono adeguatamente registrate in maniera da consentire la verifica dei processi di decisione, autorizzazione e svolgimento.*	Invio di informazioni e documentazioni utilizzando strumenti identificativi di altri operatori o dirigenti dell'Ente (ad es. Carta Regionale dei Servizi).	**0,2**	**0,5**	Accettabile	Direttore, Vicedirettore (Area Progettazione-Orientamento/Lavoro), Amministrazione, Segreteria, Responsabili d'area (Formazione,DDIF, Duale e Apprendistato)
Legalità	*l'AZIENDA si impegna a rispettare, nello svolgimento di tutte le proprie attività, le leggi internazionali, nazionali e regionali in vigore in Italia e in ciascun Paese nel quale opera anche tramite branch locali.*	Commissione di furti in determinate aree della struttura (laboratori, spogliatoi,...) agevolati dalla mancata assegnazione/assunzione di responsabilità specifiche riguardo il controllo delle aree interessate.	**0,5**	**1**	Critico	Tutte le funzioni dell'Ente
Onestà	*nei rapporti con i CLIENTI, tra i DESTINATARI e verso i TERZI, l'adesione e la concreta applicazione di quanto dichiarato nel presente CODICE ETICO costituisce elemento essenziale della buona gestione aziendale.*	Fornire informazioni agli utenti senza preventivamente verificarne le fonti normative o senza essere certi di quanto dichiarato.	**0,3**	**0,5**	Rilevante	Docenti, Tutor, Addetti Segreteria.
Trasparenza	*l'AZIENDA improntai rapporti di qualsiasi natura e verso qualsiasi stakeholder alla chiarezza delle intenzioni e all'assenza di volontà di occultamento, rispettando al contempo gli obblighi derivanti dalla normativa vigente in materia di trattamento dei dati riservati.*	Tenuta errata dei registri.	**0,1**	**0,8**	Accettabile	Docenti, Segreteria Generale
Trasparenza	*l'AZIENDA improntai rapporti di qualsiasi natura e verso qualsiasi stakeholder alla chiarezza delle intenzioni e all'assenza di volontà di occultamento, rispettando al contempo gli obblighi derivanti dalla normativa vigente in materia di trattamento dei dati riservati.*	Conflitti tra funzioni e confusione (anche operativa) dovuta a scarsa assunzione di responsabilità/definizione non puntuale delle responsabilità di ciascuna figura.	**0,25**	**0,4**	Accettabile	Tutte le funzioni del ciclo
Rispetto Privacy	*trattamento di dati personali e dati sensibili nel rispetto della normativa vigente.*	Diffuzione non autorizzata di dati personali/sensibili relativi agli alunni, anche quando trattati tramite mezzi informatici (es. e-mail, server,...).	**0,1**	**0,3**	Accettabile	Tutte le funzioni del ciclo
Rispetto Privacy	*trattamento di dati personali e dati sensibili nel rispetto della normativa vigente.*	Raccolta di dati personali delle "modelle"per attività didattica, senza raccolta autorizzazione al trattamento dei dati.	**0,25**	**0,4**	Accettabile	Alunni e docenti di laboratorio
Rispetto SGQ	*svolgimento delle attività regolamentate dal Sistema di Gestione della Qualità, adottato dall'azienda, nel pieno rispetto della politica per la Qualità aziendale, delle relative procedure e delle eventuali istruzioni operative applicabili.*	Ritardi nella compilazione dei moduli o, più in generale, nell'applicazione del SGQ (con particolre riferimento alla tenuta e consegna della documentazione a supporto delle attività svolte).	**1**	**1**	Critico	Tutte le funzioni del ciclo

CICLO AZIENDALE: Formazione (DDIF, Apprendistato, Duale)

RISK CONTROL MATRIX

SEZIONE SECONDA: Reati in danno alla Pubblica Amministrazione

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Frode informatica	*Art. 640-ter c.p.*	Inserimento nei sistemi Regionali e Provinciali di dati non reali al fine di ottenere un maggior numero di finanziamenti o far risultare requisiti non posseduti.	**0,3**	**0,8**	Rilevante	Responsabile Segreteria didattica e Responsabili d'Area
Frode informatica	*Art. 640-ter c.p.*	Potenziale alterazione del funzionamento di un sistema informatico o telematico della pubblica amministrazione, o potenziale accesso (senza averne diritto o formale autorizzazione) a dati, informazioni, programmi informatici o telematici al fine di ottenere finanziamenti più alti.	**0,3**	**0,3**	Rilevante	Responsabili d'Area, Docenti, Tutor
Truffa in danno dello Stato o di altro ente pubblico	*Art. 640, co. 2, n. 1, c.p.*	Si commette il reato di truffa in danno dello Stato o di altro ente pubblico e malversazione di erogazioni pubbliche nel momento in cui, in fase di rendicontazione delle attività svolte, il responsabile amministrativo dichiara il falso, modificando fraudolentemente i dati del corso di formazione, oppure il docente riporta dati non corretti nel registro elettronico, procurando per sé o altri un ingiusto profitto con altrui danno. A seguito della commissione dei precedente reato, l'Ente ottiene una indebita percezione di erogazioni a danno dello Stato.	**0,3**	**0,3**	Rilevante	Direttore, Responsabili d'Area, Docenti
Concussione	*Art. 317 c.p.*	Accordi illeciti con pubblici ufficiali volti all'ottenimento di benefici per l'ente.	**0,5**	**0,2**	Accettabile	Direttore, Responsabili d'Area
Corruzione	*Art. 318 c.p.* *Art. 319 c.p.* *Art. 319 bis c.p.* *Art. 319 ter c.p.* *Art. 320 c.p.* *Art. 321 c.p.* *Art. 322 c.p.*	Accordi illeciti con pubblici ufficiali volti all'ottenimento di benefici per l'ente.	**0,5**	**0,2**	Accettabile	Direttore, Responsabili d'Area

CICLO AZIENDALE:	Formazione (DDIF, Apprendistato, Duale)

RISK CONTROL MATRIX

SEZIONE TERZA - Delitti informatici e trattamento illecito di dati

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Accesso abusivo a sistema informatico e danneggiamento di informazioni, dati, programmi e sistemi informatici, anche dello Stato o altro ente pubblico o comunque di pubblico interesse	*Art. 615-ter, 615-quater, 629, co. 3, 635-bis, 635-ter, 635-quater, 635-quater.1 c.p.*	Accesso di utenti non autorizzati a sistemi aziendali protetti da misure di sicurezza (es.: sistemi interbancari). Utilizzo abusivo di password di accesso a siti di soggetti terzi, pubblici o privati, al fine di acquisire informazioni riservate e conseguire vantaggi competitivi. Accesso a una postazione PC, a sistemi di gestione aziendali, a sistemi telematici (anche della Pubblica amministrazione) con password diverse dalle proprie o senza autorizzazione specifica, con codici di accesso ottenuti violando le regole stabilite dalle policy e procedure aziendali. Detenzione abusiva di codici di accesso a sistemi informatici dell'Amministrazione giudiziaria o finanziaria, al fine di acquisire informazioni riservate su procedimenti penali/amministrativi che coinvolgano la Società. Manomissione del sistema di sorveglianza interno al fine di cancellare le registrazioni di un incidente avvenuto ai danni di un lavoratore memorizzate sul dispositivo. Assenza o inadeguatezza di un sistema di protezione dei dati e di un costante monitoraggio dei dati all'interno della rete.	**0,3**	**0,3**	Rilevante	Responsabili d'Area, Docenti, Tutor

CICLO AZIENDALE:	Formazione (DDIF, Apprendistato, Duale)

RISK CONTROL MATRIX

SEZIONE QUINTA: Reati in tema di falsità in moneta, carte di pubblico credito, valori di bollo e strumenti o segni di riconoscimento

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Spendita e introduzione nello Stato di monete falsificate anche ricevute in buona fede	*Art. 453 co. 1 n. 3 c.p.* *Art. 455 c.p.* *Art. 457 c.p.*	Ricevere pagamenti (sala/bar, laboratorio estetica e laboratorio acconciatura) in contanti con monete/banconote false non individuate e poi utilizzate.	**0,2**	**0,2**	Accettabile	Modelle, utenti bar e esterni in caso di eventi, docenti.

CICLO AZIENDALE:	Formazione (DDIF, Apprendistato, Duale)

RISK CONTROL MATRIX

SEZIONE SESTA: Delitti contro l'industria e il commercio

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Vendita di sostanze alimentari non genuine come genuine	*Art. 516 c.p.*	Durante servizi di catering, possibile utilizzo di sostanze alimentari scadute o mal conservate (ad es. mancato rispetto della catena del freddo).	**0,25**	**0,5**	Accettabile	Alunni docenti laboratorio alimentazione

CICLO AZIENDALE:	Formazione (DDIF, Apprendistato, Duale)

RISK CONTROL MATRIX

SEZIONE SETTIMA: Reati Societari

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Ostacolo all'esercizio delle attività di controllo, revisione e delle funzioni delle autorità pubbliche di vigilanza	*Art. 2625 comma 2 c.c.* *Art. 2638 comma 1 e 2 c.c.*	Alterazione dei dati richiesti durante i controlli ispettivi (ad es. facendo figurare come svolte attività non effettivamente svolte)..	**1**	**0,8**	Critico	Direzione, Vice Direzione, Amministrazione, Segreteria, Resp. Area
Corruzione tra privati	*Art. 2635 c.c.* *Art. 2635-bis c.c.*	I reati di cui agli artt. 2635 e 2635-bis c.c. potrebbero essere commessi qualora esponenti dell'Ente ricevessero somme di denaro al fine di rilasciare attestati di formazione in assenza dei requisiti e delle condizioni previste dalle procedure vigenti.	**1**	**0,8**	Critico	Direzione, Vice Direzione, Amministrazione, Segreteria, Resp. Area

CICLO AZIENDALE: Formazione (DDIF, Apprendistato, Duale)

RISK CONTROL MATRIX

SEZIONE DECIMA: Reati contro la personalità individuale

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Riduzione o mantenimento in schiavitù o servitù	*Art. 600 c.p.*	Alterazione dei rapporti tra colleghi a seguito di situazioni di conflitto operativo/ideologico.	**0,3**	**0,8**	Rilevante	Personale dipendente
Riduzione o mantenimento in schiavitù o servitù	*Art. 600 c.p.*	Alterazione rapporto docente/alunno finalizzato all'ottenimento di vantaggi per entrambi.	**0,01**	**1**	Accettabile	Alunni, tutor e docenti.

CICLO AZIENDALE: Formazione (DDIF, Apprendistato, Duale)

RISK CONTROL MATRIX

SEZIONE TREDICESIMA: Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Lesioni personali colpose	*Art. 590 c.p.*	Utilizzo incauto di attrezzature, strumenti, prodotti utilizzati nelle attività di laboratorio.	**0,5**	**0,85**	Rilevante	Alunni e docenti di laboratorio
Omicidio colposo	*Art. 589 c.p.*	Utilizzo incauto di attrezzature, strumenti, prodotti utilizzati nelle attività di laboratorio.	**0,01**	**1**	Accettabile	Alunni e docenti di laboratorio

CICLO AZIENDALE: Formazione (DDIF, Apprendistato, Duale)

RISK CONTROL MATRIX

SEZIONE DICIASSETTESIMA: Delitti in materia di violazione del diritto d'autore

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Riproduzione abusiva e diffusione (anche parziale) di opera dell'ingegno protetta	*art.171-ter l. 633/1941*	Distribuzione e utilizzo di testi fotocopiati oltre il limite previsto per legge.	**0,1**	**0,7**	Accettabile	Docenti e tutor

CICLO AZIENDALE: azione (DDIF, Apprendistato, D

RISK CONTROL MATRIX

SEZIONE DICIANNOVESIMA: Reati ambientali

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Inquinamento ambientale e delitti colposi contro l'ambiente	*Art. 452-bis, 452-quinquies c.p.*	Scorretto smaltimento degli oli usausti delle cucine	**0,1**	**0,7**	Accettabile	Resp. Area, Direzione, Sostegno, Progettazione-Orientamento-Lavoro

CICLO AZIENDALE:	Formazione (DDIF, Apprendistato, Duale)
RISK CONTROL MATRIX	

SEZIONE VENTUNESIMA: Razzismo e xenofobia

RISCHIO REATO	*RIFERIMENTI NORMATIVI*	*CONDOTTA ERRATA*	*PROBABILITA*	*IMPATTO*	*VALUTAZIONE*	*FUNZIONI COINVOLTE*
Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa	*Art. 604-bis c.p.*	Diffondere, durante attività formative/eventi, organizzati dall'ente, idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istigare a commettere o commettere atti di discriminazione per motivi razziali, etnici, nazionali o religiosi. Ed ancora, promuovere, durante attività formative/eventi, organizzati dall'ente, lo sviluppo di organizzazioni, associazioni, movimenti o gruppi che abbiano tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi	**0,3**	**0,3**	Rilevante	Direttore, Responsabili d'Area, Tutor, Docenti

AGENZIA PER LA FORMAZIONE, L'ORIENTAMENTO E IL LAVORO DELLA PROVINCIA DI COMO
CENTRO DI FORMAZIONE PROFESSIONALE
dedicato a "Luigi Grisoni"
COMO Monteolimpino via Bellinzona, 88 tel. 031/571055 - 574000 fax 575047
C.F. 95092770130 P.Iva 03095420133 e-mail: info@cfpcomo.com www.cfpcomo.com
UNI EN ISO 9001:2015
(EA 37, 38)

Gap Analysis e Piano di Azione

CICLO AZIENDALE: FORMAZIONE (DDIF, Apprendistato, Duale)

Rischio	Descrizione Rischio	Descrizione GAP	Priorità	Funzioni coinvolte	Action Plan
Verificabilità	Invio di informazioni e documentazioni utilizzando strumenti identificativi di altri operatori o dirigenti dell'Ente (ad es. Carta Regionale dei Servizi).	I controlli rilevati non risultano pienamente efficaci nel prevenire il rischio individuato.	Media	Direttore, Vicedirettore (Area Progettazione-Orientamento/Lavoro), Amministrazione, Segreteria, Responsabili d'area (Formazione,DDIF, Duale e Apprendistato)	**Utilizzo Sistema Informativo interno: prevedere la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password) e degli strumenti identificativi.**
Legalità	Commissione di furti in determinate aree della struttura (laboratori, spogliatoi,...) agevolati dalla mancata assegnazione/assunzione di responsabilità specifiche riguardo il controllo delle aree interessate.	Determinate funzioni di controllo non sono presenti o espressamente assegnate.	Media	Tutte le funzioni dell'Ente	**Previsto e montato un sistema di telecamere a circuito chiuso ai fini di videosorveglianza sia all'esterno sia all'interno della struttura. Tale sistema consente un controllo degli accessi ad aree non presidiate (ad es. chiusura a chiave degli spogliatoi al termine del loro utilizzo, deposito della chiave da parte del docente in segreteria; qualora gli alunni necessitassero di recarsi negli spogliatoi dovranno comunicarlo al docente che farà consegnare la chiave dalla segreteria).**
Onestà	Fornire informazioni agli utenti senza preventivamente verificarne le fonti normative o senza essere certi di quanto dichiarato.	Non sono stati rilevate attività di controllo a presidio del rischio individuato	Bassa	Docenti, Tutor, Addetti Segreteria.	**Sensibilizzare gli operatori a diretto contatto con l'utenza sul tema. In particolare prevedere che l'utenza possa identificare chiaramente da quali funzioni può ricevere le informazioni sul Sistema Dote e le normative applicate alle attività dell'ente (a tale proposito valutare la possibilità di colloqui presso la segreteria didattica in giorni e orari stabiliti con le figure aziendali abilitate a fornire queste informazioni).**
Trasparenza	Tenuta errata dei registri e compilazione del Registro Elettronico	I sistemi di controllo sulla corretta tenuta della documentazione a supporto delle attività svolte non prevengono pienamente il rischio individuato.	Media	Docenti, Segreteria Generale	**Sensibilizzazione dei docenti circa l'importanza della rendicontazione e del ruolo che ha la corretta e puntuale tenuta dei documenti a supporto (Registro cartaceo e Registro Elettronico).**
	Conflitti tra funzioni e confusione (anche operativa) dovuta a scarsa assunzione di responsabilità/definizione non puntuale delle responsabilità di ciascuna figura.	I controlli rilevati non risultano pienamente efficaci nel prevenire il rischio individuato.	Media	Tutte le funzioni del ciclo	**Attività di sensibilizzazione sul nuovo assetto organizzativo dell'Ente a tutto il personale. Formalizzazione e condivisione di ruoli e funzioni con l'organizzazione Verificare che la definizione dei ruoli e delle responsabilità sia formalizzata e adeguatamente condivisa/comunicata a tutti gli operatori.**

					Chiusura a chiave degli armadi dove sono archiviati dati personali e/o sensibili di qualsiasi natura (utenti, dipendenti, candidati,...).
Rispetto Privacy	Diffusione non autorizzata di dati personali/sensibili relativi agli alunni, anche quando trattati tramite mezzi informatici (es. e-mail, server,...) e/o tramite Registro elettronico	Modalità di archiviazione non sufficienti a presidiare il rischio individuato.	Bassa	Tutte le funzioni del ciclo	**Utilizzo Sistema Informativo interno e del registro elettronico con accessi personalizzati: prevedere la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password).** **Il sistema della tutela dell'Ente sulla Privacy (adottato dall'Ente in seguito alla normativa Europea - GDPR) migliora ulteriormente questo GAP**
	Raccolta di dati personali delle "modelle"per attività didattica, senza raccolta autorizzazione al trattamento dei dati.	Nessuna attività di controllo rilevata a presidio del rischio indicato.	Media	Alunni e docenti di laboratorio	**Predisposta e correttamente comunicata un'informativa sul trattamento dei dati personali raccolti a scopo didattico, da sottoporre solo una volta alle "modelle".** **Tale informativa sottoscritta dall'interessata viene raccolta e archiviata a cura del docente di estetica.**
Rispetto SGQ	Ritardi nella compilazione dei moduli o, più in generale, nell'applicazione del SGQ (con particolre riferimento alla tenuta e consegna della documentazione a supporto delle attività svolte).	Il SGQ adottato risulta poco interiorizzato dagli operatori, alcuni dei quali ignorano l'esistenza di un sistema di rendicontazione.	Alta	Tutte le funzioni del ciclo	**Formalizzazione all'interno del proprio SGQ di un'apposita procedura riguardante la Rendicontazione dei progetti finanziati.** **Sensibilizzazione dei docenti circa l'importanza della rendicontazione e del ruolo che ha la corretta e puntuale tenuta dei documenti a supporto.** **Prevista a conclusione delle attività (in particolare per quelle legate a progetti finanziati) una check list di verifica della relativa documentazione (effettuando un controllo sulla presenza del documento e un controllo sulla completezza/corretta tenuta del documento). Tale controllo potrà essere effettuato dalla Segreteria didattica in coordinamento con amministrazione e responsabili di area.** **A seguito del controllo la documentazione non dovrà più essere liberamente accessibile agli operatori.**
Frode informatica	Inserimento nei sistemi Regionali e Provinciali di dati non reali al fine di ottenere un maggior numero di finanziamenti o far risultare requisiti non posseduti.	I sistemi di controllo applicati in passato non risultavano pienamente idonei a prevenire il rischio individuato.	Media	Responsabile Segreteria didattica e Responsabili d'Area	**Utilizzo Sistema Informativo interno:** **prevista la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password).** **SI regionali/provinciali:** **identificate e comunicate responsabilità in capo a chi opera coi SI regionali e provinciali. Laddove possibile richiedere e fornire possibilità di accesso a detti sistemi con differenti profilazioni a seconda delle attività da svolgere.** **Previsto inoltre un controllo da parte di un adeguato livello aziendale sulle attività svolte dall'utente (monitoraggio dei login e dei dati inseriti).**

Truffa in danno dello Stato o di altro ente pubblico	Si commette il reato di truffa in danno dello Stato o di altro ente pubblico e malversazione di erogazioni pubbliche nel momento in cui, in fase di rendicontazione delle attività svolte, il responsabile amministrativo dichiara il falso, modificando fraudolentemente i dati del corso di formazione, oppure il docente riporta dati non corretti nel registro elettronico, procurando per sé o altri un ingiusto profitto con altrui danno.	Possibilità di alterazione dei dati dei registri utilizzati nei rapporti con la PA (registri scolastici, rendicontazione finanziamenti, selezione, appalti, ecc.)	Media	Direttore, Responsabili d'Area, Docenti	**Utilizzo Sistema Informativo interno: prevista la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password).** **SI regionali/provinciali: identificate e comunicate responsabilità in capo a chi opera coi SI regionali e provinciali. Laddove possibile richiedere e fornire possibilità di accesso a detti sistemi con differenti profilazioni a seconda delle attività da svolgere. Previsto inoltre un controllo da parte di un adeguato livello aziendale sulle attività svolte dall'utente (monitoraggio dei login e dei dati inseriti).**
Corruzione		I controlli rilevati risultano efficaci, anche se non pienamente conosciuti dagli operatori.	Bassa (accettabile)	Direttore, Responsabili d'Area	**A seguito di ciascun incontro con rappresentanti della Pubblica Amministrazione viene richiesta la comunicazione via e-mail di un report che evidenzi gli esiti dell'incontro da destinare al proprio responsabile. Il Direttore invia la medesima informativa al Presidente e (quando necessario) anche al Vice Direttore per opportuna informazione.**
Concussione	A seguito della commissione dei precedente reato, l'Ente ottiene una indebita percezione di erogazioni a danno dello Stato.				
Spendita denaro falso ricevuto in buona fede	Ricevere pagamenti (sala/bar, laboratorio estetica e laboratorio acconciatura) in contanti con monete/banconote false non individuate e poi utilizzate.	I sistemi di controllo applicati in passato non risultavano pienamente idonei a prevenire il rischio individuato.	Bassa (accettabile in seguito ad intervento)	Modelle, utenti bar e esterni in caso di eventi, docenti.	**Fornito alle aree interessate da movimenti in contanti (ad es. bar e uff. amministrazione) un rilevatore di banconote false.**
Ostacolo all'esercizio delle attività di controllo, revisione e delle funzioni delle autorità pubbliche di vigilanza	Alterazione dei dati richiesti durante i controlli ispettivi (ad es. facendo figurare come svolte attività non effettivamente svolte)..	I sistemi di controllo sulla corretta tenuta della documentazione a supporto delle attività svolte non prevengono pienamente il rischio individuato.	Medio-Alta	Direzione, Vice Direzione, Amministrazione, Segreteria, Resp. Area	**Formalizzazione all'interno del proprio SGQ di un'apposita procedura riguardante la Rendicontazione dei progetti finanziati.** **Sensibilizzazione dei docenti circa l'importanza della rendicontazione e del ruolo che ha la corretta e puntuale tenuta dei documenti a supporto.** **Prevista a conclusione delle attività (in particolare per quelle legate a progetti finanziati) una check list di verifica della relativa documentazione (effettuando un controllo sulla presenza del documento e un controllo sulla completezza/corretta tenuta del documento). Tale controllo potrà essere effettuato dalla Segreteria didattica in coordinamento con amministrazione e responsabili di area. A seguito del controllo la documentazione non dovrà più essere liberamente accessibile agli operatori.**
Corruzione tra privati	I reati di cui agli artt. 2635 e 2635-bis c.c. potrebbero essere commessi qualora esponenti dell'Ente ricevessero somme di denaro al fine di rilasciare attestati di formazione in assenza dei requisiti e delle condizioni previste dalle procedure vigenti.	Comportamenti illeciti personali	Media	Direzione, Vice Direzione, Amministrazione, Segreteria, Resp. Area	**Diffusione del PTCPT e massima condivisione del processo decisionale, puntuale rendicontazione delle attività di vigilanza e controllo**

Riduzione o mantenimento in schiavitù o servitù	Alterazione dei rapporti tra colleghi a seguito di situazioni di conflitto operativo/ideologico.	Non sono stati rilevate attività di controllo a presidio del rischio individuato	Alta (diventa media)	Personale dipendente	**A chiusura del processo riorganizzativo, prevedere una raccolta di feedback da parte degli operatori. Valutare un'azione di analisi del clima lavorativo in diverse aree aziendali.**
	Alterazione rapporto docente/alunno finalizzato all'ottenimento di vantaggi per entrambi.	I sistemi di controllo rilevati non risultano pienamente idonei a prevenire il rischio individuato.	Media (accettabile)	Alunni, tutor e docenti.	**Evidenziato in ogni contratto predisposto con docenti un richiamo al rispetto del Codice Etico dell'Ente e relativa clausola espressa di rescissione del contratto.**
Lesioni colpose	Utilizzo incauto di attrezzature, strumenti, prodotti utilizzati nelle attività di laboratorio.	Nessun GAP rilevato.	Bassa	Alunni e docenti di laboratorio	**Sensibilizzazione degli alunni da parte dei docenti sulle tematiche inerenti l'utilizzo in sicurezza di macchinari, attrezzature e prodotti potenzialmente pericolosi.** **Predisposizione e diffuzione del "Regolamento di Laboratorio" per ciascun Laboratorio**
Omicidio colposo	Utilizzo incauto di attrezzature, strumenti, prodotti utilizzati nelle attività di laboratorio.	Nessun GAP rilevato.	Bassa	Alunni e docenti di laboratorio	**Sensibilizzazione degli alunni da parte dei docenti sulle tematiche inerenti l'utilizzo in sicurezza di macchinari, attrezzature e prodotti potenzialmente pericolosi.** **Predisposizione e diffuzione del "Regolamento di Laboratorio"**
Inquinamento ambientale e delitti colposi contro l'ambiente	Scorretto smaltimento degli oli usausti delle cucine	Nessun GAP rilevato.	Bassa	Tutte le figure operanti nel ciclio	**Formalizzazione di un contratto per lo smaltimento degli olii esausti e procedure operative**
Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa	Diffondere, durante attività formative/eventi, organizzati dall'ente, idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istigare a commettere o commettere atti di discriminazione per motivi razziali, etnici, nazionali o religiosi. Ed ancora, promuovere, durante attività formative/eventi, organizzati dall'ente, lo sviluppo di organizzazioni, associazioni, movimenti o gruppi che abbiano tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi	Nessun GAP rilevato.	Bassa	Direttore, Responsabili d'Area, Tutor, Docenti	**Sensibilizzazione del personale**

Vendita di sostanze alimentari non genuine come genuine	Durante servizi di catering, possibile utilizzo di sostanze alimentari scadute o mal conservate (ad es. mancato rispetto della catena del freddo).	Nessun GAP rilevato.	-	Alunni docenti laboratorio alimentazione	
Riproduzione abusiva e diffusione (anche parziale) di opera dell'ingegno protetta	Distribuzione e utilizzo di testi fotocopiati oltre il limite previsto per legge.	Nessun GAP rilevato.	-	Docenti e tutor	-
Frode Informatica	Potenziale alterazione del funzionamento di un sistema informatico o telematico della pubblica amministrazione, o potenziale accesso (senza averne diritto o formale autorizzazione) a dati, informazioni, programmi informatici o telematici al fine di ottenere finanziamenti più alti.	Possibilità di accesso di personale non autorizzato alla sala server; possibilità di installazione di software malevoli e/o non autoirzzati da parte degli utenti sulle proprie macchine; dischi di backup vulnerabili e a rischio di perdita di dati	Medio-Alta	Tutte le figure del ciclo.	**ARCHIVI FISICI: Introdurre registro per gli accessi alla sala ced. introdurre sistema di spegnimento automatizzato e sicuro dell'infrastruttura server in caso di prolungata assenza di corrente. ANTIMALWARE: integrare la esistente con la parte di Cyber Secuirty per essere aggiornati sulle nuove minacce. AUTENTICAZIONE: definire il passaggio al nuovo sistema di posta con entrambi i domini ed attivare una password policy efficace e doppio fattore di autenticazione (MFA). Rafforzare la password policy attiva aumentando i caratteri delle password portandoli almeno a 12, aumentare la history delle password almeno a 15/20, inserire blocco degli account dopo 10 tentativi sbagliati (può andare bene anche un bocco temporizzato). SISTEMA DI AUTORIZZAZIONE: Rendere gli utenti delle postazioni di lavoro non amministratori della propria macchina se possibile così da diminuire la possibilità di installazione di software malevolo e/o non autorizzato. BACKUP E DISASTER RECOVERY: Valutare il Backup in cloud o immutabile in sostituzione del backup su dischi usb. INFRASTRUTTURA DI NETWORKING: Ridondare i dispositivi critici di rete principali come switch e firewall. RACCOLTA DI LOG E MONITORAGGIO: introdurre sistema di monitoraggio dei server e servizi di rete principali; introdurre sistema di raccolta log ADS.**
Accesso abusivo a sistema informatico e danneggiamento di informazioni, dati, programmi e sistemi informatici, anche dello Stato o altro ente pubblico o comunque di pubblico interesse	Accesso di utenti non autorizzati a sistemi aziendali protetti da misure di sicurezza (es.: sistemi interbancari). Utilizzo abusivo di password di accesso a siti di soggetti terzi, pubblici o privati, al fine di acquisire informazioni riservate e conseguire vantaggi competitivi. Accesso a una postazione PC, a sistemi di gestione aziendali, a sistemi telematici (anche della Pubblica amministrazione) con password diverse dalle proprie o senza autorizzazione specifica, con codici di accesso ottenuti violando le regole stabilite dalle policy e procedure aziendali. Detenzione abusiva di codici di accesso a sistemi informatici dell'Amministrazione giudiziaria o finanziaria, al fine di acquisire informazioni riservate su procedimenti penali/amministrativi che coinvolgano la Società. Manomissione del sistema di sorveglianza interno al fine di cancellare le registrazioni di un incidente avvenuto ai danni di un lavoratore memorizzate sul dispositivo. Assenza o inadeguatezza di un sistema di protezione dei dati e di un costante monitoraggio dei dati all'interno della rete.				

UNI EN ISO 9001:2015
(EA 37, 38)
AGENZIA PER LA FORMAZIONE, L'ORIENTAMENTO E IL LAVORO DELLA PROVINCIA DI COMO
CENTRO DI FORMAZIONE PROFESSIONALE
dedicato a "Luigi Grisoni"
COMO Monteolimpino via Bellinzona, 88 tel. 031/571055 - 574000 fax 575047
C.F. 95092770130 P.Iva 03095420133 e-mail: info@cfpcomo.com www.cfpcomo.com

MAPPATURA ATTIVITA

CICLO AZIENDALE:	***Orientamento/Lavoro***
RESPONSABILE	***Resp Area Progettazione, Orientamento/Lavoro***

ATTIVITA SVOLTE	DESCRIZIONE	FUNZIONI COINVOLTE
ANALISI E RELAZIONI CON IL TERRITORIO	Analisi delle opportunità offerte dai diversi Bandi/Avvisi (provinciali, regionali, nazionali e UE) dei fabbisogni specifici espressi dai diversi committenti pubblici e privati abbinata allo studio dei fabbisogni di orientamento/lavoro in ambito territoriale attraverso le informazioni recepite da: -relazioni con il sistema istituzionale e sociale locale; -relazioni con il sistema produttivo.Attività di promozione dell'attività dell'Agenzia presso destinatari istituzionali e del mondo produttivo	**DIRETTORE** **VICEDIRETTORE - RESPONSABILE AREA PROGETTAZIONE ORIENTAMENTO/LAVORO** **RESPONSABILE AREA FORMAZIONE (DDIF, APPRENDISTATO, DUALE)**
GESTIONE BUDGET DI PROGETTO	Gestione dei budget di progetto in base ai diversi interventi proposti, in collaborazione con la Direzione e il Responsabile amministrativo dell'Agenzia.	**DIRETTORE** **VICEDIRETTORE - RESPONSABILE AREA PROGETTAZIONE ORIENTAMENTO/LAVORO** **RESPONSABILE AMMINISTRATIVO**
PROGETTAZIONE	Sulla base degli indirizzi del Piano Programma il responsabile di area procede all'elaborazione dei singoli progetti (secondo vincoli e risorse dei singoli dispositivi e/o contratti di servizio). Ogni singolo progetto viene sottoposto al riesame della Direzione e ad una verifica formale prima della presentazione. I Responsabili dell'Area PROGETTAZIONE, ORIENTAMENTO/LAVORO, FORMAZIONE (DDIF, APPRENDISTATO, DUALE), prima dell'attivazione del progetto, effettuano i necessari controlli per l'accertamento dei requisiti richiesti dai singoli bandi di riferimento. Ciascun Responsabile individua dunque le risorse e le modalità organizzative necessarie alla realizzazione dei progetti/corsi assegnati.	**DIRETTORE** **VICEDIRETTORE - RESPONSABILE AREA PROGETTAZIONE ORIENTAMENTO/LAVORO** **RESPONSABILE AREA FORMAZIONE (DDIF, APPRENDISTATO, DUALE)**
EROGAZIONE	Il processo di erogazione del servizio orientamento/lavoro prevede le seguenti tipologie di servizio (MQ capitolo quinto): -Servizi orientativi di base; -Servizi orientativi specialistici; -Accompagnamento e sostegno al lavoro; -Formazioni individuale o di gruppo (tra cui attività di tirocinio internazionale); Attività formative; Azioni di sistema (innovazione, partnerariato strategico, eventi)	**VICEDIRETTORE - RESPONSABILE AREA ORIENTAMENTO/LAVORO,** **RESPONSABILE AREA FORMAZIONE (DDIF, APPRENDISTATO, DUALE)** **TUTOR** **DOCENTI**
CONCLUSIONE E RENDICONTAZIONE	Vengono svolti, in ogni fase dell'erogazione del servizio, controlli sull'idoneità delle aule/laboratori e strumenti didattici e sui partecipanti (selezione e verifica dei requisiti ecc....). La rintracciabilità del servizio portato a termine è garantito dalla tenuta dei documenti di supporto (registri, calendari, questionari, ecc...) in ogni fase dell'erogazione. I dati vengono registrati elettronicamente sui portali previsti dai dispositivi di finanziamento. Tutta la documentazione a supporto permette di ripercorrere a ritroso l'iter progettuale al fine di evidenziare eventuali criticità sopraggiunte durante l'erogazione del servizio e costituisce il punto di partenza per il processo di rendicontazione.	**VICEDIRETTORE - RESPONSABILE AREA ORIENTAMENTO/LAVORO,** **RESPONSABILE AREA FORMAZIONE (DDIF, APPRENDISTATO, DUALE)** **TUTOR** **DOCENTI**
GESTIONE DEI SISTEMI INFORMATIVI - ANTIMALWARE	L'azienda si è dotata di vari sistemi di sicurezza per contrastare i malware; per la parte client server è installato l'antivirus Eset, l'antivirus comprende servizi di antiransomware, application control e webfiltering, la gestione è centralizzata su console cloud gestita da cierre. A Protezione dell'infrastruttura è presente un firewall zyxell usg300 (in fase sdi aggiornamento, il prodotto è a fine vita) con servizi attivi di content filtering e antivirus. I servizi mail sono divisi in due parti una parte on premise su server mdeamon che comprende anche un antivirus interno per la parte amministrativa con dominio cfpcomo.com; la parte didattica invece è configurata su servizi google apps con il dominio cfpcomo.education.com i sistemi di sicurezza sono proprietari di google. All'interno dell'infrastruttura non è presente un sistema di gestione delle patch di sicurezza, per la parte client i pc si aggiornano automaticamente e gli utenti decidono quando installare gli updates, per la parte server sono automatizzati. Il firewall si aggiorna ogni settimana in modo automatico, per gli altri apparati di rete come siwtch, access point, nas ecc. gli aggiornamenti sono manuali e non programmati. L'aggiornamento firmware dei server viene svolto all'occorrenza. I collaboratori sono formati e informati sull'utilizzo degli asset, viene svolta formazione attiva durante l'anno, le procedure d'utilizzo risultano documentate. Presente regolamento informatico con procedure documentate a disposizione degli incaricati e degli ADS.	**TUTTE LE FUNZIONI DEL CICLO**

GESTIONE DEI SISTEMI INFORMATIVI - AUTENTICAZIONE	"L'accesso ai Vari PC e SERVER è gestito da credenziali univoche, presente password policy con le seguenti caratteristiche: 8 caratteri comprensivi di caratteri speciali, scadenza password ogni 3 mesi, history standard, blocco account a seguito di multipli tentitivi d'accesso falliti non attivo. Sono presente due domini separati uno utilizzato dalla parte amministrativa e uno per la parte di didattica. La revisione degli accessi viene svolta all'occorrenza in corrispondenza dell'off-boarding di un utente. Le Password della posta elettronica non scadono, non è presente MFA. L'accesso al gestionale amministrativo/didattica/magazzino e personale esterno avviene con la stessa password dell'utente di dominio. L'accesso al portale zucchetti per visualizzare le timbrature, richiesta permessi ecc. è gestito con credenziali univoche per ogni utente, la password scade regolarmente tramite procedura automatizzata, il personale interno ha l'accesso amministratore per gestire e forzare la scadenza password degli account."	**TUTTE LE FUNZIONI DEL CICLO**
GESTIONE DEI SISTEMI INFORMATIVI - SISTEMA DI AUTORIZZAZIONE	L'azienda usa i 2 server di dominio active directory di Microsoft per gestire le Autorizzazioni, uno per la parte amministrativa e uno per la parte Didattica. Non è presente procedura documentata di on-boarding e off-boarding, ma risulta esserci prassi consolidata tra la direzione e L'IT. (nella procedura di off-boarding e regolamento informatico sono specificati i dettagli della gestione degli account di dominio e e-mail) Presente riesame annuale degli accessi ai sistemi. Gli utenti sono amministratori della macchina.	**TUTTE LE FUNZIONI DEL CICLO**
GESTIONE DEI SISTEMI INFORMATIVI - BACKUP E DISASTER RECOVERY	Presente sistema di backup Veeam Backup & Replication che svolge il backup di tutte le macchine virtuali, i backup sono giornalieri e vengono svolti su NAS. È attivo un sistema di repliche gestito sempre da Veeam Backup & Replication, le repliche sono attive durante le ore di lavoroe vengono eseguite ogni ora. E' presente un backup aggiuntivo su disco USB che viene portato fuori sede, il disco viene cambiato ogni settimana da Denise, i backup su disco esterno sono Cifrati. I NAS sono presso la sala CED. È presente un Backup in cloud solo per la PEC istituzionale svolto su amazon S3. Presente procedura interna con la documentaizone dei backup e procedura di restore, manca procedura di disaster recovery. Durante l'anno sono stati fatti restore granulari all'occorrenza. Sono presenti alert di buon funzionamento.	**TUTTE LE FUNZIONI DEL CICLO**
GESTIONE DEI SISTEMI INFORMATIVI - INFRASTRUTTURA DI NETWORKING	Lq rete risulta segmentata, presente Vlan management e vlan backup. Presente rete wi-fi cfp_didattica che può essere utilizzata a fronte di registrazione del mac address del dispositivo e della password di accesso, la registrazione viene gestita da Moriani. La rete wifi è utilizzabile da chi ne fa richiesta, anche a titolo temporaneo come esterni che vengono ad operare al CFP per tempi contingentati. Il mac address viene registrato e poi rimosso al termine dell'attività. I dispositivi collegati a questa rete posson osolamente accedere alla parte relativa alla didattica su apposito server dedicato. La rete uffici amministrativi è separate da quella della Didattica, i sistemi di rete non sono ridondati, i server hanno la ridondanza con alimentatore, 'dischi e scheda di rete. Sono presenti servizi pubblicati tramite firewall drytek, come webmail di mdeamon e il sistema di videosorveglianza, il sistema di video sorveglianza è su una rete separata. Presente connettività dati che serve sia la parte di navigazione internet che la fonia, presente linea di backup con tecnologia wifi.	**TUTTE LE FUNZIONI DEL CICLO**
GESTIONE DEI SISTEMI INFOMRATIVI - RACCOLTA DI LOG E MONITORAGGIO	È in fase di introduzione un sistema di monitoraggio dei server e dei servizi di rete principali, nonché di un sistema di raccolta log ADS.	**TUTTE LE FUNZIONI DEL CICLO**

CICLO AZIENDALE:	Progettazione, Orientamento/Lavoro	
#	SEZIONI NUOVE DOPO AGGIORNAMENTO REATI PRESUPPOSTO 2024	CHECK
1	Violazioni del Codice Etico aziendale	Y
2	Reati in danno alla Pubblica Amministrazione	Y
3	Delitti informatici e trattamento illecito di dati	Y
4	Delitti di criminalità organizzata	N/A
5	Reati in tema di falsità in moneta, carte di pubblico credito, valori di bollo e strumenti o segni di riconoscimento	N/A
6	Delitti contro l'industria e il commercio	N/A
7	Reati societari	Y
10	Delitti contro la personalità individuale	N/A
13	Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro	N/A
14	Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio	N/A
15	Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori	N/A
16	Altre fattispecie in materia di strumenti di pagamento diversi dai contanti	N/A
17	Delitti in materia di violazione del diritto d'autore	Y
18	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	N/A
19	Reati ambientali	Y
20	Impiego di cittadini di paesi terzi il cui soggiorno è irregolare	N/A
21	Razzismo e xenofobia	Y

Ciclo Orientamento e Lavoro – Risk Control Matrix

CICLO AZIENDALE:	Progettazione - Orientamento/Lavoro					
RISK CONTROL MATRIX						
SEZIONE PRIMA: Comportamenti non conformi al Codice Etico aziendale						
VIOLAZIONE	**DESCRIZIONE PRINCIPIO DI RIFERIMENTO**	**CONDOTTA ERRATA**	**PROBABILITA**	**IMPATTO**	**VALUTAZIONE**	**FUNZIONI COINVOLTE**
Legalità	*l'AZIENDA si impegna a rispettare, nello svolgimento di tutte le proprie attività, le leggi internazionali, nazionali e regionali in vigore in Italia e in ciascun Paese nel quale opera anche tramite branch locali.*	Comunicazione di dati falsificati per ottenere vantaggi personali o per l'ente (ad es. ore presenza, attività svolte) e conseguente inserimento dei dati a sistema senza consapevolezza della responsabilità operativa personale.	**0,5**	**0,9**	Rilevante	Tutte le funzioni coinvolte nella gestione del Sistema Dote
Trasparenza	*l'AZIENDA impronta i rapporti di qualsiasi natura e verso qualsiasi stakeholder alla chiarezza delle intenzioni e all'assenza di volontà di occultamento, rispettando al contempo gli obblighi derivanti dalla normativa vigente in materia di trattamento dei dati riservati.*	Utilizzo di profili informatici di altri per svolgere attività a sistema. Mancanza di segnalazioni di situazioni in cui si rende necessario l'intervento di altri per sanare ritardi/mancanze.	**0,8**	**0,3**	Rilevante	Tutte le funzioni dell'Ente
Rispetto Privacy	*trattamento di dati personali e dati sensibili nel rispetto della normativa vigente.*	Scorretta archiviazione dei dati e possibile conseguente diffusione degli stessi a persone non autorizzate.	**0,2**	**0,5**	Accettabile	Tutte le funzioni del ciclo.
Rispetto SGQ	*svolgimento delle attività regolamentate dal Sistema di Gestione della Qualità, adottato dall'azienda, nel pieno rispetto della politica per la Qualità aziendale, delle relative procedure e delle eventuali istruzioni operative applicabili.*	Adempimenti richiesti confliggono/si sovrappongono a quanto richiesto dalla normativa vigente applicata alle attività del ciclo.	**0,6**	**0,2**	Accettabile	Tutte le funzioni del ciclo.
Rispetto SGQ	*svolgimento delle attività regolamentate dal Sistema di Gestione della Qualità, adottato dall'azienda, nel pieno rispetto della politica per la Qualità aziendale, delle relative procedure e delle eventuali istruzioni operative applicabili.*	Mancata applicazione e/o ritardi negli adempimenti previsti dal SGQ.	**0,5**	**0,25**	Accettabile	Tutte le funzioni del ciclo.

CICLO AZIENDALE:	Progettazione - Orientamento/Lavoro					
RISK CONTROL MATRIX						
SEZIONE TERZA: Reati in danno alla Pubblica Amministrazione						
RISCHIO REATO	**RIFERIMENTI NORMATIVI**	**CONDOTTA ERRATA**	**PROBABILITA**	**IMPATTO**	**VALUTAZIONE**	**FUNZIONI COINVOLTE**
Frode informatica	*Art. 640-ter c.p.*	Inserimento di dati alterati per ottenere maggiori finanziamenti.	**0,5**	**0,2**	Accettabile	Tutte le funzioni che utilizzano GEFO Servizi/Sintesi.
Frode informatica	*Art. 640-ter c.p.*	Potenziale alterazione del funzionamento di un sistema informatico o telematico della pubblica amministrazione, o potenziale accesso (senza averne diritto o formale autorizzazione) a dati, informazioni, programmi informatici o telematici al fine di ottenere finanziamenti più alti.	**0,3**	**0,3**	Rilevante	Tutte le funzioni del ciclo
Truffa in danno dello Stato o di altro ente pubblico	*Art. 640, co. 2, n. 1, c.p.*	Si commette il reato di truffa in danno dello Stato o di altro ente pubblico e malversazione di erogazioni pubbliche nel momento in cui, in fase di rendicontazione delle attività svolte, il Responsabile dell'Area orientamento/Laovoro dichiara il falso, modificando fraudolentemente i dati del corso di formazione, procurando per sé o altri un ingiusto profitto con altrui danno. A seguito della commissione dei precedente reato, l'Ente ottiene una indebita percezione di erogazioni a danno dello Stato.	**0,3**	**0,3**	Rilevante	Vice-Direttore, Responsabili d'Area
Concussione	*Art. 317 c.p.*	Accordi illeciti con pubblici ufficiali volti all'ottenimento di benefici per l'ente.	**0,5**	**0,2**	Accettabile	Vice-Direttore, Responsabili d'Area
Corruzione	*Art. 318 c.p.* *Art. 319 c.p.* *Art. 319 bis c.p.* *Art. 319 ter c.p.* *Art. 320 c.p.* *Art. 321 c.p.* *Art. 322 c.p.*	Accordi illeciti con pubblici ufficiali volti all'ottenimento di benefici per l'ente.	**0,5**	**0,2**	Accettabile	Vide-Direttore, Responsabili d'Area

CICLO AZIENDALE: Progettazione - Orientamento/Lavoro

RISK CONTROL MATRIX

SEZIONE SETTIMA: Reati Societari

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Accesso abusivo a sistema informatico e danneggiamento di informazioni, dati, programmi e sistemi informatici, anche dello Stato o altro ente pubblico o comunque di pubblico interesse	*Art. 615-ter, 615-quater, 629, co. 3, 635-bis, 635-ter, 635-quater, 635-quater.1 c.p.*	Accesso di utenti non autorizzati a sistemi aziendali protetti da misure di sicurezza (es.: sistemi interbancari). Utilizzo abusivo di password di accesso a siti di soggetti terzi, pubblici o privati, al fine di acquisire informazioni riservate e conseguire vantaggi competitivi. Accesso a una postazione PC, a sistemi di gestione aziendali, a sistemi telematici (anche della Pubblica amministrazione) con password diverse dalle proprie o senza autorizzazione specifica, con codici di accesso ottenuti violando le regole stabilite dalle policy e procedure aziendali. Detenzione abusiva di codici di accesso a sistemi informatici dell'Amministrazione giudiziaria o finanziaria, al fine di acquisire informazioni riservate su procedimenti penali/amministrativi che coinvolgano la Società. Manomissione del sistema di sorveglianza interno al fine di cancellare le registrazioni di un incidente avvenuto ai danni di un lavoratore memorizzate sul dispositivo. Assenza o inadeguatezza di un sistema di protezione dei dati e di un costante monitoraggio dei dati all'interno della rete.	**0,3**	**0,3**	Rilevante	Tutte le funzioni del ciclo

CICLO AZIENDALE: Progettazione - Orientamento/Lavoro

RISK CONTROL MATRIX

SEZIONE SETTIMA: Reati Societari

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Ostacolo all'esercizio delle attività di controllo, revisione e delle funzioni delle autorità pubbliche di vigilanza	*Art. 2625 comma 2 c.c.* *Art. 2638 comma 1 e 2 c.c.*	Fornire documentazione falsa o alterata in qualsivoglia maniera (firme, presenze,...)	**0,7**	**0,2**	Accettabile	Tutte le funzioni coinvolte nell'erogazione dei servizi.

CICLO AZIENDALE: Progettazione - Orientamento/Lavoro

RISK CONTROL MATRIX

SEZIONE DICIASSETTESIMA: Delitti in materia di violazione del diritto d'autore

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Riproduzione abusiva e diffusione (anche parziale) di opera dell'ingegno protetta	*art.171-ter l. 633/1941*	Distribuzione e utilizzo di testi fotocopiati oltre il limite previsto per legge.	**0,1**	**0,7**	Accettabile	Docenti e tutor

CICLO AZIENDALE: gettazione - Orientamento/Lav

RISK CONTROL MATRIX

SEZIONE DICIANNOVESIMA: Reati ambientali

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Inquinamento ambientale e delitti colposi contro l'ambiente	*Art. 452-bis, 452-quinquies c.p.*	Scorretto smaltimento degli oli usausti delle cucine	**0,1**	**0,7**	Accettabile	Resp. Area, Direzione, Formazione, Sostegno

CICLO AZIENDALE:	Progettazione - Orientamento/Lavoro

RISK CONTROL MATRIX

SEZIONE VENTUNESIMA: Razzismo e xenofobia

RISCHIO REATO	*RIFERIMENTI NORMATIVI*	*CONDOTTA ERRATA*	*PROBABILITA*	*IMPATTO*	*VALUTAZIONE*	*FUNZIONI COINVOLTE*
Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa	*Art. 604-bis c.p.*	Diffondere, durante attività formative/eventi, organizzati dall'ente, idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istigare a commettere o commettere atti di discriminazione per motivi razziali, etnici, nazionali o religiosi. Ed ancora, promuovere, durante attività formative/eventi, organizzati dall'ente, lo sviluppo di organizzazioni, associazioni, movimenti o gruppi che abbiano tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi	**0,3**	**0,3**	Rilevante	Direttore, Responsabili d'Area, Tutor, Docenti

Gap Analysis e Piano di Azione

CICLO AZIENDALE: PROGETTAZIONE/ORIENTAMENTO/LAVORO

Rischio	Descrizione Rischio	Descrizione GAP	Priorità	Funzioni coinvolte	Action Plan
Legalità	Comunicazione di dati falsificati per ottenere vantaggi personali o per l'ente (ad es. ore presenza, attività svolte) e conseguente inserimento dei dati a sistema senza consapevolezza della responsabilità operativa personale.	I sistemi di controllo applicati risultano parzialmente idonei a prevenire il rischio individuato.	Media	Tutte le funzioni coinvolte nella gestione del Sistema Dote	**Attività di sensibilizzazione svolta sul nuovo assetto organizzativo dell'Ente a tutto il personale. Verificare che definizione dei ruoli e delle responsabilità sia formalizzata e adeguatamente condivisa/comunicata a tutti gli operatori. Utilizzo Sistema Informativo interno: prevista la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password). SI regionali/provinciali: identificate e comunicate responsabilità in capo a chi opera coi SI regionali e provinciali. Laddove possibile richiedere e fornire possibilità di accesso a detti sistemi con differenti profilazioni a seconda delle attività da svolgere. Previsto inoltre un controllo da parte di un adeguato livello aziendale sulle attività svolte dall'utente (monitoraggio dei login e dei dati inseriti).**
Trasparenza	Utilizzo di profili informatici di altri per svolgere attività a sistema. Mancanza di segnalazioni di situazioni in cui si rende necessario l'intervento di altri per sanare ritardi/mancanze.	I sistemi di controllo applicati risultano parzialmente idonei a prevenire il rischio individuato.	Media	Tutte le funzioni dell'Ente	**Attività di sensibilizzazione svolta sul nuovo assetto organizzativo dell'Ente a tutto il personale. Verificare che definizione dei ruoli e delle responsabilità sia formalizzata e adeguatamente condivisa/comunicata a tutti gli operatori. Utilizzo Sistema Informativo interno: prevista la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password).**
Rispetto Privacy	Scorretta archiviazione dei dati e possibile conseguente diffusione degli stessi a persone non autorizzate.	Modalità di archiviazione non totalmente sufficienti a presidiare il rischio individuato.	Bassa (Accettabile)	Tutte le funzioni del ciclo.	**Chiusura a chiave degli armadi dove sono archiviati dati personali e/o sensibili di qualsiasi natura (utenti, dipendenti, candidati). Accesso consentito solo previa autorizzazione del Vicedirettore (Resp. Area Progettazione - Orientamento/Lavoro) Il sistema della tutela dell'Ente sulla Privacy (adottato dall'Ente in seguito alla normativa Europea - GDPR) migliora ulteriormente questo GAP**
Rispetto SGQ	Adempimenti richiesti confliggono/si sovrappongono a quanto richiesto dalla normativa vigente applicata alle attività del ciclo.	Nessun GAP rilevato	-	Tutte le funzioni del ciclo.	-
	Mancata applicazione e/o ritardi negli adempimenti previsti dal SGQ.	Il SGQ adottato risulta non pienamente interiorizzato dagli operatori	Media	Tutte le funzioni del ciclo.	**Impostata e svolta attività di sensibilizzazione sulle Procedure, raccogliendo feedback operativi da parte di chi è chiamato ad applicare il SGQ. Sulla base di tali feedback andranno valutate eventuali revisioni future. Adottata check-list al fine di verificare le attività e i controlli sui Responsabili d'Area in merito ai progetti/corsi finanziati**

					Utilizzo Sistema Informativo interno: prevista la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password).
Frode Informatica	Inserimento di dati alterati per ottenere maggiori finanziamenti.	I sistemi di controllo applicati non risultano pienamente idonei a prevenire il rischio individuato.	Media	Tutte le funzioni che utilizzano GEFO Servizi/Sintesi.	**SI regionali/provinciali (GEFO Servizi/Sintesi):** **identificate e comunicate responsabilità in capo a chi opera coi SI regionali e provinciali. Laddove possibile richiedere e fornire possibilità di accesso a detti sistemi con differenti profilazioni a seconda delle attività da svolgere.** **Previsto inoltre un controllo da parte di un adeguato livello aziendale sulle attività svolte dall'utente (monitoraggio dei login e dei dati inseriti).**
Truffa in danno dello Stato o di altro ente pubblico	Si commette il reato di truffa in danno dello Stato o di altro ente pubblico e malversazione di erogazioni pubbliche nel momento in cui, in fase di rendicontazione delle attività svolte, il Responsabile dell'Area orientamento/Laovoro dichiara il falso, modificando fraudolentemente i dati del corso di formazione, procurando per sé o altri un ingiusto profitto con altrui danno. A seguito della commissione dei precedente reato, l'Ente ottiene una indebita percezione di erogazioni a danno dello Stato.	Possibilità di alterazione dei dati dei registri utilizzati nei rapporti con la PA (registri scolastici, rendicontazione finanziamenti, selezione, appalti, ecc.)	Media	Vice-Direttore, Responsabili d'Area	**Utilizzo Sistema Informativo interno: prevista la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password).** **SI regionali/provinciali: identificate e comunicate responsabilità in capo a chi opera coi SI regionali e provinciali. Laddove possibile richiedere e fornire possibilità di accesso a detti sistemi con differenti profilazioni a seconda delle attività da svolgere.** **Previsto inoltre un controllo da parte di un adeguato livello aziendale sulle attività svolte dall'utente (monitoraggio dei login e dei dati inseriti).**
Concussione	Accordi illeciti con pubblici ufficiali volti all'ottenimento di benefici per l'ente.	I controlli rilevati risultano efficaci, anche se non pienamente conosciuti dagli operatori.	Bassa (Accettabile)	Vice-Direttore, Responsabili d'Area	**A seguito di ciascun incontro con rappresentanti della Pubblica Amministrazione viene richiesta la comunicazione via e-mail di un report che evidenzi gli esiti dell'incontro da destinare al proprio responsabile. Il Direttore invia la medesima informativa al Presidente e (quando necessario) anche al Vice Direttore per opportuna informazione.**
Corruzione	Accordi illeciti con pubblici ufficiali volti all'ottenimento di benefici per l'ente.	I controlli rilevati risultano efficaci, anche se non pienamente conosciuti dagli operatori.	Bassa (Accettabile)	Vice-Direttore, Responsabili d'Area	**A seguito di ciascun incontro con rappresentanti della Pubblica Amministrazione viene richiesta la comunicazione via e-mail di un report che evidenzi gli esiti dell'incontro da destinare al proprio responsabile. Il Direttore invia la medesima informativa al Presidente e (quando necessario) anche al Vice Direttore per opportuna informazione.**
Ostacolo all'esercizio delle attività di controllo, revisione e delle funzioni delle autorità pubbliche di vigilanza	Fornire documentazione falsa o alterata in qualsivoglia maniera (firme, presenze,…)	I sistemi di controllo sulla corretta tenuta della documentazione a supporto delle attività svolte non prevengono pienamente il rischio individuato.	Media	Tutte le funzioni coinvolte nell'erogazione dei servizi.	**Formalizzazione all'interno del proprio SGQ di un'apposita procedura riguardante la Rendicontazione dei progetti finanziati.** **Sensibilizzazione dei docenti circa l'importanza della rendicontazione e del ruolo che ha la corretta e puntuale tenuta dei documenti a supporto.** **Prevista a conclusione delle attività (in particolare per quelle legate a progetti finanziati) una check list di verifica della relativa documentazione (effettuando un controllo sulla presenza del documento e un controllo sulla completezza/corretta tenuta del documento). Tale controllo potrà essere effettuato dalla Segreteria didattica in coordinamento con amministrazione e responsabili di area.** **A seguito del controllo la documentazione non dovrà più essere liberamente accessibile agli operatori.**
Riproduzione abusiva e diffusione (anche parziale) di opera dell'ingegno protetta	Distribuzione e utilizzo di testi fotocopiati oltre il limite previsto per legge.	Nessun GAP rilevato	Bassa (Accettabile)	Docenti e tutor	**Sensibilizzazione del personale**

Inquinamento ambientale e delitti colposi contro l'ambiente	Scorretto smaltimento degli oli usausti delle cucine	Nessun GAP rilevato	Bassa (Accettabile)	Tutte le figure operanti nel ciclo	**Formalizzazione di un contratto per lo smaltimento degli olii esausti e procedure operative**
Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa	Diffondere, durante attività formative/eventi, organizzati dall'ente, idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istigare a commettere o commettere atti di discriminazione per motivi razziali, etnici, nazionali o religiosi. Ed ancora, promuovere, durante attività formative/eventi, organizzati dall'ente, lo sviluppo di organizzazioni, associazioni, movimenti o gruppi che abbiano tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi	Nessun GAP rilevato	Bassa (Accettabile)	Direttore, Responsabili d'Area, Tutor, Docenti	**Sensibilizzazione del personale**
Frode Informatica	Potenziale alterazione del funzionamento di un sistema informatico o telematico della pubblica amministrazione, o potenziale accesso (senza averne diritto o formale autorizzazione) a dati, informazioni, programmi informatici o telematici al fine di ottenere finanziamenti più alti.	Possibilità di accesso di personale non autorizzato alla sala server; possibilità di installazione di software malevoli e/o non autoirzzati da parte degli utenti sulle proprie macchine; dischi di backup vulnerabili e a rischio di perdita di dati	Medio-Alta	Tutte le figure del ciclo.	**ARCHIVI FISICI: Introdurre registro per gli accessi alla sala ced. introdurre sistema di spegnimento automatizzato e sicuro dell'infrastruttura server in caso di prolungata assenza di corrente. ANTIMALWARE: integrare la esistente con la parte di Cyber Secuirty per essere aggiornati sulle nuove minacce. AUTENTICAZIONE: definire il passaggio al nuovo sistema di posta con entrambi i domini ed attivare una password policy efficace e doppio fattore di autenticazione (MFA). Rafforzare la password policy attiva aumentando i caratteri delle password portandoli almeno a 12, aumentare la history delle password almeno a 15/20, inserire blocco degli account dopo 10 tentativi sbagliati (può andare bene anche un bocco temporizzato). SISTEMA DI AUTORIZZAZIONE: Rendere gli utenti delle postazioni di lavoro non amministratori della propria macchina se possibile così da diminuire la possibilità di installazione di software malevolo e/o non autorizzato. BACKUP E DISASTER RECOVERY: Valutare il Backup in cloud o immutabile in sostituzione del backup su dischi usb. INFRASTRUTTURA DI NETWORKING: Ridondare i dispositivi critici di rete principali come switch e firewall. RACCOLTA DI LOG E MONITORAGGIO: introdurre sistema di monitoraggio dei server e servizi di rete principali; introdurre sistema di raccolta log ADS.**
Accesso abusivo a sistema informatico e danneggiamento di informazioni, dati, programmi e sistemi informatici, anche dello Stato o altro ente pubblico o comunque di pubblico interesse	Accesso di utenti non autorizzati a sistemi aziendali protetti da misure di sicurezza (es.: sistemi interbancari). Utilizzo abusivo di password di accesso a siti di soggetti terzi, pubblici o privati, al fine di acquisire informazioni riservate e conseguire vantaggi competitivi. Accesso a una postazione PC, a sistemi di gestione aziendali, a sistemi telematici (anche della Pubblica amministrazione) con password diverse dalle proprie o senza autorizzazione specifica, con codici di accesso ottenuti violando le regole stabilite dalle policy e procedure aziendali. Detenzione abusiva di codici di accesso a sistemi informatici dell'Amministrazione giudiziaria o finanziaria, al fine di acquisire informazioni riservate su procedimenti penali/amministrativi che coinvolgano la Società. Manomissione del sistema di sorveglianza interno al fine di cancellare le registrazioni di un incidente avvenuto ai danni di un lavoratore memorizzate sul dispositivo. Assenza o inadeguatezza di un sistema di protezione dei dati e di un costante monitoraggio dei dati all'interno della rete.				

Ciclo Segreteria – Mappatura

MAPPATURA ATTIVITA		
CICLO AZIENDALE:	***Segreteria***	
RESPONSABILE	***Resp di Segreteria***	
ATTIVITA SVOLTE	***DESCRIZIONE***	***FUNZIONI COINVOLTE***
PRIMA ACCOGLIENZA	La segreteria mette a disposizione degli utenti un servizio di prima accoglienza e di screening dell'utenza (i processi sono riportati nel MQ al capitolo quarto). La segreteria si relaziona direttamente con l'utenza per dare informazioni e favorire l'auto consultazione del materiale informativo nonchè offrire consulenza orientativa di primo livello. La segreteria collabora alla gestione dell'intero processo e supporta gli utenti nell'intero percorso fino alla consegna delle certificazioni (attestazioni, certificati di frequenza, ecc....) per le attività svolte.	**RESPONSABILE DI SEGRERTERIA GENERALE** **ACCOGLIENZA INFORMAZIONE LOGISTICA**
SEGRETERIA CORSI/PROGETTI	La segreteria generale raccoglie le iscrizioni ai corsi da parte dei clienti/utenti. Predispone i registri, i documenti e tutto il materiale necessario all'avvio e allo svolgimento di tutti i corsi e di tutte le attività che si svolgono presso l'Agenzia, compresa l'archiviazione dei materiali di tipo cartaceo/informatico, garantendone l'ordine e la reperibilità. Nell'adempimento dei compiti sopra citati si relaziona direttamente con le aree di formazione e di orientamento/lavoro.	**RESPONSABILE DI SEGRETERIA GENERALE** **RESPONSABILE AREA FORMAZIONE DDIF APPRENDISTATO, DUALE** **RESPONSABILE AREA PROGETTAZIONE, ORIENTAMENTO/LAVORO**
GESTIONE COMUNICAZIONI/ INFORMAZIONI/GESTIONE CANCELLERIA	La segreteria generale, in accordo con la Direzione, cura tutte le comunicazioni/informazioni in entrata e in uscita di tipo cartaceo/informatico, comprese le comunicazioni con le famiglie degli allievi. Consegna, avvalendosi dell'operatore tecnico ausiliario, informative, comunicazioni, materiale di cancelleria all'interno dell'Agenzia e verso gli utenti/clienti esterni.	**RESPONSABILE DI SEGRERTERIA GENERALE** **ACCOGLIENZA INFORMAZIONE LOGISTICA** **RESPONSABILE AREA FORMAZIONE DDIF APPRENDISTATO, DUALE** **DIRETTORE**
GESTIONE PROGETTI DDIF	Inserimento a sistema dell'anagrafica allievi (Portale Regionale SIUF) con i dati per l'avvio e la chiusura dei corsi in DDIF. Nell'ambito del SIUF viene inoltre curata la gestione del Registro Elettronico GRS, con invio quotidiano delle presenze degli allievi (che vengono registrate direttamente dai docenti). Inserimento a sistema (Portale BES) dei dati (ore e presenze) per richiedere i finanziamenti, nonchè per la relativa rendicontazione finale (ore e presenze).	**RESPONSABILE DI SEGRETERIA**
GESTIONE DEI SISTEMI INFORMATIVI - ARCHIVI FISICI	Lo stabile storico è situato a Como in via bellinzona 88, la struttura è delimitata esternamente da una muraglia con cancelli automatici chiusi L'ingresso principale è monitorato dalla Segreteria. La sala ced risiede al primo piano interrato, la porta d'accesso REI tagliafuoco risulta chiusa a chiave. L'accesso è monitorato da una telecamera di sorveglianza. La sala è utilizzata anche come magazzino di materiale informatico. Le chiavi della sala ced sono in segreteria, non presente un registro per gli accessi. All'interno della sala ced sono presenti due armadi rack, uno che ospita la parte server e l'altro per le apparecchiature di rete e fonia. Entrambi gli armadi sono protetti da un gruppo UPS per gestire gli sbalzi di tensione e interruzioni di corrente, l'Ups però non gestisce lo spegnimento automatizzato dei server. Attualmente non sono presenti sonde d'allarme, i server sono tarati per lo spegnimento in caso di alte temperature ma senza una procedura di sicurezza, sono presenti avvisi via mail ricevuti da cierre. La sala ced ha un sistema di raffrescamento interno. E' presente inventario degli asset interno gestito da Cierre che comprende hardware, software si tratta più che altro di un inventario operativo che di gestione Asset. Gli archivi cartacei sono stipati in Garage eterni sotto il parcheggio, gli archivi risultano chiusi a chiave le chiavi sono disponibiliti in segreteria.	**TUTTE LE FUNZIONI AZIENDALI DEL CICLO**

GESTIONE DEI SISTEMI INFORMATIVI - ANTIMALWARE	L'azienda si è dotata di vari sistemi di sicurezza per contrastare i malware; per la parte client server è installato l'antivirus Eset, l'antivirus comprende servizi di antiransomware, application control e webfiltering, la gestione è centralizzata su console cloud gestita da cierre. A Protezione dell'infrastruttura è presente un firewall zyxell usg300 (in fase sdi aggiornamento, il prodotto è a fine vita) con servizi attivi di content filtering e antivirus. I servizi mail sono divisi in due parti una parte on premise su server mdeamon che comprende anche un antivirus interno per la parte amministrativa con dominio cfpcomo.com; la parte didattica invece è configurata su servizi google apps con il dominio cfpcomo.education.com i sistemi di sicurezza sono proprietari di google. All'interno dell'infrastruttura non è presente un sistema di gestione delle patch di sicurezza, per la parte client i pc si aggiornano automaticamente e gli utenti decidono quando installare gli updates, per la parte server sono automatizzati. Il firewall si aggiorna ogni settimana in modo automatico, per gli altri apparati di rete come siwtch, access point, nas ecc. gli aggiornamenti sono manuali e non programmati. L'aggiornamento firmware dei server viene svolto all'occorrenza. I collaboratori sono formati e informati sull'utilizzo degli asset, viene svolta formazione attiva durante l'anno, le procedure d'utilizzo risultano documentate. Presente regolamento informatico con procedure documentate a disposizione degli incaricati e degli ADS.	**TUTTE LE FUNZIONI AZIENDALI DEL CICLO**
GESTIONE DEI SISTEMI INFORMATIVI - AUTENTICAZIONE	L'accesso ai Vari PC e SERVER è gestito da credenziali univoche, presente password policy con le seguenti caratteristiche: 8 caratteri comprensivi di caratteri speciali, scadenza password ogni 3 mesi, history standard, blocco account a seguito di multipli tentitivi d'accesso falliti non attivo. Sono presente due domini separati uno utilizzato dalla parte amministrativa e uno per la parte di didattica. La revisione degli accessi viene svolta all'occorrenza in corrispondenza dell'off-boarding di un utente. Le Password della posta elettronica non scadono, non è presente MFA. L'accesso al gestionale amministrativo/didattica/magazzino e personale esterno avviene con la stessa password dell'utente di dominio. L'accesso al portale zucchetti per visualizzare le timbrature, richiesta permessi ecc. è gestito con credenziali univoche per ogni utente, la password scade regolarmente tramite procedura automatizzata, il personale interno ha l'accesso amministratore per gestire e forzare la scadenza password degli account.	**TUTTE LE FUNZIONI AZIENDALI DEL CICLO**
GESTIONE DEI SISTEMI INFORMATIVI - SISTEMA DI AUTORIZZAZIONE	L'azienda usa i 2 server di dominio active directory di Microsoft per gestire le Autorizzazioni, uno per la parte amministrativa e uno per la parte Didattica. Non è presente procedura documentata di on-boarding e off-boarding, ma risulta esserci prassi consolidata tra la direzione e L'IT. (nella procedura di off-boarding e regolamento informatico sono specificati i dettagli della gestione degli account di dominio e e-mail) Presente riesame annuale degli accessi ai sistemi. Gli utenti sono amministratori della macchina.	**TUTTE LE FUNZIONI AZIENDALI DEL CICLO**
GESTIONE DEI SISTEMI INFORMATIVI - BACKUP E DISASTER RECOVERY	Presente sistema di backup Veeam Backup & Replication che svolge il backup di tutte le macchine virtuali, i backup sono giornalieri e vengono svolti su NAS. È attivo un sistema di repliche gestito sempre da Veeam Backup & Replication, le repliche sono attive durante le ore di lavoroe vengono eseguite ogni ora. E' presente un backup aggiuntivo su disco USB che viene portato fuori sede, il disco viene cambiato ogni settimana da Denise, i backup su disco esterno sono Cifrati. I NAS sono presso la sala CED. È presente un Backup in cloud solo per la PEC istituzionale svolto su amazon S3. Presente procedura interna con la documentaizone dei backup e procedura di restore, manca procedura di disaster recovery. Durante l'anno sono stati fatti restore granulari all'occorrenza. Sono presenti alert di buon funzionamento.	**TUTTE LE FUNZIONI AZIENDALI DEL CICLO**
GESTIONE DEI SISTEMI INFORMATIVI - INFRASTRUTTURA DI NETWORKING	Lq rete risulta segmentata, presente Vlan management e vlan backup. Presente rete wi-fi cfp_didattica che può essere utilizzata a fronte di registrazione del mac address del dispositivo e della password di accesso, la registrazione viene gestita da Moriani. La rete wifi è utilizzabile da chi ne fa richiesta, anche a titolo temporaneo come esterni che vengono ad operare al CFP per tempi contingentati. Il mac address viene registrato e poi rimosso al termine dell'attività. I dispositivi collegati a questa rete posson osolamente accedere alla parte relativa alla didattica su apposito server dedicato. La rete uffici amministrativi è separate da quella della Didattica, i sistemi di rete non sono ridondati, i server hanno la ridondanza con alimentatore, 'dischi e scheda di rete. Sono presenti servizi pubblicati tramite firewall drytek, come webmail di mdeamon e il sistema di videosorveglianza, il sistema di video sorveglianza è su una rete separata. Presente connettività dati che serve sia la parte di navigazione internet che la fonia, presente linea di backup con tecnologia wifi.	**TUTTE LE FUNZIONI AZIENDALI DEL CICLO**
GESTIONE DEI SISTEMI INFOMRATIVI - RACCOLTA DI LOG E MONITORAGGIO	È in fase di introduzione un sistema di monitoraggio dei server e dei servizi di rete principali, nonché di un sistema di raccolta log ADS.	**TUTTE LE FUNZIONI AZIENDALI DEL CICLO**

Ciclo Segreteria – Sensibilità al rischio

CICLO AZIENDALE:	Segreteria	
#	SEZIONI NUOVE DOPO AGGIORNAMENTO REATI PRESUPPOSTO 2024	CHECK
1	Violazioni del Codice Etico aziendale	Y
2	Reati in danno alla Pubblica Amministrazione	Y
3	Delitti informatici e trattamento illecito di dati	Y
4	Delitti di criminalità organizzata	N/A
5	Reati in tema di falsità in moneta, carte di pubblico credito, valori di bollo e strumenti o segni di riconoscimento	Y
6	Delitti contro l'industria e il commercio	N/A
7	Reati societari	Y
10	Delitti contro la personalità individuale	N/A
13	Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro	N/A
14	Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio	N/A
15	Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori	N/A
16	Altre fattispecie in materia di strumenti di pagamento diversi dai contanti	N/A
17	Delitti in materia di violazione del diritto d'autore	N/A
18	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	N/A
19	Reati ambientali	N/A
20	Impiego di cittadini di paesi terzi il cui soggiorno è irregolare	N/A
21	Razzismo e xenofobia	Y

Ciclo Segreteria – Risk Control Matrix

CICLO AZIENDALE:	Segreteria					
RISK CONTROL MATRIX						
SEZIONE PRIMA: Comportamenti non conformi al Codice Etico aziendale						
VIOLAZIONE	DESCRIZIONE PRINCIPIO DI RIFERIMENTO	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Rispetto Privacy	*trattamento di dati personali e dati sensibili nel rispetto della normativa vigente.*	Accesso ai dati personali e/o sensibili da parte di persone non autorizzate	0,2	0,8	Rilevante	Personale dipendente
Rispetto SGQ	*svolgimento delle attività regolamentate dal Sistema di Gestione della Qualità, adottato dall'azienda, nel pieno rispetto della politica per la Qualità aziendale, delle relative procedure e delle eventuali istruzioni operative applicabili.*	Ritardi nella consegna dei moduli previsti dal SGQ.	0,02	0,05	Accettabile	Segreteria e docenti

CICLO AZIENDALE:	Segreteria					
RISK CONTROL MATRIX						
SEZIONE TERZA: Reati in danno alla Pubblica Amministrazione						
RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Frode informatica	*Art. 640-ter c.p.*	Inserimento di dati alterati nei sistemi informativi pubblici utilizzati, al fine di ottenere maggiori finanziamenti.	0,5	0,2	Accettabile	Tutte le funzioni che utilizzano GEFO Servizi/Sintesi.
Frode informatica	*Art. 640-ter c.p.*	Potenziale alterazione del funzionamento di un sistema informatico o telematico della pubblica amministrazione, o potenziale accesso (senza averne diritto o formale autorizzazione) a dati, informazioni, programmi informatici o telematici al fine di ottenere finanziamenti più alti.	0,3	0,3	Rilevante	Responsabile di Segreteria
Truffa in danno dello Stato o di altro ente pubblico	*Art. 640, co. 2, n. 1, c.p.*	Si commette il reato di truffa in danno dello Stato o di altro ente pubblico e malversazione di erogazioni pubbliche nel momento in cui, in fase di gestione del registro elettronico, il responsabile di segreteria dichiara il falso, modificando fraudolentemente i dati relativi alle presenze degli allievi, procurando per sé o altri un ingiusto profitto con altrui danno. A seguito della commissione dei precedente reato, l'Ente ottiene una indebita percezione di erogazioni a danno dello Stato.	0,5	0,2	Accettabile	Responsabile di Segreteria, Docenti
Concussione	*Art. 317 c.p.*	Accordi illeciti con pubblici ufficiali volti all'ottenimento di benefici per l'ente.	0,5	0,2	Accettabile	Responsabile di Segreteria
Corruzione	*Art. 318 c.p.* *Art. 319 c.p.* *Art. 319 bis c.p.* *Art. 319 ter c.p.* *Art. 320 c.p.* *Art. 321 c.p.* *Art. 322 c.p.*	Accordi illeciti con pubblici ufficiali volti all'ottenimento di benefici per l'ente.	0,5	0,2	Accettabile	Responsabile di Segreteria

CICLO AZIENDALE:	Segreteria					
RISK CONTROL MATRIX						
SEZIONE TERZA - Delitti informatici e trattamento illecito di dati						
RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Accesso abusivo a sistema informatico e danneggiamento di informazioni, dati, programmi e sistemi informatici, anche dello Stato o altro ente pubblico o comunque di pubblico interesse	*Art. 615-ter, 615-quater, 629, co. 3, 635-bis, 635-ter, 635-quater, 635-quater.1 c.p.*	Accesso di utenti non autorizzati a sistemi aziendali protetti da misure di sicurezza (es.: sistemi interbancari). Utilizzo abusivo di password di accesso a siti di soggetti terzi, pubblici o privati, al fine di acquisire informazioni riservate e conseguire vantaggi competitivi. Accesso a una postazione PC, a sistemi di gestione aziendali, a sistemi telematici (anche della Pubblica amministrazione) con password diverse dalle proprie o senza autorizzazione specifica, con codici di accesso ottenuti violando le regole stabilite dalle policy e procedure aziendali. Detenzione abusiva di codici di accesso a sistemi informatici dell'Amministrazione giudiziaria o finanziaria, al fine di acquisire informazioni riservate su procedimenti penali/amministrativi che coinvolgano la Società. Manomissione del sistema di sorveglianza interno al fine di cancellare le registrazioni di un incidente avvenuto ai danni di un lavoratore memorizzate sul dispositivo. Assenza o inadeguatezza di un sistema di protezione dei dati e di un costante monitoraggio dei dati all'interno della rete.	0,3	0,3	Rilevante	Tutte le funzioni aziendali del ciclo

CICLO AZIENDALE: Segreteria

RISK CONTROL MATRIX

SEZIONE QUINTA: Reati in tema di falsità in moneta, carte di pubblico credito, valori di bollo e strumenti o segni di riconoscimento

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Spendita e introduzione nello Stato di monete falsificate anche ricevute in buona fede	*Art. 453 co. 1 n. 3 c.p.* *Art. 455 c.p.* *Art. 457 c.p.*	Raccolta di anticipi in contanti per il materiale individuale, con potenziale raccolta di denaro falso.	**0,02**	**0,05**	Accettabile	Alunni/famiglie alunni, Segreteria e Amministrazione

CICLO AZIENDALE: Segreteria

RISK CONTROL MATRIX

SEZIONE SETTIMA: Reati societari

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Ostacolo all'esercizio delle attività di controllo, revisione e delle funzioni delle autorità pubbliche di vigilanza	*Art. 2625 comma 2 c.c.* *Art. 2638 comma 1 e 2 c.c.*	Fornire documenti alterati o falsi di fronte alla richiesta di documentazione.	**0,7**	**0,2**	Accettabile	Tutte le funzioni coinvolte nell'erogazione dei servizi.
Corruzione tra privati	*Art. 2635 c.c.* *Art. 2635-bis c.c.*	I reati di cui agli artt. 2635 e 2635-bis c.c. potrebbero essere commessi qualora esponenti dell'Ente ricevessero somme di denaro al fine di rilasciare attestati di formazione in assenza dei requisiti e delle condizioni previste dalle procedure vigenti.	**1**	**0,8**	Critico	Responsabile di Segreteria Generale, Resp. Area Formazione, Resp. Area Progettazione, Orientamento/Lavoro

CICLO AZIENDALE: Segreteria

RISK CONTROL MATRIX

SEZIONE VENTUNESIMA: Razzismo e xenofobia

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa	*Art. 604-bis c.p.*	Trattare una persona meno favorevolmente di quanto sia, sia stata o sarebbe trattata un'altra in una situazione analoga, a causa della razza, etnia, nazionalità o religione.	**0,3**	**0,3**	Rilevante	Responsabile Segreteria, Accoglienza informazione logistica, Responsabili d'Area

Ciclo Segreteria – Gap analysis e Piano d'Azione

Gap Analysis e Piano di Azione

CICLO AZIENDALE: SEGRETERIA

Rischio	Descrizione Rischio	Descrizione GAP	Priorità	Funzioni coinvolte	Action Plan
Rispetto Privacy	Accesso ai dati personali e/o sensibili da parte di persone non autorizzate	Modalità di archiviazione non totalmente sufficienti a presidiare il rischio individuato.	Bassa (Accettabile)	Personale dipendente	**Chiusura a chiave degli armadi dove sono archiviati dati personali e/o sensibili di qualsiasi natura (utenti, dipendenti, candidati).** **Accesso consentito solo previa autorizzazione del Direttore o del Resp. Segreteria** **Il sistema della tutela dell'Ente sulla Privacy (adottato dall'Ente in seguito alla normativa Europea - GDPR) migliora ulteriormente questo GAP**
Rispetto SGQ	Ritardi nella consegna dei moduli previsti dal SGQ.	Il SGQ adottato risulta poco interiorizzato dagli operatori, alcuni dei quali ignorano l'esistenza di un sistema di rendicontazione.	Media	Segreteria e docenti	**Impostata e svolta attività di sensibilizzazione sulle Procedure, raccogliendo feedback operativi da parte di chi è chiamato ad applicare il SGQ. Sulla base di tali feedback andranno valutate eventuali revisioni future.** **Formalizzazione all'interno del proprio SGQ di un'apposita procedura riguardante la Rendicontazione dei progetti finanziati.** **Sensibilizzazione dei docenti circa l'importanza della rendicontazione e del ruolo che ha la corretta e puntuale tenuta dei documenti a supporto.**
Frode Informatica	Inserimento di dati alterati nei sistemi informativi pubblici utilizzati, al fine di ottenere maggiori finanziamenti.	I sistemi di controllo applicati non risultano pienamente idonei a prevenire il rischio individuato.	Media	Tutte le funzioni che utilizzano GEFO Servizi/Sintesi.	**Utilizzo Sistema Informativo interno: prevista la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password).** **SI regionali/provinciali (GEFO Servizi/Sintesi):** **identificate e comunicate responsabilità in capo a chi opera coi SI regionali e provinciali. Laddove possibile richiedere e fornire possibilità di accesso a detti sistemi con differenti profilazioni a seconda delle attività da svolgere.** **Previsto inoltre un controllo da parte di un adeguato livello aziendale sulle attività svolte dall'utente (monitoraggio dei login e dei dati inseriti).**

Truffa in danno dello Stato o di altro ente pubblico	Si commette il reato di truffa in danno dello Stato o di altro ente pubblico e malversazione di erogazioni pubbliche nel momento in cui, in fase di gestione del registro elettronico, il responsabile di segreteria dichiara il falso, modificando fraudolentemente i dati relativi alle presenze degli allievi, procurando per sé o altri un ingiusto profitto con altrui danno. A seguito della commissione del precedente reato, l'Ente ottiene una indebita percezione di erogazioni a danno dello Stato.	Possibilità di alterazione dei dati dei registri utilizzati nei rapporti con la PA (registri scolastici, rendicontazione finanziamenti, selezione, appalti, ecc.)	Media	Responsabile di Segreteria, Docenti	**Utilizzo Sistema Informativo interno: prevista la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password).** **SI regionali/provinciali: identificate e comunicate responsabilità in capo a chi opera coi SI regionali e provinciali. Laddove possibile richiedere e fornire possibilità di accesso a detti sistemi con differenti profilazioni a seconda delle attività da svolgere.** **Previsto inoltre un controllo da parte di un adeguato livello aziendale sulle attività svolte dall'utente (monitoraggio dei login e dei dati inseriti).**
Concussione	Accordi illeciti con pubblici ufficiali volti all'ottenimento di benefici per l'ente.	I controlli rilevati risultano efficaci, anche se non	Bassa	Responsabile di Segreteria, Docenti	**A seguito di ciascun incontro con rappresentanti della Pubblica Amministrazione viene richiesta la comunicazione via e-mail di**
Corruzione	Accordi illeciti con pubblici ufficiali volti all'ottenimento di benefici per l'ente.	I controlli rilevati risultano efficaci, anche se non pienamente conosciuti dagli operatori	Bassa	Responsabile di Segreteria	**A seguito di ciascun incontro con rappresentanti della Pubblica Amministrazione viene richiesta la comunicazione via e-mail di un report che evidenzi gli esiti dell'incontro da destinare al proprio responsabile. Il Direttore**
Spendita e introduzione nello Stato di monete falsificate anche ricevute in buona fede	Raccolta di anticipi in contanti per il materiale individuale, con potenziale raccolta di denaro falso.	I sistemi di controllo applicati in passato non risultavano pienamente idonei a prevenire il rischio individuato.	Bassa (Accettabile)	Alunni/famiglie alunni, Segreteria e Amministrazione	**Fornito alle aree interessate da movimenti in contanti (ad es. bar e uff. amministrazione) un rilevatore di banconote false.**
Ostacolo all'esercizio delle attività di controllo, revisione e delle funzioni delle autorità pubbliche di vigilanza	Fornire documenti alterati o falsi di fronte alla richiesta di documentazione.	I sistemi di controllo sulla corretta tenuta della documentazione a supporto delle attività svolte non prevengono pienamente il rischio individuato.	Media	Tutte le funzioni coinvolte nell'erogazione dei servizi.	**Formalizzazione all'interno del proprio SGQ di un'apposita procedura riguardante la Rendicontazione dei progetti finanziati.** **Sensibilizzazione dei docenti e dei referenti all'accoglienza e al primo contatto con l'utenza circa l'importanza della rendicontazione (anche in vista di controlli e/o verifiche ispettive) e del ruolo che ha la corretta e puntuale tenuta dei documenti a supporto.** **Prevista a conclusione delle attività (in particolare per quelle legate a progetti finanziati) una check list di verifica della relativa documentazione (effettuando un controllo sulla presenza del documento e un controllo sulla completezza/corretta tenuta del documento). Tale controllo potrà essere effettuato dalla Segreteria didattica in coordinamento con i Responsabili di area (Formazione, DDIF e Apprendistato).** **A seguito del controllo la documentazione non dovrà più essere liberamente accessibile agli operatori.**
Corruzione tra privati	I reati di cui agli artt. 2635 e 2635-bis c.c. potrebbero essere commessi qualora esponenti dell'Ente ricevessero somme di denaro al fine di rilasciare attestati di formazione in assenza dei requisiti e delle condizioni previste dalle procedure vigenti.	Comportamenti illeciti personali	Bassa	Responsabile di Segreteria Generale, Resp. Area Formazione, Resp. Area Progettazione, Orientamento/Lavoro	**Diffusione del PTCPT e massima condivisione del processo decisionale, puntuale rendicontazione delle attività di vigilanza e controllo**
Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa	Trattare una persona meno favorevolmente di quanto sia, sia stata o sarebbe trattata un'altra in una situazione analoga, a causa della razza, etnia, nazionalità o religione.	Nessun GAP rilevato	Bassa	Responsabile Segreteria, Accoglienza informazione logistica, Responsabili d'Area	**Sensibilizzazione del personale**

Frode Informatica	Potenziale alterazione del funzionamento di un sistema informatico o telematico della pubblica amministrazione, o potenziale accesso (senza averne diritto o formale autorizzazione) a dati, informazioni, programmi informatici o telematici al fine di ottenere finanziamenti più alti.	Possibilità di accesso di personale non autorizzato alla sala server; possibilità di installazione di software malevoli e/o non autoirzzati da parte degli utenti sulle proprie macchine; dischi di backup vulnerabili e a rischio di perdita di dati	Medio-Alta	Tutte le figure del ciclo.	**ARCHIVI FISICI: Introdurre registro per gli accessi alla sala ced. introdurre sistema di spegnimento automatizzato e sicuro dell'infrastruttura server in caso di prolungata assenza di corrente. ANTIMALWARE: integrare la esistente con la parte di Cyber Secuirty per essere aggiornati sulle nuove minacce. AUTENTICAZIONE: definire il passaggio al nuovo sistema di posta con entrambi i domini ed attivare una password policy efficace e doppio fattore di autenticazione (MFA). Rafforzare la password policy attiva aumentando i caratteri delle password portandoli almeno a 12, aumentare la history delle password almeno a 15/20, inserire blocco degli account dopo 10 tentativi sbagliati (può andare bene anche un bocco temporizzato). SISTEMA DI AUTORIZZAZIONE: Rendere gli utenti delle postazioni di lavoro non amministratori della propria macchina se possibile così da diminuire la possibilità di installazione di software malevolo e/o non autorizzato. BACKUP E DISASTER RECOVERY: Valutare il Backup in cloud o immutabile in sostituzione del backup su dischi usb. INFRASTRUTTURA DI NETWORKING: Ridondare i dispositivi critici di rete principali come switch e firewall. RACCOLTA DI LOG E MONITORAGGIO: introdurre sistema di monitoraggio dei server e servizi di rete principali; introdurre sistema di raccolta log ADS.**
Accesso abusivo a sistema informatico e danneggiamento di informazioni, dati, programmi e sistemi informatici, anche dello Stato o altro ente pubblico o comunque di pubblico interesse	Accesso di utenti non autorizzati a sistemi aziendali protetti da misure di sicurezza (es.: sistemi interbancari). Utilizzo abusivo di password di accesso a siti di soggetti terzi, pubblici o privati, al fine di acquisire informazioni riservate e conseguire vantaggi competitivi. Accesso a una postazione PC, a sistemi di gestione aziendali, a sistemi telematici (anche della Pubblica amministrazione) con password diverse dalle proprie o senza autorizzazione specifica, con codici di accesso ottenuti violando le regole stabilite dalle policy e procedure aziendali. Detenzione abusiva di codici di accesso a sistemi informatici dell'Amministrazione giudiziaria o finanziaria, al fine di acquisire informazioni riservate su procedimenti penali/amministrativi che coinvolgano la Società. Manomissione del sistema di sorveglianza interno al fine di cancellare le registrazioni di un incidente avvenuto ai danni di un lavoratore memorizzate sul dispositivo. Assenza o inadeguatezza di un sistema di protezione dei dati e di un costante monitoraggio dei dati all'interno della rete.				

Ciclo Sostegno – Mappatura

MAPPATURA ATTIVITA

CICLO AZIENDALE:	***Sostegno***
RESPONSABILE	***Responsabile Area Sostegno***

ATTIVITA SVOLTE	***DESCRIZIONE***	***FUNZIONI COINVOLTE***
ANALISI E RELAZIONI CON IL TERRITORIO	Analisi delle opportunità offerte dai diversi Bandi/Avvisi (provinciali, regionali, nazionali e UE) dei fabbisogni specifici espressi dai diversi committenti pubblici e privati abbinata allo studio dei fabbisogni di formazione in ambito territoriale attraverso le informazioni recepite da: -relazioni con il sistema istituzionale e sociale locale; -relazioni con il sistema produttivo; -relazioni con il sistema scolastico; -relazioni con le famiglie degli allievi; - relazione con i servizi di riferimento per gli allievi con BES.	**DIRETTORE** **VICE-DIRETTORE** **RESPONSABILI AREA SOSTEGNO E FORMAZIONE** **RESPONSABILE AREA PROGETTAZIONE, ORIENTAMENTO/LAVORO**
GESTIONE BUDGET	Gestione dei budget di progetto in base ai diversi interventi proposti in collaborazione con la Direzione e il Responsabile Amministrativo dell'Agenzia.	**DIRETTORE** **VICE-DIRETTORE** **RESPONSABILE AREA PROGETTAZIONE, ORIENTAMENTO/LAVORO** **RESPONSABILE AMMINISTRATIVO**
PROGETTAZIONE	Sulla base degli indirizzi del Piano Programma il responsabile di area procede all'elaborazione dei singoli progetti (secondo vincoli e risorse dei singoli dispositivi e/o contratti di servizio). Ogni singolo progetto viene sottoposto al riesame della Direzione e ad una verifica formale prima della presentazione. I Responsabili dell'Area PROGETTAZIONE, ORIENTAMENTO/LAVORO, FORMAZIONE (DDIF, APPRENDISTATO, DUALE), prima dell'attivazione del progetto, effettuano i necessari controlli per l'accertamento dei requisiti richiesti dai singoli bandi di riferimento. La progettazione rivolta ad allievi con BES è concertata anche con i servizi di riferimento, le famiglie, i consigli di classe e i coordinatori del corso. Ciascun Responsabile individua dunque le risorse e le modalità organizzative necessarie alla realizzazione dei progetti/corsi assegnati. Viene progettata ed erogata l'attività di orientamento sia in ingresso (relazionandosi con gli istituti secondari di primo grado) sia in uscita per l'orientamento post qualifica/diploma (inserimento lavorativo).	**DIRETTORE** **VICE-DIRETTORE** **RESPONSABILE AREA PROGETTAZIONE, ORIENTAMENTO/LAVORO** **RESPONSABILI AREA SOSTEGNO E FORMAZIONE**
EROGAZIONE	Il processo di erogazione del servizio formativo si articola in servizi erogati all'interno dell'Agenzia e servizi e attività realizzate fuori dall'edificio scolastico. I processi vengono descritti nell'allegato al capitolo quinto del MQ e prevedono: accoglienza, lezioni frontali, lezioni erogate individualmente o a piccolo gruppo a supporto delle lezioni di classe (allievi BES), attività laboratoriali, verifiche finali e in itinere (supporto alle verifiche per allievi con BES), stage (compresi stage interni e esterni protetti per allievi con BES), visite guidate e gite scolastiche (con supporto per allievi con BES).	**RESPONSABILI AREA SOSTEGNO E FORMAZIONE** **TUTOR** **DOCENTI**
CONCLUSIONE E RENDICONTAZIONE	Vengono effettuati i controlli necessari (in avvio, in itinere e a conclusione dell'erogazione) su aspetti logistici, didattici e di apprendimento. I dettagli sono descritti al capitolo quinto del MQ. La rintracciabilità del servizio portato a termine è garantito dalla tenuta dei documenti di supporto (registri, calendari, questionari, ecc...) in ogni fase dell'erogazione. I dati vengono registrati sul sistema GRS direttamente dai singoli docenti, e quotidianamente inviati a Regione Lombardia. Tutta la documentazione a supporto permette di ripercorrere a ritroso l'iter formativo al fine di evidenziare eventuali criticità sopraggiunte durante l'erogazione del servizio e costituisce il punto di partenza per il processo di rendicontazione.	**RESPONSABILI AREA SOSTEGNO E FORMAZIONE** **TUTOR** **DOCENTI**

GESTIONE DEI SISTEMI INFORMATIVI - ANTIMALWARE	L'azienda si è dotata di vari sistemi di sicurezza per contrastare i malware; per la parte client server è installato l'antivirus Eset, l'antivirus comprende servizi di antiransomware, application control e webfiltering, la gestione è centralizzata su console cloud gestita da cierre. A Protezione dell'infrastruttura è presente un firewall zyxell usg300 (in fase sdi aggiornamento, il prodotto è a fine vita) con servizi attivi di content filtering e antivirus. I servizi mail sono divisi in due parti una parte on premise su server mdeamon che comprende anche un antivirus interno per la parte amministrativa con dominio cfpcomo.com; la parte didattica invece è configurata su servizi google apps con il dominio cfpcomo.education.com i sistemi di sicurezza sono proprietari di google. All'interno dell'infrastruttura non è presente un sistema di gestione delle patch di sicurezza, per la parte client i pc si aggiornano automaticamente e gli utenti decidono quando installare gli updates, per la parte server sono automatizzati. Il firewall si aggiorna ogni settimana in modo automatico, per gli altri apparati di rete come siwtch, access point, nas ecc. gli aggiornamenti sono manuali e non programmati. L'aggiornamento firmware dei server viene svolto all'occorrenza. I collaboratori sono formati e informati sull'utilizzo degli asset, viene svolta formazione attiva durante l'anno, le procedure d'utilizzo risultano documentate. Presente regolamento informatico con procedure documentate a disposizione degli incaricati e degli ADS.	**Tutte le funzioni del ciclo**
GESTIONE DEI SISTEMI INFORMATIVI - AUTENTICAZIONE	"L'accesso ai Vari PC e SERVER è gestito da credenziali univoche, presente password policy con le seguenti caratteristiche: 8 caratteri comprensivi di caratteri speciali, scadenza password ogni 3 mesi, history standard, blocco account a seguito di multipli tentitivi d'accesso falliti non attivo. Sono presente due domini separati uno utilizzato dalla parte amministrativa e uno per la parte di didattica. La revisione degli accessi viene svolta all'occorrenza in corrispondenza dell'off-boarding di un utente. Le Password della posta elettronica non scadono, non è presente MFA. L'accesso al gestionale amministrativo/didattica/magazzino e personale esterno avviene con la stessa password dell'utente di dominio. L'accesso al portale zucchetti per visualizzare le timbrature, richiesta permessi ecc. è gestito con credenziali univoche per ogni utente, la password scade regolarmente tramite procedura automatizzata, il personale interno ha l'accesso amministratore per gestire e forzare la scadenza password degli account."	**Tutte le funzioni del ciclo**
GESTIONE DEI SISTEMI INFORMATIVI - SISTEMA DI AUTORIZZAZIONE	L'azienda usa i 2 server di dominio active directory di Microsoft per gestire le Autorizzazioni, uno per la parte amministrativa e uno per la parte Didattica. Non è presente procedura documentata di on-boarding e off-boarding, ma risulta esserci prassi consolidata tra la direzione e L'IT. (nella procedura di off-boarding e regolamento informatico sono specificati i dettagli della gestione degli account di dominio e e-mail) Presente riesame annuale degli accessi ai sistemi. Gli utenti sono amministratori della macchina.	**Tutte le funzioni del ciclo**
GESTIONE DEI SISTEMI INFORMATIVI - BACKUP E DISASTER RECOVERY	Presente sistema di backup Veeam Backup & Replication che svolge il backup di tutte le macchine virtuali, i backup sono giornalieri e vengono svolti su NAS. È attivo un sistema di repliche gestito sempre da Veeam Backup & Replication, le repliche sono attive durante le ore di lavoroe vengono eseguite ogni ora. E' presente un backup aggiuntivo su disco USB che viene portato fuori sede, il disco viene cambiato ogni settimana da Denise, i backup su disco esterno sono Cifrati. I NAS sono presso la sala CED. È presente un Backup in cloud solo per la PEC istituzionale svolto su amazon S3. Presente procedura interna con la documentaizone dei backup e procedura di restore, manca procedura di disaster recovery. Durante l'anno sono stati fatti restore granulari all'occorrenza. Sono presenti alert di buon funzionamento.	**Tutte le funzioni del ciclo**
GESTIONE DEI SISTEMI INFORMATIVI - INFRASTRUTTURA DI NETWORKING	Lq rete risulta segmentata, presente Vlan management e vlan backup. Presente rete wi-fi cfp_didattica che può essere utilizzata a fronte di registrazione del mac address del dispositivo e della password di accesso, la registrazione viene gestita da Moriani. La rete wifi è utilizzabile da chi ne fa richiesta, anche a titolo temporaneo come esterni che vengono ad operare al CFP per tempi contingentati. Il mac address viene registrato e poi rimosso al termine dell'attività. I dispositivi collegati a questa rete posson osolamente accedere alla parte relativa alla didattica su apposito server dedicato. La rete uffici amministrativi è separate da quella della Didattica, i sistemi di rete non sono ridondati, i server hanno la ridondanza con alimentatore, 'dischi e scheda di rete. Sono presenti servizi pubblicati tramite firewall drytek, come webmail di mdeamon e il sistema di videosorveglianza, il sistema di video sorveglianza è su una rete separata. Presente connettività dati che serve sia la parte di navigazione internet che la fonia, presente linea di backup con tecnologia wifi.	**Tutte le funzioni del ciclo**
GESTIONE DEI SISTEMI INFOMRATIVI - RACCOLTA DI LOG E MONITORAGGIO	È in fase di introduzione un sistema di monitoraggio dei server e dei servizi di rete principali, nonché di un sistema di raccolta log ADS.	**Tutte le funzioni del ciclo**

Ciclo Sostegno – Sensibilità al rischio

CICLO AZIENDALE:	Sostegno	
#	SEZIONI NUOVE DOPO AGGIORNAMENTO REATI PRESUPPOSTO 2024	CHECK
1	Violazioni del Codice Etico aziendale	Y
2	Reati in danno alla Pubblica Amministrazione	Y
3	Delitti informatici e trattamento illecito di dati	Y
4	Delitti di criminalità organizzata	N/A
5	Reati in tema di falsità in moneta, carte di pubblico credito, valori di bollo e strumenti o segni di riconoscimento	Y
6	Delitti contro l'industria e il commercio	Y
7	Reati societari	Y
10	Delitti contro la personalità individuale	Y
13	Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro	Y
14	Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio	N/A
15	Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori	N/A
16	Altre fattispecie in materia di strumenti di pagamento diversi dai contanti	N/A
17	Delitti in materia di violazione del diritto d'autore	Y
18	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	N/A
19	Reati ambientali	Y
20	Impiego di cittadini di paesi terzi il cui soggiorno è irregolare	Y
21	Razzismo e xenofobia	Y

Ciclo Sostegno – Risk Control Matrix

CICLO AZIENDALE:	Sostegno

RISK CONTROL MATRIX

SEZIONE PRIMA: Comportamenti non conformi al Codice Etico aziendale

VIOLAZIONE	DESCRIZIONE PRINCIPIO DI RIFERIMENTO	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Verificabilità	*tutte le attività dell'AZIENDA vengono adeguatamente registrate in maniera da consentire la verifica dei processi di decisione, autorizzazione e svolgimento.*	Invio di informazioni e documentazioni utilizzando strumenti identificativi di altri operatori o dirigenti dell'Ente (ad es. Carta Regionale dei Servizi).	**0,2**	**0,5**	Accettabile	Direttore, Vicedirettore (Area Progettazione-Orientamento/Lavoro), Amministrazione, Segreteria, Responsabili d'area (Sostegno, Formazione,DDIF, Duale e Apprendistato)
Legalità	*l'AZIENDA si impegna a rispettare, nello svolgimento di tutte le proprie attività, le leggi internazionali, nazionali e regionali in vigore in Italia e in ciascun Paese nel quale opera anche tramite branch locali.*	Commissione di furti in determinate aree della struttura (laboratori, spogliatoi,..) agevolati dalla mancata assegnazione/assunzione di responsabilità specifiche riguardo il controllo delle aree interessate.	**0,5**	**1**	Critico	Tutte le funzioni dell'Ente
Onestà	*nei rapporti con i CLIENTI, tra i DESTINATARI e verso i TERZI, l'adesione e la concreta applicazione di quanto dichiarato nel presente CODICE ETICO costituisce elemento essenziale della buona gestione aziendale.*	Fornire informazioni agli utenti senza preventivamente verificarne le fonti normative o senza essere certi di quanto dichiarato.	**0,3**	**0,5**	Rilevante	Docenti, Tutor, Addetti Segreteria.
Trasparenza	*l'AZIENDA impronta i rapporti di qualsiasi natura e verso qualsiasi stakeholder alla chiarezza delle intenzioni e all'assenza di volontà di occultamento, rispettando al contempo gli obblighi derivanti dalla normativa vigente in materia di trattamento dei dati riservati.*	Tenuta errata dei registri.	**0,1**	**0,8**	Accettabile	Docenti, Segreteria Generale
Trasparenza	*l'AZIENDA impronta i rapporti di qualsiasi natura e verso qualsiasi stakeholder alla chiarezza delle intenzioni e all'assenza di volontà di occultamento, rispettando al contempo gli obblighi derivanti dalla normativa vigente in materia di trattamento dei dati riservati.*	Conflitti tra funzioni e confusione (anche operativa) dovuta a scarsa assunzione di responsabilità/definizione non puntuale delle responsabilità di ciascuna figura.	**0,25**	**0,4**	Accettabile	Tutte le funzioni del ciclo
Rispetto Privacy	*trattamento di dati personali e dati sensibili nel rispetto della normativa vigente.*	Diffuzione non autorizzata di dati personali/sensibili relativi agli alunni, anche quando trattati tramite mezzi informatici (es. e-mail, server,...).	**0,1**	**0,3**	Accettabile	Tutte le funzioni del ciclo
Rispetto Privacy	*trattamento di dati personali e dati sensibili nel rispetto della normativa vigente.*	Raccolta di dati personali delle "modelle"per attività didattica, senza raccolta autorizzazione al trattamento dei dati.	**0,25**	**0,4**	Accettabile	Alunni e docenti di laboratorio
Rispetto SGQ	*svolgimento delle attività regolamentate dal Sistema di Gestione della Qualità, adottato dall'azienda, nel pieno rispetto della politica per la Qualità aziendale, delle relative procedure e delle eventuali istruzioni operative applicabili.*	Ritardi nella compilazione dei moduli o, più in generale, nell'applicazione del SGQ (con particolre riferimento alla tenuta e consegna della documentazione a supporto delle attività svolte).	**1**	**1**	Critico	Tutte le funzioni del ciclo

CICLO AZIENDALE:	Sostegno

RISK CONTROL MATRIX

SEZIONE SECONDA: Reati in danno alla Pubblica Amministrazione

RISCHIO REATO	RIFERIMENTI NORMATIVI	CONDOTTA ERRATA	PROBABILITA	IMPATTO	VALUTAZIONE	FUNZIONI COINVOLTE
Frode informatica	*Art. 640-ter c.p.*	Inserimento nei sistemi Regionali e Provinciali di dati non reali al fine di ottenere un maggior numero di finanziamenti o far risultare requisiti non posseduti.	**0,3**	**0,8**	Rilevante	Responsabile Segreteria didattica e Responsabili d'Area
Frode informatica	*Art. 640-ter c.p.*	Potenziale alterazione del funzionamento di un sistema informatico o telematico della pubblica amministrazione, o potenziale accesso (senza averne diritto o formale autorizzazione) a dati, informazioni, programmi informatici o telematici al fine di ottenere finanziamenti più alti.	**0,3**	**0,3**	Rilevante	Tutte le funzioni del ciclo
Truffa in danno dello Stato o di altro ente pubblico	*Art. 640, co. 2, n. 1, c.p.*	Si commette il reato di truffa in danno dello Stato o di altro ente pubblico e malversazione di erogazioni pubbliche nel momento in cui, in fase di rendicontazione delle attività svolte, il responsabile amministrativo dichiara il falso, modificando fraudolentemente i dati del corso di formazione, procurando per sé o altri un ingiusto profitto con altrui danno. A seguito della commissione del precedente reato, l'Ente ottiene una indebita percezione di erogazioni a danno dello Stato.	**0,3**	**0,3**	Rilevante	Direttore, Responsabili d'Area
Concussione	*Art. 317 c.p.*	Accordi illeciti con pubblici ufficiali volti all'ottenimento di benefici per l'ente.	**0,5**	**0,2**	Accettabile	Direttore, Responsabili d'Area
Corruzione	*Art. 318 c.p.* *Art. 319 c.p.* *Art. 319 bis c.p.* *Art. 319 ter c.p.* *Art. 320 c.p.* *Art. 321 c.p.* *Art. 322 c.p.*	Accordi illeciti con pubblici ufficiali volti all'ottenimento di benefici per l'ente.	**0,5**	**0,2**	Accettabile	Direttore, Responsabili d'Area

CICLO AZIENDALE:	Sostegno					
RISK CONTROL MATRIX						
SEZIONE TERZA - Delitti informatici e trattamento illecito di dati						
RISCHIO REATO	**RIFERIMENTI NORMATIVI**	**CONDOTTA ERRATA**	**PROBABILITA**	**IMPATTO**	**VALUTAZIONE**	**FUNZIONI COINVOLTE**
Accesso abusivo a sistema informatico e danneggiamento di informazioni, dati, programmi e sistemi informatici, anche dello Stato o altro ente pubblico o comunque di pubblico interesse	*Art. 615-ter, 615-quater, 629, co. 3, 635-bis, 635-ter, 635-quater, 635-quater.1 c.p.*	Accesso di utenti non autorizzati a sistemi aziendali protetti da misure di sicurezza (es.: sistemi interbancari). Utilizzo abusivo di password di accesso a siti di soggetti terzi, pubblici o privati, al fine di acquisire informazioni riservate e conseguire vantaggi competitivi. Accesso a una postazione PC, a sistemi di gestione aziendali, a sistemi telematici (anche della Pubblica amministrazione) con password diverse dalle proprie o senza autorizzazione specifica, con codici di accesso ottenuti violando le regole stabilite dalle policy e procedure aziendali. Detenzione abusiva di codici di accesso a sistemi informatici dell'Amministrazione giudiziaria o finanziaria, al fine di acquisire informazioni riservate su procedimenti penali/amministrativi che coinvolgano la Società. Manomissione del sistema di sorveglianza interno al fine di cancellare le registrazioni di un incidente avvenuto ai danni di un lavoratore memorizzate sul dispositivo. Assenza o inadeguatezza di un sistema di protezione dei dati e di un costante monitoraggio dei dati all'interno della rete.	**0,3**	**0,3**	Rilevante	Tutte le funzioni del ciclo

CICLO AZIENDALE:	Sostegno					
RISK CONTROL MATRIX						
SEZIONE QUINTA: Reati in tema di falsità in moneta, carte di pubblico credito, valori di bollo e strumenti o segni di riconoscimento						
RISCHIO REATO	**RIFERIMENTI NORMATIVI**	**CONDOTTA ERRATA**	**PROBABILITA**	**IMPATTO**	**VALUTAZIONE**	**FUNZIONI COINVOLTE**
Spendita e introduzione nello Stato di monete falsificate anche ricevute in buona fede	*Art. 453 co. 1 n. 3 c.p.* *Art. 455 c.p.* *Art. 457 c.p.*	Ricevere pagamenti (sala/bar, laboratorio estetica e laboratorio acconciatura) in contanti con monete/banconote false non individuate e poi utilizzate.	**0,2**	**0,2**	Accettabile	Modelle, utenti bar e esterni in caso di eventi, docenti.

CICLO AZIENDALE:	Sostegno					
RISK CONTROL MATRIX						
SEZIONE SESTA: Delitti contro l'industria e il commercio						
RISCHIO REATO	**RIFERIMENTI NORMATIVI**	**CONDOTTA ERRATA**	**PROBABILITA**	**IMPATTO**	**VALUTAZIONE**	**FUNZIONI COINVOLTE**
Vendita di sostanze alimentari non genuine come genuine	*Art. 516 c.p.*	Durante servizi di catering, possibile utilizzo di sostanze alimentari scadute o mal conservate (ad es. mancato rispetto della catena del freddo).	**0,25**	**0,5**	Accettabile	Alunni docenti laboratorio alimentazione

CICLO AZIENDALE:	Sostegno					
RISK CONTROL MATRIX						
SEZIONE SETTIMA: Reati Societari						
RISCHIO REATO	**RIFERIMENTI NORMATIVI**	**CONDOTTA ERRATA**	**PROBABILITA**	**IMPATTO**	**VALUTAZIONE**	**FUNZIONI COINVOLTE**
Ostacolo all'esercizio delle attività di controllo, revisione e delle funzioni delle autorità pubbliche di vigilanza	*Art. 2625 comma 2 c.c.* *Art. 2638 comma 1 e 2 c.c.*	Alterazione dei dati richiesti durante i controlli ispettivi (ad es. facendo figurare come svolte attività non effettivamente svolte)..	**1**	**0,8**	Critico	Direzione, Vice Direzione, Amministrazione, Segreteria, Resp. Area
Corruzione tra privati	*Art. 2635 c.c.* *Art. 2635-bis c.c.*	I reati di cui agli artt. 2635 e 2635-bis c.c. potrebbero essere commessi qualora esponenti dell'Ente ricevessero somme di denaro al fine di rilasciare attestati di formazione in assenza dei requisiti e delle condizioni previste dalle procedure vigenti.	**1**	**0,8**	Critico	Direzione, Vice Direzione, Amministrazione, Segreteria, Resp. Area

CICLO AZIENDALE:	Sostegno					
RISK CONTROL MATRIX						
SEZIONE DECIMA: Reati contro la personalità individuale						
RISCHIO REATO	**RIFERIMENTI NORMATIVI**	**CONDOTTA ERRATA**	**PROBABILITA**	**IMPATTO**	**VALUTAZIONE**	**FUNZIONI COINVOLTE**
Riduzione o mantenimento in schiavitù o servitù	*Art. 600 c.p.*	Alterazione dei rapporti tra colleghi a seguito di situazioni di conflitto operativo/ideologico.	**0,3**	**0,8**	Rilevante	Personale dipendente
Riduzione o mantenimento in schiavitù o servitù	*Art. 600 c.p.*	Alterazione rapporto docente/alunno finalizzato all'ottenimento di vantaggi per entrambi.	**0,01**	**1**	Accettabile	Alunni, tutor e docenti.

CICLO AZIENDALE:	Sostegno					
RISK CONTROL MATRIX						
SEZIONE TREDICESIMA: Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro						
RISCHIO REATO	**RIFERIMENTI NORMATIVI**	**CONDOTTA ERRATA**	**PROBABILITA**	**IMPATTO**	**VALUTAZIONE**	**FUNZIONI COINVOLTE**
Lesioni personali colpose	*Art. 590 c.p.*	Utilizzo incauto di attrezzature, strumenti, prodotti utilizzati nelle attività di laboratorio.	**0,5**	**0,85**	Rilevante	Alunni e docenti di laboratorio
Omicidio colposo	*Art. 589 c.p.*	Utilizzo incauto di attrezzature, strumenti, prodotti utilizzati nelle attività di laboratorio.	**0,01**	**1**	Accettabile	Alunni e docenti di laboratorio

CICLO AZIENDALE:	Sostegno					
RISK CONTROL MATRIX						
SEZIONE DICIASSETTESIMA: Delitti in materia di violazione del diritto d'autore						
RISCHIO REATO	**RIFERIMENTI NORMATIVI**	**CONDOTTA ERRATA**	**PROBABILITA**	**IMPATTO**	**VALUTAZIONE**	**FUNZIONI COINVOLTE**
Riproduzione abusiva e diffusione (anche parziale) di opera dell'ingegno protetta	*art.171-ter l. 633/1941*	Distribuzione e utilizzo di testi fotocopiati oltre il limite previsto per legge.	**0,1**	**0,7**	Accettabile	Docenti

CICLO AZIENDALE:	Sostegno					
RISK CONTROL MATRIX						
SEZIONE DICIANNOVESIMA: Reati ambientali						
RISCHIO REATO	**RIFERIMENTI NORMATIVI**	**CONDOTTA ERRATA**	**PROBABILITA**	**IMPATTO**	**VALUTAZIONE**	**FUNZIONI COINVOLTE**
Inquinamento ambientale e delitti colposi contro l'ambiente	*Art. 452-bis, 452-quinquies c.p.*	Scorretto smaltimento degli oli usausti delle cucine	**0,1**	**0,7**	Accettabile	Resp. Area, Amministrazione, Formazione, Progettazione-Orientamento-Lavoro

CICLO AZIENDALE:	Sostegno					
RISK CONTROL MATRIX						
SEZIONE VENTUNESIMA: Razzismo e xenofobia						
RISCHIO REATO	***RIFERIMENTI NORMATIVI***	***CONDOTTA ERRATA***	***PROBABILITA***	***IMPATTO***	***VALUTAZIONE***	***FUNZIONI COINVOLTE***
Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa	*Art. 604-bis c.p.*	Diffondere, durante attività formative/eventi, organizzati dall'ente, idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istigare a commettere o commettere atti di discriminazione per motivi razziali, etnici, nazionali o religiosi. Ed ancora, promuovere, durante attività formative/eventi, organizzati dall'ente, lo sviluppo di organizzazioni, associazioni, movimenti o gruppi che abbiano tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi	**0,3**	**0,3**	Rilevante	Direttore, Responsabili d'Area, Tutor, Docenti

Ciclo Sostegno – Gap analysis e Piano d'Azione

Gap Analysis e Piano di Azione

CICLO AZIENDALE: SOSTEGNO

Rischio	Descrizione Rischio	Descrizione GAP	Priorità	Funzioni coinvolte	Action Plan
Verificabilità	Invio di informazioni e documentazioni utilizzando strumenti identificativi di altri operatori o dirigenti dell'Ente (ad es. Carta Regionale dei Servizi).	I controlli rilevati non risultano pienamente efficaci nel prevenire il rischio individuato.	Media	Direttore, Vicedirettore (Area Progettazione-Orientamento/Lavoro), Amministrazione, Segreteria, Responsabili d'area (Formazione,DDIF, Duale e Apprendistato)	**Utilizzo Sistema Informativo interno: prevedere la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password) e degli strumenti identificativi.**
Legalità	Commissione di furti in determinate aree della struttura (laboratori, spogliatoi,...) agevolati dalla mancata assegnazione/assunzione di responsabilità specifiche riguardo il controllo delle aree interessate.	Determinate funzioni di controllo non sono presenti o espressamente assegnate.	Media	Tutte le funzioni dell'Ente	**Previsto e montato un sistema di telecamere a circuito chiuso ai fini di videosorveglianza sia all'esterno sia all'interno della struttura.** **Tale sistema consente un controllo degli accessi ad aree non presidiate (ad es. chiusura a chiave degli spogliatoi al termine del loro utilizzo, deposito della chiave da parte del docente in segreteria; qualora gli alunni necessitassero di recarsi negli spogliatoi dovranno comunicarlo al docente che farà consegnare la chiave dalla segreteria).**
Onestà	Fornire informazioni agli utenti senza preventivamente verificarne le fonti normative o senza essere certi di quanto dichiarato.	Non sono stati rilevate attività di controllo a presidio del rischio individuato	Bassa	Docenti, Tutor, Addetti Segreteria.	**Sensibilizzare gli operatori a diretto contatto con l'utenza sul tema. In particolare prevedere che l'utenza possa identificare chiaramente da quali funzioni può ricevere le informazioni sul Sistema Dote e le normative applicate alle attività dell'ente (a tale proposito valutare la possibilità di colloqui presso la segreteria didattica in giorni e orari stabiliti con le figure aziendali abilitate a fornire queste informazioni).**
Trasparenza	Tenuta errata dei registri e compilazione del Registro Elettronico	I sistemi di controllo sulla corretta tenuta della documentazione a supporto delle attività svolte non prevengono pienamente il rischio individuato.	Media	Docenti, Segreteria Generale	**Sensibilizzazione dei docenti circa l'importanza della rendicontazione e del ruolo che ha la corretta e puntuale tenuta dei documenti a supporto (Registro cartaceo e Registro Elettronico).**
	Conflitti tra funzioni e confusione (anche operativa) dovuta a scarsa assunzione di responsabilità/definizione non puntuale delle responsabilità di ciascuna figura.	I controlli rilevati non risultano pienamente efficaci nel prevenire il rischio individuato.	Media	Tutte le funzioni del ciclo	**Attività di sensibilizzazione sul nuovo assetto organizzativo dell'Ente a tutto il personale.** **Formalizzazione e condivisione di ruoli e funzioni con l'organizzazione** **Verificare che la definizione dei ruoli e delle responsabilità sia formalizzata e adeguatamente condivisa/comunicata a tutti gli operatori.**

Rispetto Privacy	Diffuzione non autorizzata di dati personali/sensibili relativi agli alunni, anche quando trattati tramite mezzi informatici (es. e-mail, server,...) e/o tramite Registro elettronico	Modalità di archiviazione non sufficienti a presidiare il rischio individuato.	Bassa	Tutte le funzioni del ciclo	**Chiusura a chiave degli armadi dove sono archiviati dati personali e/o sensibili di qualsiasi natura (utenti, dipendenti, candidati,...).** **Utilizzo Sistema Informativo interno e del registro elettronico con accessi personalizzati:** **prevedere la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password).** **Il sistema della tutela dell'Ente sulla Privacy (adottato dall'Ente in seguito alla normativa Europea - GDPR) migliora ulteriormente questo GAP**
	Raccolta di dati personali delle "modelle"per attività didattica, senza raccolta autorizzazione al trattamento dei dati.	Nessuna attività di controllo rilevata a presidio del rischio indicato.	Media	Alunni e docenti di laboratorio	**Predisposta e correttamente comunicata un'informativa sul trattamento dei dati personali raccolti a scopo didattico, da sottoporre solo una volta alle "modelle".** **Tale informativa sottoscritta dall'interessata viene raccolta e archiviata a cura del docente di estetica.**
Rispetto SGQ	Ritardi nella compilazione dei moduli o, più in generale, nell'applicazione del SGQ (con particolre riferimento alla tenuta e consegna della documentazione a supporto delle attività svolte).	Il SGQ adottato risulta poco interiorizzato dagli operatori, alcuni dei quali ignorano l'esistenza di un sistema di rendicontazione.	Alta	Tutte le funzioni del ciclo	**Formalizzazione all'interno del proprio SGQ di un'apposita procedura riguardante la Rendicontazione dei progetti finanziati.** **Sensibilizzazione dei docenti circa l'importanza della rendicontazione e del ruolo che ha la corretta e puntuale tenuta dei documenti a supporto.** **Prevista a conclusione delle attività (in particolare per quelle legate a progetti finanziati) una check list di verifica della relativa documentazione (effettuando un controllo sulla presenza del documento e un controllo sulla completezza/corretta tenuta del documento). Tale controllo potrà essere effettuato dalla Segreteria didattica in coordinamento con amministrazione e responsabili di area.** **A seguito del controllo la documentazione non dovrà più essere liberamente accessibile agli operatori.**
Frode informatica	Inserimento nei sistemi Regionali e Provinciali di dati non reali al fine di ottenere un maggior numero di finanziamenti o far risultare requisiti non posseduti.	I sistemi di controllo applicati in passato non risultavano pienamente idonei a prevenire il rischio individuato.	Media	Responsabile Segreteria didattica e Responsabili d'Area	**Utilizzo Sistema Informativo interno:** **prevista la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password).** **SI regionali/provinciali:** **identificate e comunicate responsabilità in capo a chi opera coi SI regionali e provinciali. Laddove possibile richiedere e fornire possibilità di accesso a detti sistemi con differenti profilazioni a seconda delle attività da svolgere.** **Previsto inoltre un controllo da parte di un adeguato livello aziendale sulle attività svolte dall'utente (monitoraggio dei login e dei dati inseriti).**

Truffa in danno dello Stato o di altro ente pubblico	Si commette il reato di truffa in danno dello Stato o di altro ente pubblico e malversazione di erogazioni pubbliche nel momento in cui, in fase di rendicontazione delle attività svolte, il responsabile amministrativo dichiara il falso, modificando fraudolentemente i dati del corso di formazione, oppure il docente riporta dati non corretti nel registro elettronico, procurando per sé o altri un ingiusto profitto con altrui danno.	Possibilità di alterazione dei dati dei registri utilizzati nei rapporti con la PA (registri scolastici, rendicontazione finanziamenti, selezione, appalti, ecc.)	Media	Direttore, Responsabili d'Area, Docenti	**Utilizzo Sistema Informativo interno: prevista la personalizzazione delle password e sensibilizzare tutti gli operatori a un utilizzo consapevole delle proprie password (evitare di comunicare a colleghi le proprie password).** **SI regionali/provinciali: identificate e comunicate responsabilità in capo a chi opera coi SI regionali e provinciali. Laddove possibile richiedere e fornire possibilità di accesso a detti sistemi con differenti profilazioni a seconda delle attività da svolgere. Previsto inoltre un controllo da parte di un adeguato livello aziendale sulle attività svolte dall'utente (monitoraggio dei login e dei dati inseriti).**
Corruzione		I controlli rilevati risultano efficaci, anche se non pienamente conosciuti dagli operatori.	Bassa (accettabile)	Direttore, Responsabili d'Area	**A seguito di ciascun incontro con rappresentanti della Pubblica Amministrazione viene richiesta la comunicazione via e-mail di un report che evidenzi gli esiti dell'incontro da destinare al proprio responsabile. Il Direttore invia la medesima informativa al Presidente e (quando necessario) anche al Vice Direttore per opportuna informazione.**
Concussione	A seguito della commissione dei precedente reato, l'Ente ottiene una indebita percezione di erogazioni a danno dello Stato.				
Spendita denaro falso ricevuto in buona fede	Ricevere pagamenti (sala/bar, laboratorio estetica e laboratorio acconciatura) in contanti con monete/banconote false non individuate e poi utilizzate.	I sistemi di controllo applicati in passato non risultavano pienamente idonei a prevenire il rischio individuato.	Bassa (accettabile in seguito ad intervento)	Modelle, utenti bar e esterni in caso di eventi, docenti.	**Fornito alle aree interessate da movimenti in contanti (ad es. bar e uff. amministrazione) un rilevatore di banconote false.**
Ostacolo all'esercizio delle attività di controllo, revisione e delle funzioni delle autorità pubbliche di vigilanza	Alterazione dei dati richiesti durante i controlli ispettivi (ad es. facendo figurare come svolte attività non effettivamente svolte)..	I sistemi di controllo sulla corretta tenuta della documentazione a supporto delle attività svolte non prevengono pienamente il rischio individuato.	Medio-Alta	Direzione, Vice Direzione, Amministrazione, Segreteria, Resp. Area	**Formalizzazione all'interno del proprio SGQ di un'apposita procedura riguardante la Rendicontazione dei progetti finanziati.** **Sensibilizzazione dei docenti circa l'importanza della rendicontazione e del ruolo che ha la corretta e puntuale tenuta dei documenti a supporto.** **Prevista a conclusione delle attività (in particolare per quelle legate a progetti finanziati) una check list di verifica della relativa documentazione (effettuando un controllo sulla presenza del documento e un controllo sulla completezza/corretta tenuta del documento). Tale controllo potrà essere effettuato dalla Segreteria didattica in coordinamento con amministrazione e responsabili di area. A seguito del controllo la documentazione non dovrà più essere liberamente accessibile agli operatori.**

Corruzione tra privati	I reati di cui agli artt. 2635 e 2635-bis c.c. potrebbero essere commessi qualora esponenti dell'Ente ricevessero somme di denaro al fine di rilasciare attestati di formazione in assenza dei requisiti e delle condizioni previste dalle procedure vigenti.	Comportamenti illeciti personali	Media	Direzione, Vice Direzione, Amministrazione, Segreteria, Resp. Area	**Diffusione del PTCPT e massima condivisione del processo decisionale, puntuale rendicontazione delle attività di vigilanza e controllo**
Riduzione o mantenimento in schiavitù o servitù	Alterazione dei rapporti tra colleghi a seguito di situazioni di conflitto operativo/ideologico.	Non sono stati rilevate attività di controllo a presidio del rischio individuato	Alta (diventa media)	Personale dipendente	**A chiusura del processo riorganizzativo, prevedere una raccolta di feedback da parte degli operatori. Valutare un'azione di analisi del clima lavorativo in diverse aree aziendali.**
	Alterazione rapporto docente/alunno finalizzato all'ottenimento di vantaggi per entrambi.	I sistemi di controllo rilevati non risultano pienamente idonei a prevenire il rischio individuato.	Media (accettabile)	Alunni, tutor e docenti.	**Evidenziato in ogni contratto predisposto con docenti un richiamo al rispetto del Codice Etico dell'Ente e relativa clausola espressa di rescissione del contratto.**
Lesioni colpose	Utilizzo incauto di attrezzature, strumenti, prodotti utilizzati nelle attività di laboratorio.	Nessun GAP rilevato.	Bassa	Alunni e docenti di laboratorio	**Sensibilizzazione degli alunni da parte dei docenti sulle tematiche inerenti l'utilizzo in sicurezza di macchinari, attrezzature e prodotti potenzialmente pericolosi.** **Predisposizione e diffuzione del "Regolamento di Laboratorio" per ciascun Laboratorio**
Omicidio colposo	Utilizzo incauto di attrezzature, strumenti, prodotti utilizzati nelle attività di laboratorio.	Nessun GAP rilevato.	Bassa	Alunni e docenti di laboratorio	**Sensibilizzazione degli alunni da parte dei docenti sulle tematiche inerenti l'utilizzo in sicurezza di macchinari, attrezzature e prodotti potenzialmente pericolosi.** **Predisposizione e diffuzione del "Regolamento di Laboratorio"**
Inquinamento ambientale e delitti colposi contro l'ambiente	Scorretto smaltimento degli oli usausti delle cucine	Nessun GAP rilevato.	Bassa	Tutte le figure operanti nel ciclio	**Formalizzazione di un contratto per lo smaltimento degli olii esausti e procedure operative**

Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa	Diffondere, durante attività formative/eventi, organizzati dall'ente, idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istigare a commettere o commettere atti di discriminazione per motivi razziali, etnici, nazionali o religiosi. Ed ancora, promuovere, durante attività formative/eventi, organizzati dall'ente, lo sviluppo di organizzazioni, associazioni, movimenti o gruppi che abbiano tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi	Nessun GAP rilevato.	Bassa	Direttore, Responsabili d'Area, Tutor, Docenti	**Sensibilizzazione del personale**
Vendita di sostanze alimentari non genuine come genuine	Durante servizi di catering, possibile utilizzo di sostanze alimentari scadute o mal conservate (ad es. mancato rispetto della catena del freddo).	Nessun GAP rilevato.	-	Alunni docenti laboratorio alimentazione	
Riproduzione abusiva e diffusione (anche parziale) di opera dell'ingegno protetta	Distribuzione e utilizzo di testi fotocopiati oltre il limite previsto per legge.	Nessun GAP rilevato.	-	Docenti e tutor	-
Frode Informatica	Potenziale alterazione del funzionamento di un sistema informatico o telematico della pubblica amministrazione, o potenziale accesso (senza averne diritto o formale autorizzazione) a dati, informazioni, programmi informatici o telematici al fine di ottenere finanziamenti più alti.	Possibilità di accesso di personale non autorizzato alla sala server; possibilità di installazione di software malevoli e/o non autoirzzati da parte degli utenti sulle proprie macchine; dischi di backup vulnerabili e a rischio di perdita di dati	Medio-Alta	Tutte le figure del ciclo.	**ARCHIVI FISICI: Introdurre registro per gli accessi alla sala ced. introdurre sistema di spegnimento automatizzato e sicuro dell'infrastruttura server in caso di prolungata assenza di corrente. ANTIMALWARE: integrare la esistente con la parte di Cyber Secuirty per essere aggiornati sulle nuove minacce. AUTENTICAZIONE: definire il passaggio al nuovo sistema di posta con entrambi i domini ed attivare una password policy efficace e doppio fattore di autenticazione (MFA). Rafforzare la password policy attiva aumentando i caratteri delle password portandoli almeno a 12, aumentare la history delle password almeno a 15/20, inserire blocco degli account dopo 10 tentativi sbagliati (può andare bene anche un bocco temporizzato). SISTEMA DI AUTORIZZAZIONE: Rendere gli utenti delle postazioni di lavoro non amministratori della propria macchina se possibile così da diminuire la possibilità di installazione di software malevolo e/o non autorizzato. BACKUP E DISASTER RECOVERY: Valutare il Backup in cloud o immutabile in sostituzione del backup su dischi usb. INFRASTRUTTURA DI NETWORKING: Ridondare i dispositivi critici di rete principali come switch e firewall. RACCOLTA DI LOG E MONITORAGGIO: introdurre sistema di monitoraggio dei server e servizi di rete principali; introdurre sistema di raccolta log ADS.**
Accesso abusivo a sistema informatico e danneggiamento di informazioni, dati, programmi e sistemi informatici, anche dello Stato o altro ente pubblico o comunque di pubblico interesse	Accesso di utenti non autorizzati a sistemi aziendali protetti da misure di sicurezza (es.: sistemi interbancari). Utilizzo abusivo di password di accesso a siti di soggetti terzi, pubblici o privati, al fine di acquisire informazioni riservate e conseguire vantaggi competitivi. Accesso a una postazione PC, a sistemi di gestione aziendali, a sistemi telematici (anche della Pubblica amministrazione) con password diverse dalle proprie o senza autorizzazione specifica, con codici di accesso ottenuti violando le regole stabilite dalle policy e procedure aziendali. Detenzione abusiva di codici di accesso a sistemi informatici dell'Amministrazione giudiziaria o finanziaria, al fine di acquisire informazioni riservate su procedimenti penali/amministrativi che coinvolgano la Società. Manomissione del sistema di sorveglianza interno al fine di cancellare le registrazioni di un incidente avvenuto ai danni di un lavoratore memorizzate sul dispositivo. Assenza o inadeguatezza di un sistema di protezione dei dati e di un costante monitoraggio dei dati all'interno della rete.				