5	Controlli organizzativi		APPLICABILITÀ		MOTIVAZIONE APPLICABILITA'/NON APPLICABILITA'
			SI	NO	
5.1	Politiche per la sicurezza delle informazioni	**Controllo** La politica per la sicurezza delle informazioni e le politiche specifiche devono essere definite, approvate dalla direzione, pubblicate, comunicate e accettate dal personale pertinente e dalle parti interessate pertinenti e riesaminate a intervalli pianificati e quando si verificano cambiamenti significativi. (5.1.1)	☒	☐	*Vedi 2_M_A.5 Politiche per la Sicurezza delle informazioni* *Il documento internamente è stato diffuso mediante invio mail a tutti i dipendenti e pubblicato sul sito di Carraro Lab.* *Il documento viene sottoposto a riesame in occasione della riunione annuale della direzione, come previsto sul verbale del riesame modello 11_M_9.3.2 Riesame di direzione.*
5.2	Ruoli e responsabilità per la sicurezza delle informazioni	**Controllo** I ruoli e le responsabilità per la sicurezza delle informazioni devono essere definiti e assegnati in base alle esigenze dell'organizzazione. (6.1.1)	☒	☐	*I ruoli e le responsabilità sono indicati all'interno dell'Organigramma nominale.* *Vedi organigramma* *Esempi:* *Direzione generale: Gualtiero Carraro* *Direzione ricerca & Sviluppo: Roberto Gualtiero* *DPO: Avv. Francesca Armaroli* *Amministratore di sistema: Facchetti Francesca.* *I ruoli al momento non sono stati ancora comunicati, previsto invio mail con organigramma.* *Ulteriori informazioni circa il proprio ruolo sono riportate all'interno dell'NDA dei singoli dipendenti. 4_MA.13.2.4 Accordo di riservatezza* *Vedi Elenco Addetti e mansioni*

5.3	Separazione dei compiti	**Controllo** I compiti e le aree di responsabilità in conflitto devono essere separati. (6.1.2)	☒	☐	*Dall'organigramma e dal mansionario si evince una separazione dei compiti che possono generare conflitti, nel limite dell'organizzazione considerate le dimensioni ridotte.*
5.4	Responsabilità della direzione	**Controllo** La direzione deve richiedere a tutto il personale di applicare la sicurezza delle informazioni in conformità con la politica per la sicurezza delle informazioni, le politiche specifiche e le procedure dell'organizzazione in vigore. (7.2.1)	☒	☐	*Come richiesta al personale sono stati elaborati i seguenti documenti:* *Vedi 4_MA.13.2.4 Accordo di riservatezza* *16_M_Modulo di consegna device – al par.4 è riportata la politica dell'azienda in merito all'uso sicuro dei Device consegnati.* *I documenti vengono consegnati e fatti sottoscrivere dai singoli dipendenti.*
5.5	Contatti con le autorità	**Controllo** L'organizzazione deve stabilire e mantenere i contatti con le autorità competenti. (6.1.3)	☒	☐	*Procedura Data Breach.* *Nella procedura vengono descritte le modalità di comunicazione con il Garante della Privacy in caso di incidenti che possono compromettere la sicurezza dei dati personali.* *Non applicabile la direttiva NIS 2 in merito a grandezza dell'organizzazione e tipologia di dati trattati.*
5.6	Contatti con gruppi specialistici	**Controllo** L'organizzazione deve stabilire e mantenere contatti con gruppi specialistici o altri forum di sicurezza specializzati e associazioni professionali. (6.1.4)	☒	☐	*L'organizzazione mantiene contatti con AWS anche mediante la partecipazione a specifici webinar.* *Iscrizione a newsletter a siti e gruppi specialistici.* *Vedi 1-8_M_6.1.3_All.5.6_(Allegati mail)*
5.7	Threat intelligence	**Controllo** Le informazioni relative alle minacce alla sicurezza delle informazioni devono essere raccolte e analizzate per produrre threat intelligence. (11.1.4 – 11.2.1)	☒	☐	*Le informazioni circa le minacce sono analizzate sia all'interno del modulo 12_M_ID 6.1 Valutazione dei rischi per le informazioni* *Presente inoltre:* *Modulo 13_M_Modulo analisi incidenti nel quale vengono raccolti ed analizzati gli incidenti.* *Modulo 14_M_Registro analisi incidenti*
5.8	Sicurezza delle informazioni nella gestione dei progetti	**Controllo** La sicurezza delle informazioni deve essere integrata nella gestione dei progetti. (6.1.5)	☒	☐	*Per i progetti viene redatto un documento tecnico denominato Documento di analisi funzionale.* *Esempio* *Documento di analisi funzionale progetto "Startup Generator".*

					Nel documento funzionale sono riportate tutte le specifiche tecniche per la sicurezza delle informazioni che utili alla progettazione. *Esempio* *Sono descritte le modalità di protezione dei contenuti multimediali utili allo sviluppo del prodotto finale.*
5.9	Inventario delle informazioni e degli altri asset relativi	**Controllo** Deve essere sviluppato e mantenuto un inventario delle informazioni e degli altri asset relativi, compresi i responsabili. (8.1.1 – 8.1.2)	☒	☐	*Vedi 17_M_Prospetto elenco asset* *Nel documento sono riportate le seguenti informazioni:* *Area, Asset, Descrizione, Chi ha accesso, Modalità di accesso, Backup, Tipologia di dati, livello di riservatezza, protezione del dispositivo, per le responsabilità si rimanda al modulo di consegna del device, in quanto ogni persona è responsabile dell'uso del singolo device.*
5.10	Uso accettabile delle informazioni e degli altri asset relativi	**Controllo** Le regole per l'uso accettabile e le procedure per il trattamento delle informazioni e degli altri asset relativi devono essere identificate, documentate e attuate. (8.1.3)	☒	☐	*Vedi 4_MA.13.2.4 Accordo di riservatezza* *Vedi 16_M_Modulo di consegna device – al par.4 è riportata la politica dell'azienda in merito all'uso sicuro dei Device consegnati.* *I documenti vengono consegnati e fatti sottoscrivere dai singoli dipendenti*
5.11	Restituzione degli asset	**Controllo** Il personale e le altre parti interessate, a seconda dei casi, devono restituire tutti gli asset dell'organizzazione in loro possesso in caso di cambiamento o cessazione del rapporto di lavoro, del contratto o dell'accordo. (8.1.4).	☒	☐	*Nel modulo di consegna sono specificale le modalità di riconsegna degli Asset, con la revoca degli accessi a tutti gli applicativi e database in possesso del singolo dipendente.* *Vedi MOD. 16_M_Mod. Consegna_Riconsegna Device*
5.12	Classificazione delle informazioni	**Controllo** Le informazioni devono essere classificate in base alle esigenze di sicurezza delle informazioni dell'organizzazione sulla base dei requisiti di riservatezza, integrità, disponibilità e delle parti interessate pertinenti. (8.2.1)	☒	☐	*Vedi modello 3_M_A.8.2.1 Politica per la classificazione delle informazioni* *La classificazione prevede nr 4 livelli* *Liv. 1- PUB: Pubblico / non classificato (azzurro)* *Liv. 2- INT: Uso Interno / Internal (verde)* *Liv. 3- RIS: Riservato / Restricted (giallo)* *Liv. 4- STR: Strettamente Riservato / Confidential (rosso)*

					Esempio: *Il documento 3_M_A.8.2.1 Politica per la classificazione delle informazioni è stato classificato come ad uso interno.*
5.13	Etichettatura delle informazioni	**Controllo** Un insieme appropriato di procedure per l'etichettatura delle informazioni deve essere sviluppato e implementato in conformità con lo schema di classificazione delle informazioni adottato dall'organizzazione. (8.2.2)	☒	☐	*In base alla classificazione delle informazioni le stesse vengono opportunamente etichettate* *La classificazione viene fatta utilizzando un colore diverso per le cartelle ed etichettando i files salvati all'interno del Google Drive.*
5.14	Trasferimento delle informazioni	**Controllo** Devono essere in vigore regole, procedure o accordi per il trasferimento delle informazioni per tutte le tipologie di strutture di trasferimento all'interno dell'organizzazione e tra l'organizzazione e altre parti. (11.2.5)	☒	☐	*Come sistema di trasferimento delle informazioni internamente viene utilizzato Google Drive* *Mentre le informazioni trasmesse all'esterno avvengono mediante Gmail (per allegati fino a 25 MB, mentre oltre questa dimensione fino a 5GB attraverso Google Drive).* *Le regole di trasferimento sono indicate all'interno delle NDA consegnate e sottoscritte dai dipendenti.*
5.15	Controllo degli accessi	**Controllo** Le regole per controllare l'accesso fisico e logico alle informazioni e agli altri asset relativi devono essere stabilite e implementate sulla base dei requisiti di business e di sicurezza delle informazioni. (9.1.1)	☒	☐	*Vedi 4_MA.13.2.4 Accordo di riservatezza* *Vedi 16_M_Modulo di consegna device – al par.4 è riportata la politica dell'azienda in merito all'uso sicuro dei Device consegnati.* *L'organizzazione attua da anni lo smart Working pertanto non sono state elaborate regole per quanto riguarda l'accesso fisico.*
5.16	Gestione delle identità	**Controllo** L'intero ciclo di vita delle identità deve essere gestito.	☒	☐	*Vedi documento 1-1_M_6.1.3_All 5.16 Gestione delle identità.*
5.17	Informazioni di autenticazione	**Controllo** L'assegnazione e la gestione delle informazioni di autenticazione devono essere controllate da un processo gestionale, che preveda di informare il	☒	☐	*Vedi 4_MA.13.2.4 Accordo di riservatezza* *Vedi 16_M_Modulo di consegna device – al par.4 è riportata la politica dell'azienda in merito all'uso sicuro delle credenziali di accesso.*

		personale in merito al trattamento appropriato delle informazioni di autenticazione. (9.4.1 – 9.2.4 – 9.3.1)			
5.18	Diritti d'accesso	**Controllo** I diritti di accesso alle informazioni e agli altri asset relativi devono essere forniti, riesaminati, modificati e rimossi in accordo con la politica specifica e le regole per il controllo degli accessi dell'organizzazione. (9.2.5 – 9.2.6)	☒	☐	*Vedi 16_M_Modulo di consegna device* *Il riesame avviene annualmente in occasione del riesame della direzione o in occasione di licenziamenti o cambio mansioni.* *Vedi: 11_Mod. M_9.3.2 Riesame di direzione SGI*
5.19	Sicurezza delle informazioni nelle relazioni con i fornitori	**Controllo** Devono essere stabiliti e implementati processi e procedure per gestite i rischi della sicurezza delle informazioni associati all'utilizzo di prodotti o servizi del fornitore. (15.1.1 – 15.1.2).	☒	☐	*Vista Pro_Valutazione_Fornitori (integrata con Sistema ISO9001)* *Vedi Mod 4 Elenco fornitori qualificati (integrato con Sistema ISO9001)* *Vedi 18_ Mod. 08.01_Questionario qualifica fornitore.* *Vista 1-2_M6.1.3_All 5.19-5.24 Procedura qualifica fornitori critici.*
5.20	Sicurezza delle informazioni negli accordi con i fornitori	**Controllo** I requisiti di sicurezza delle informazioni pertinenti devono essere stabiliti e concordati con ciascun fornitore in base al tipo di rapporto con il fornitore. (15.1.1 a 15.2.2)	☒	☐	*NDA con collaboratori* *4_M_A.13.2.4 Accordo di Riservatezza (NDA)* *Contratto quadro con Cloudbits* *CONTRATTO_Fornitori_software_Carraro_Cloudbits_CL-CB_signed* *1-2_M_6.1.3_All.5.19-5.24_Procedura Qualifica Fornitori Critici*
5.21	Gestione della sicurezza delle informazioni nella filiera di fornitura per l'ICT	**Controllo** Devono essere definiti e attuati processi e procedure per gestire i rischi relativi alla sicurezza delle informazioni associati alla filiera di fornitura di prodotti e servizi ICT. (15.1.3)	☒	☐	*NDA con collaboratori* *4_M_A.13.2.4 Accordo di Riservatezza (NDA)* *Contratto quadro con Cloudbits* *CONTRATTO_Fornitori_software_Carraro_Cloudbits_CL-CB_signed* *1-2_M_6.1.3_All.5.19-5.24_Procedura Qualifica Fornitori Critici*

5.22	Monitoraggio, riesame e gestione dei cambiamenti dei servizi dei fornitori	**Controllo** L'organizzazione deve monitorare, riesaminare, valutare e gestire regolarmente i cambiamenti nelle pratiche di sicurezza delle informazioni dei fornitori e nell'erogazione dei servizi. (15.2.1)	☒	☐	*NDA con collaboratori* *4_M_A.13.2.4 Accordo di Riservatezza (NDA)* *Contratto quadro con Cloudbits* *CONTRATTO_Fornitori_software_Carraro_Cloudbits_CL-CB_signed* *1-2_M_6.1.3_All.5.19-5.24_Procedura Qualifica Fornitori Critici*
5.23	Sicurezza delle informazioni per l'utilizzo di servizi cloud	**Controllo** I processi per l'acquisizione, l'utilizzo, la gestione e l'uscita dai servizi cloud devono essere stabiliti in conformità con i requisiti di sicurezza delle informazioni dell'organizzazione.	☒	☐	*NDA con collaboratori* *4_M_A.13.2.4 Accordo di Riservatezza (NDA)* *Contratto quadro con Cloudbits* *CONTRATTO_Fornitori_software_Carraro_Cloudbits_CL-CB_signed* *1-2_M_6.1.3_All.5.19-5.24_Procedura Qualifica Fornitori Critici*
5.24	Pianificazione e preparazione per la gestione degli incidenti relativi alla sicurezza delle informazioni	**Controllo** L'organizzazione deve pianificare e prepararsi per la gestione degli incidenti relativi alla sicurezza delle informazioni definendo, stabilendo e comunicando processi, ruoli e responsabilità di gestione degli incidenti relativi alla sicurezza delle informazioni.	☒	☐	*NDA con collaboratori 4_M_A.13.2.4 Accordo di Riservatezza (NDA)* *Contratto quadro con Cloudbits* *Modulo 13_M_Modulo analisi incidenti nel quale vengono raccolte ed analizzati gli incidenti.* *Modulo 14_M_Registro analisi incidenti* *1-2_M_6.1.3_All.5.19-5.24_Procedura Qualifica Fornitori Critici* *La NIS2 non è pertinente per la tipologia di dati trattati, ovvero non siamo soggetti alla comunicazione al CSRIT di pertinenza.* *Pro_Valutazione_Fornitori (integrata con Sistema ISO9001)* *Mod. 4 Elenco Fornitori qualificati_(integrata con Sistema ISO9001)*
5.25	Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni	**Controllo** L'organizzazione deve valutare gli eventi relativi alla sicurezza delle informazioni e decidere se devono	☒	☐	*Vista 1-3_M6.1.3_All 5.25 Valutazione e decisione sugli eventi di sicurezza*

		essere classificati come incidenti relativi alla sicurezza delle informazioni. (16.1.4)			*Modulo 13_M_Modulo analisi incidenti nel quale vengono raccolte ed analizzati gli incidenti.* *Modulo 14_M_Registro analisi incidenti*
5.26	Risposta agli incidenti relativi alla sicurezza delle informazioni	**Controllo** Gli incidenti relativi alla sicurezza delle informazioni devono essere risolti secondo le procedure documentate. (16.1.5)	☒	☐	*Vista 1-4_M6.1.3_All 5.26-5.29* *Modulo 13_M_Modulo analisi incidenti nel quale vengono raccolte ed analizzati gli incidenti.* *Modulo 14_M_Registro analisi incidenti*
5.27	Apprendimento dagli incidenti relativi alla sicurezza delle informazioni	**Controllo** Le conoscenze acquisite dagli incidenti relativi alla sicurezza delle informazioni devono essere utilizzate per rafforzare e migliorare i controlli di sicurezza delle informazioni. (16.1.6)	☒	☐	*Vista 1-4_M6.1.3_All 5.26-5.29* *Modulo 13_M_Modulo analisi incidenti nel quale vengono raccolte ed analizzati gli incidenti.* *Modulo 14_M_Registro analisi incidenti*
5.28	Raccolta di prove	**Controllo** L'organizzazione deve stabilire e attuare procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione delle prove relative agli eventi relativi alla sicurezza delle informazioni. (16.1.7)	☒	☐	*Vista 1-4_M6.1.3_All 5.26-5.29* *Modulo 13_M_Modulo analisi incidenti nel quale vengono raccolte ed analizzati gli incidenti.* *Modulo 14_M_Registro analisi incidenti*
5.29	Sicurezza delle informazioni durante le interruzioni	**Controllo** L'organizzazione deve pianificare come mantenere la sicurezza delle informazioni a un livello appropriato durante le interruzioni.	☒	☐	*Vista 1-4_M6.1.3_All 5.26-5.29* *I dipendenti lavorano in smart working con computer portatile. In caso di interruzione della rete internet utilizzano come alternativa l'hotspot da dispositivo portatile.* *Per quanto riguarda le interruzioni lato utente, vengono gestite dall'Amministratore di Sistema in qualità di gestore dell'infrastruttura hosting di AWS.*
5.30	Prontezza dell'ICT per la continuità operativa	**Controllo** La prontezza dell'ICT deve essere pianificata, attuata, mantenuta e testata sulla base degli obiettivi di continuità operativa e dei requisiti di continuità dell'ICT.	☒	☐	*Vedi allegato 1-5_M_6.1.3_All.5.30_Continuità Operativa*
5.31	Identificazione dei requisiti legali, statutari,	**Controllo** I requisiti legali, statutari, regolamentari e contrattuali relativi alla sicurezza delle informazioni e l'approccio	☒	☐	*Vedi elenco norme, leggi e regolamenti 19_M_E_Normative Esterne* *I requisiti sono indicati all'interno dei capitolati tecnici o altra documentazione relativa ai bandi pubblici.* Vedi allegato:

	regolamentari e contrattuali	dell'organizzazione per soddisfare tali requisiti devono essere identificati, documentati e tenuti aggiornati.			1-6_M_6.1.3_All.5.31_Requisiti Legali, Statutari, Regolamentari e Contrattuali *Esempio* *Procedure negoziata senza pubblicazione di bando – Fondazione ITS Turismo Liguria* *Oggetto: Potenziamento dell'offerta formativa ITS Accademy* *Codice avviso: M4C1|1.5-2023-1082* *Capitolato tecnico con condizioni esecutive fornitura di attrezzature per l'allestimento dei laboratori immersivi con intelligenza artificiale.*
5.32	Diritti di proprietà intellettuale	**Controllo** L'organizzazione deve attuare procedure appropriate per proteggere i diritti di proprietà intellettuale. (18.1.2)	☒	☐	*Come proprietà intellettuale, l'organizzazione ha elaborato una metodologia per l'accesso e la fruizione di contenuti digitali basato sull'integrazione di realtà estesa e intelligenza artificiale.* *Tale metodo è stato oggetto di brevetto.* *Vista registrazione al Ministero delle Imprese e del Made in Italy* *N102023000022941* *Del 31/10/2023* *Le modalità di protezione dei diritti sono indicate all'interno degli accordi di riservatezza sottoscritti da fornitori, dipendenti.* *4_M_A.13.2.4 Accordo di Riservatezza (NDA)*
5.33	Protezione delle registrazioni	**Controllo** Le registrazioni devono essere protette da perdita, distruzione, falsificazione, accesso non autorizzato e rilascio non autorizzato. (18.1.3)	☒	☐	*Tutte le registrazioni sono salvate in forma digitale all'interno di Google drive dove gli accessi sono consentiti esclusivamente agli utenti dell'organizzazione in base ruolo e alle autorizzazioni definite dalla direzione.* *Google Drive riduce al minimo la probabilità di distruzione, ovvero perdita delle registrazioni.*
5.34	Privacy e protezione dei dati personali	**Controllo** L'organizzazione deve identificare e soddisfare i requisiti relativi alla tutela della privacy e alla protezione dei dati personali secondo le leggi e i regolamenti applicabili e i requisiti contrattuali. (18.1.4)	☒	☐	*Per soddisfare tutti i requisiti previsti dal GDPR 679/16 l'organizzazione ha stipulato un contratto di consulenza con società esterna e nomina DPO nella persona di Avv. Francesca Armaroli.* *Tutti i requisiti relativi ai dati personali vengono definiti a livello contrattuale con i clienti, fornitori e i dipendenti, attraverso specifiche nei contratti, negli accordi di*

					riservatezza e in tutti i documenti in cui si ritiene necessario specificare le modalità di trattamento dei dati personali. *Vedi modello informativa clienti* *4_M_A.13.2.4 Accordo di Riservatezza (NDA)* *12_ M ID 6.1 Valutazione dei rischi.*
5.35	Riesame indipendente della sicurezza delle informazioni	**Controllo** L'approccio dell'organizzazione alla gestione della sicurezza delle informazioni e alla sua attuazione, che include personale, processi e tecnologie, deve essere riesaminato in modo indipendente a intervalli pianificati o quando si verificano cambiamenti significativi. (18.2.1)	☒	☐	*Il sistema è oggetto di riesame annuale da parte della Direzione.* *Vedi 11_Mod_M_9.3.2 Riesame della direzione* *Vedi 1-7_M_6.1.3_All. 5.35 Riesame*
5.36	Conformità alle politiche e alle norme per la sicurezza delle informazioni	**Controllo** La conformità alla politica per la sicurezza delle informazioni dell'organizzazione, alle politiche specifiche, alle regole e agli standard deve essere riesaminata regolarmente. (18.2.2)	☒	☐	*La politica per la sicurezza delle informazioni nonché tutte le altre disposizioni e politiche sono oggetto di riesame annuale come previsto dal punto 9.3 della norma ISO 27001:2023.* *Vedi 11_Mod_M_9.3.2 Riesame della direzione*
5.37	Procedure operative documentate	**Controllo** Le procedure operative per le strutture di elaborazione delle informazioni dovrebbero essere documentate e messe a disposizione del personale che ne ha bisogno. (12.1.1)	☒	☐	*Vedi 24_M_P.8.01_Gestione dei Cambiamenti*

6	Controlli sul personale		APPLICABILITÀ		MOTIVAZIONE APPLICABILITA'/NON APPLICABILITA'
			SI	NO	
6.1	Screening	**Controllo** I controlli di verifica del background di tutti i candidati all'impiego devono essere effettuati prima dell'ingresso nell'organizzazione e su base continuativa, tenendo conto delle leggi, dei regolamenti e dell'etica applicabili ed essere proporzionati ai requisiti di business, alla classificazione delle informazioni a cui si deve accedere e ai rischi percepiti. (7.1.1)	☒	☐	*Sono state definite le competenze minime del personale, in termini formativi e di esperienze pregresse.* *Mod. 14- Elenco Addetti Mansioni (integrato con Sistema ISO9001)* *Esempio* *Impiegata grafica* *Competenze minime: conoscenza della normativa su GDP 679/16 e cyber security.* *Vengono esaminati per ogni candidato il relativo curriculum vitae.* *Viene Effettuato colloquio conoscitivo approfondito sulle esperienze pregresse al fine di verificare le reali conoscenze in materia di sicurezza delle informazioni.*
6.2	Termini e condizioni d'impiego	**Controllo** Gli accordi contrattuali di lavoro devono indicare le responsabilità del personale e dell'organizzazione relative alla sicurezza delle informazioni. (7.1.2)	☒	☐	*Il controllo è attuato mediate accordi contrattuali, sottoscrizione dell'NDA e della politica di utilizzo accettabile degli asset.* *4_M_A13.2.4 Accordi di riservatezza* *5_M_A8.1.3 Politica di utilizzo accettabile degli asset.*
6.3	Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni	**Controllo** Il personale dell'organizzazione e le parti interessate pertinenti devono acquisire adeguate consapevolezza, istruzione e formazione relative alla sicurezza delle informazioni e aggiornamenti regolari della politica per la sicurezza delle informazioni dell'organizzazione, delle politiche specifiche e delle procedure, secondo quanto pertinente alla loro funzione lavorativa. (7.2.2)	☒	☐	*Vedi:* *Pro_Formazione - Procedura formazione integrata con il sistema ISO 9001:2015* *10_Mod. M_10_Registro_Formazione* *9_Mod. M_9_Programma_Formazione* *14- Elenco Addetti Mansioni (integrato con Sistema ISO9001) – con la definizione delle competenze minime.* *Il programma della formazione viene elaborato annualmente in occasione del Riesame della direzione.*
6.4	Processo disciplinare	**Controllo** Un processo disciplinare deve essere formalizzato e comunicato per intraprendere azioni contro il personale e altre parti interessate pertinenti che hanno commesso una violazione della politica per la sicurezza delle informazioni. (7.2.3)	☒	☐	*L'organizzazione ha deciso di applicare il disciplinare definito dal CCNL.*

6.5	Responsabilità dopo la cessazione o il cambio d'impiego	**Controllo** Le responsabilità e gli obblighi in materia di sicurezza delle informazioni che rimangono validi dopo la cessazione o il cambio d'impiego devono essere definiti, applicati e comunicati al personale pertinente e alle altre parti interessate. (8.1.4)	☒	☐	*Gestita attraverso la sottoscrizione dell'NDA e della politica accettabile degli asset con il verbale di riconsegna degli asset.* *4_M_A.13.2.4 Accordo di Riservatezza (NDA)*
6.6	Accordi di riservatezza o di non divulgazione	**Controllo** Gli accordi di riservatezza o non divulgazione che riflettono le esigenze dell'organizzazione per la protezione delle informazioni devono essere identificati, documentati, riesaminati regolarmente e firmati dal personale e dalle altre parti interessate pertinenti. (13.2.4)	☒	☐	*Gestita attraverso la sottoscrizione dell'NDA e della politica accettabile degli asset con il verbale di riconsegna degli asset* *Gli accordi sono oggetto di riesame annuale in occasione del riesame della direzione.* *Tutti gli accordi di riservatezza son ostati consegnati ai lavoratori e fatti sottoscrivere.* *4_M_A.13.2.4 Accordo di Riservatezza (NDA)*
6.7	Lavoro a distanza	**Controllo** Quando il personale lavora a distanza, devono essere attuate misure di sicurezza per proteggere le informazioni a cui è possibile accedere o che sono elaborate o memorizzate al di fuori dei locali dell'organizzazione (6.2.2)	☒	☐	*Tutto il personale di Carraro Lab lavora in modalità smart working.* *Tutte le attività lavorative vengono svolte utilizzando strumenti di Google come Google Drive per la memorizzazione dei documenti, e Gmail per le comunicazioni.* *Ogni dipendente ha il proprio account e ha l'obbligo di non salvare documenti sul device utilizzato.* *Stabilita e fatta sottoscrivere l'informativa per il lavoro agile.* *16_M_Mod.Consegna_Riconsegna Device / Carraro_Verbale_Consegna_Device*
6.8	Segnalazione degli eventi relativi alla sicurezza delle informazioni	**Controllo** L'organizzazione deve fornire un meccanismo che consenta al personale di segnalare tempestivamente, attraverso canali appropriati, gli eventi relativi alla sicurezza delle informazioni osservati o sospetti (16.1.2)	☒	☐	*La segnalazione avviene a mezzo mail sull'indirizzo specifico alert@carraro-lab.com* *Le segnalazioni vengono lette dall'Amministratore di Sistema e analizzate insieme alla direzione* *5_M_A.8.1.3 Politica di utilizzo accettabile degli asset*

7	**Controlli fisici**		**APPLICABILITÀ**		**MOTIVAZIONE APPLICABILITA'/NON APPLICABILITA'**
			SI	**NO**	
7.1	Perimetro di sicurezza fisica	**Controllo** I perimetri di sicurezza devono essere definiti e utilizzati per proteggere le aree che contengono le informazioni e gli altri asset relativi. (11.1.1)	☐	☒	*L'organizzazione non opera all'interno della sede, i dipendenti lavorano in smart Working dalle proprie abitazioni.*
7.2	Controlli di accesso fisico	**Controllo** Le aree sicure devono essere protette da adeguati controlli all'ingresso e ai punti di accesso. (11.1.2.)	☐	☒	*L'organizzazione non opera all'interno della sede, i dipendenti lavorano in smart Working dalle proprie abitazioni.*
7.3	Messa in sicurezza di uffici, locali e strutture	**Controllo** La sicurezza fisica di uffici, stanze e strutture deve essere progettata e attuata. (11.1.1)	☐	☒	*L'organizzazione non opera all'interno della sede, i dipendenti lavorano in smart Working dalle proprie abitazioni.*
7.4	Monitoraggio della sicurezza fisica	**Controllo** Le sedi devono essere costantemente monitorate per l'accesso fisico non autorizzato (11.1.1)	☐	☒	*L'organizzazione non opera all'interno della sede, i dipendenti lavorano in smart Working dalle proprie abitazioni.*
7.5	Protezione dalle minacce fisiche e ambientali	**Controllo** Deve essere progettata e attuata la protezione contro le minacce fisiche e ambientali, come i disastri naturali e altre minacce fisiche intenzionali o non intenzionali all'infrastruttura. (11.1.4)	☐	☒	*L'organizzazione non opera all'interno della sede, i dipendenti lavorano in smart Working dalle proprie abitazioni.*
7.6	Lavoro in aree sicure	**Controllo** Devono essere progettate e attuate misure di sicurezza per lavorare in aree sicure. (11.1.5)	☐	☒	*L'organizzazione non opera all'interno della sede, i dipendenti lavorano in smart Working dalle proprie abitazioni.*
7.7	Schermo e scrivania puliti	**Controllo** Devono essere definite e opportunamente applicate regole chiare relative ai documenti cartacei e ai supporti di memorizzazione rimovibili e, per le strutture di elaborazione delle informazioni, regole chiare relative allo schermo. (11.2.9)	☒	☐	*Vedi 5_M_A8.1.3 Politica di utilizzo accettabile degli asset (par.3.2)* *Per il trasferimento dei files gli utenti possono utilizzare solo Google Drive*
7.8	Disposizione delle apparecchiature e loro protezione	**Controllo** Le apparecchiature devono essere posizionate in modo sicuro e protetto. (11.2.1)	☒	☐	*Vedi 5_M_A8.1.3 Politica di utilizzo accettabile degli asset*

7.9	Sicurezza degli asset all'esterno delle sedi	**Controllo** Gli asset al di fuori delle sedi devono essere protetti. (11.2.6)	☒	☐	*Vedi 5_M_A8.1.3 Politica di utilizzo accettabile degli asset*
7.10	Supporti di memorizzazione	**Controllo** I supporti di memorizzazione devono essere gestiti lungo tutto il loro ciclo di vita di acquisizione, uso, trasporto e smaltimento in conformità con lo schema di classificazione dell'organizzazione e con i requisiti di trattamento. (11.2.7)	☒	☐	*Vedi 5_M_A8.1.3 Politica di utilizzo accettabile degli asset* *Non possono essere utilizzati supporti di memorizzazione esterni.* *In caso di dismissione, il disco viene sottoposto a scrittura per la cancellazione dei dati con software Eraser.*
7.11	Infrastrutture di supporto	**Controllo** Le strutture di elaborazione delle informazioni devono essere protette da interruzioni di corrente e altre interruzioni causate da guasti nelle infrastrutture di supporto. (11.2.2)	☒	☐	*Utilizzo di personal computer portatili dotati di batteria, pertanto in caso di interruzione della corrente elettrica, l'operatore ha la possibilità di salvare il lavoro e spegnere il device.* *Vista informativa lavoro agile.*
7.12	Sicurezza dei cablaggi	**Controllo** I cavi che trasportano alimentazione, dati o servizi informativi di supporto devono essere protetti da intercettazioni, interferenze o danni. (11.2.3)	☐	☒	*L'organizzazione non opera all'interno della sede, i dipendenti lavorano in smart Working dalle proprie abitazioni.*
7.13	Manutenzione delle apparecchiature	**Controllo** Le apparecchiature devono essere mantenute correttamente per assicurare la disponibilità, l'integrità e la riservatezza delle informazioni. (11.2.4)	☒	☐	*Il Controllo degli aggiornamenti, e degli errori di sistema dei dispositivi viene effettuato periodicamente (ogni 6 mesi) dall'Amministratore di Sistema.* *Vedi:* *17_M_PROSPETTO ELENCO ASSET (Foglio Registro_Manutenzioni)*
7.14	Dismissione sicura o riutilizzo delle apparecchiature	**Controllo** Prima del loro smaltimento o riutilizzo, gli elementi delle apparecchiature contenenti supporti di memorizzazione devono essere verificati per assicurare che tutti i dati sensibili e il software in licenza siano stati rimossi o sovrascritti in modo sicuro. (11.2.7)	☒	☐	*In caso di dismissione, il disco viene sottoposto a scrittura per la cancellazione dei dati con software Eraser.* *16_Mod. Consegna_Riconsegna Device* *17_M_PROSPETTO ELENCO ASSET (Foglio REGISTRO Asset Dismessi)*

8	**Controlli tecnologici**		**APPLICABILITÀ**		**MOTIVAZIONE APPLICABILITA'/NON APPLICABILITA'**
			SI	**NO**	
8.1	Endpoint degli utenti	**Controllo** Le informazioni memorizzate, elaborate o accessibili tramite gli endpoint degli utenti devono essere protette.	☒	☐	*Le modalità sono indicate all'interno del 5_M_A8.1.3 Politica di utilizzo accettabile degli asset.*
8.2	Diritti di accesso privilegiato	**Controllo** L'assegnazione e l'uso dei diritti di accesso privilegiato devono essere limitati e gestiti. (9.2.3)	☒	☐	*Le modalità sono indicate all'interno del 5_M_A8.1.3 Politica di utilizzo accettabile degli asset.*
8.3	Limitazione degli accessi alle informazioni	**Controllo** Gli accessi alle informazioni e agli altri asset relativi devono essere limitati in conformità con la politica specifica per il controllo degli accessi. (9.4.1)	☒	☐	*Le modalità sono indicate all'interno del 5_M_A8.1.3 Politica di utilizzo accettabile degli asset – par. 3.8*
8.4	Accesso al codice sorgente	**Controllo** L'accesso in lettura e scrittura al codice sorgente, agli strumenti di sviluppo e alle librerie software deve essere gestito in modo appropriato. (9.4.5)	☐	☒	*L'organizzazione commissiona la scrittura del codice alla ditta Cloudbits che detiene il codice sorgente.* *Cloudbits ha un obbligo contrattuale di far accedere Carraro Lab all'ambiente dove si trova il codice sorgente, esclusivamente con la loro supervisione.* *Contratto quadro con Cloudbits (Art.6)*
8.5	Autenticazione sicura	**Controllo** Le tecnologie e le procedure di autenticazione sicura devono essere attuate in base alle limitazioni degli accessi alle informazioni e alla politica specifica per il controllo degli accessi.	☒	☐	*Per Carraro Lab l'Amministratore di Sistema è autorizzato ad accedere a Google Workspace + AWS (con profilo ADMIN), e a gestire gli accessi secondo le varie limitazioni e autorizzazioni, come indicato nel documento:* *5_M_A8.1.3 Politica di utilizzo accettabile degli asset – par. 3.7 e par. 3.8.*
8.6	Gestione della capacità	**Controllo** L'uso delle risorse deve essere monitorato e adeguato in linea con i requisiti di capacità attuali e previsti. (12.1.3)	☒	☐	*Le capacità dei server Aws su cui sono appoggiati i progetti/software vengono monitorati dal fornitore Cloudbits.* *I fornitori monitorano le prestazioni e i requisiti di capacità e segnalano alla direzione di Carraro Lab eventuali esigenze di adeguamenti.* *L'Amministratore di Sistema (in accordo con la Direzione) effettua il monitoraggio periodico della capacità di risorse disponibili su Google Workspace*

					La capacità dei computer portatili utilizzati dai dipendenti è oggetto della manutenzione periodica affidata all'ADS. *Vedi 17_Excel ELENCO ASSET (Foglio Registro Manutenzioni)*
8.7	Protezione dal malware	**Controllo** La protezione dal malware deve essere attuata e supportata da un'adeguata consapevolezza degli utenti. (12.2.1)	☒	☐	*Il controllo dei malware per i PC in dotazione ai dipendenti e all'ADS è affidato al software antivirus (Norton e Defender per macchine con S.O. Windows, mentre per MAC si approva la protezione standard offerta dal sistema operativo* *Protezione anti-malware nativa di macOS (XProtect, Gatekeeper), che viene tenuto aggiornato in automatico dalla singola macchina.* *Vedi:* *5_M_A.8.1.3 Politica di utilizzo accettabile degli asset - Paragrafo 3.3 - Utilizzo della Posta Elettronica* *17_Excel ELENCO ASSET*
8.8	Gestione delle vulnerabilità tecniche	**Controllo** Si devono ottenere informazioni sulle vulnerabilità tecniche dei sistemi informativi in uso, valutare l'esposizione dell'organizzazione a tali vulnerabilità e adottare misure appropriate. (12.6.1)	☒	☐	*Le vulnerabilità dei sistemi su AWS sono affidate operativamente a Cloudbits, con supervisione dell'ADS; entrambi hanno accesso alla console AWS. Cloudbits rileva l'anomalia e segnala malware o vulnerabilità a Carraro Lab.*
8.9	Gestione delle configurazioni	**Controllo** Le configurazioni, comprese le configurazioni di sicurezza, di hardware, software, servizi e reti devono essere stabilite, documentate, attuate, monitorate e riesaminate.	☒	☐	*Le configurazioni di AWS vengono gestite da Cloudbits sulla base delle specifiche date da Carraro Lab, o da quelle provenienti dai capitolati tecnici dei bandi.* *Affidato operativamente a Cloudbits, con supervisione ADS, entrambi hanno accesso a console AWS.* *Le configurazioni dei pc vengono stabilite da Carraro al momento della consegna del device all'operatore, Le configurazioni vengono gestite in base alle esigenze del progetto e gestite dall'Amministratore di Sistema.* *Vedi 16_M_Mod.consegna e riconsegna device*

8.10	Cancellazione delle informazioni	**Controllo** Le informazioni memorizzate nei sistemi informatici, nei dispositivi o in qualsiasi altro supporto di memorizzazione devono essere cancellate quando non sono più necessarie. (8.3.2)	☒	☐	*Vedi 16_M_Mod.consegna e riconsegna device* *I supporti di memorizzazione sono protetti tramite crittografia dell'intero disco (BitLocker su Windows, FileVault su macOS, Eraser dove applicabile).* *Vedi 5_M_A.8.1.3 Politica di utilizzo accettabile degli asset*
8.11	Mascheramento dei dati	**Controllo** Il mascheramento dei dati deve essere utilizzato in conformità con la politica specifica dell'organizzazione per il controllo degli accessi e con gli altri requisiti specifici e di business correlati, tenendo in considerazione le norme di legge applicabili.	☒	☐	*Per le informazioni che necessitano di mascheramento, Carraro Lab provvede all'oscuramento di voli, targhe di automobili o altri elementi sensibili mediante controllo umano diretto, vista l'eterogeneità degli elementi potenzialmente sensibili.* *Il mascheramento avviene comunque nel rispetto del GDPR 679/16 e di eventuali linee guida del garante della Privacy.* *Mod. Liberatoria per utilizzo immagini esterni_GDPR (2026)*
8.12	Prevenzione di leakage delle informazioni	**Controllo** Le misure di prevenzione di leakage dei dati devono essere applicate a sistemi, reti e qualsiasi altro dispositivo che elabora, memorizza o trasmette informazioni sensibili.	☒	☐	*Il sistema AWS è dotato di protezione per la perdita dei dati, tale sistema viene gestito direttamente da AWS.* *Per i documenti prodotti dagli operatori di Carraro, la protezione è affidata alle modalità di sicurezza di Google Drive.* *La trasmissione di informazioni avviene sempre mantenendo il file originale in Google Drive. Gli account di posta elettronica sono gestiti da Google Workspace pertanto soggetti a backup e conservazione con modalità cloud.* *Vedi 4_M_A.13.2.4 Accordo Riservatezza – Dipendenti - Rif. Art.3 Punto e)*
8.13	Backup delle informazioni	**Controllo** Le copie di backup di informazioni, software e sistemi devono essere mantenute e testate regolarmente secondo quanto stabilito dalla politica specifica per il backup. (12.3.1)	☒	☐	*Il backup viene effettuato su Google Workspace, tramite la sincronizzazione automatica delle cartelle di lavoro.* *Per quanto riguarda gli applicativi software, il backup viene effettuato su AWS.* *17_Excel ELENCO ASSET Foglio Registro_BACKUP*

8.14	Ridondanza delle strutture di elaborazione delle informazioni	**Controllo** Le strutture di elaborazione delle informazioni devono essere attuate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità. (17.2.1)	☒	☐	*La ridondanza dei sistemi interni è garantita dal fatto che si può accedere all'account di Google utilizzando un qualunque altro device collegato ad internet.* *Lato utente software la ridondanza è garantita dall'architettura di AWS.*
8.15	Raccolta di log	**Controllo** I log che registrano attività, eccezioni, guasti e altri eventi significativi devono essere prodotti, memorizzati, protetti e analizzati. (12.4.1)	☒	☐	*Su Google Drive vengono mantenuti i log relativi agli accessi degli account e alle attività svolte sui documenti.* *Per AWS i log vengono gestiti dal fornitore principale Cloudbits e forniti in caso di richiesta.*
8.16	Attività di monitoraggio	**Controllo** Reti, sistemi e applicazioni devono essere monitorati relativamente a comportamenti anomali e dovrebbero essere intraprese azioni appropriate per valutare potenziali incidenti relativi alla sicurezza delle informazioni.	☒	☐	*Il controllo dei sistemi viene affidato a Cloudbits.*
8.17	Sincronizzazione degli orologi	**Controllo** Gli orologi dei sistemi di elaborazione delle informazioni utilizzati dall'organizzazione devono essere sincronizzati con origini temporali approvate. (12.4.4)	☒	☐	*Gli orologi di sistema dei dispositivi sono sincronizzati automaticamente tramite il protocollo NTP (Network Time Protocol), affidandosi ai servizi di sincronizzazione oraria integrati nel sistema operativo. I dispositivi Windows utilizzano il servizio Windows Time (W32Time), mentre i dispositivi macOS utilizzano il servizio integrato (timed), connettendosi a server orari attendibili (ad esempio time.windows.com, time.apple.com o time.nist.gov) per garantire l'esattezza di data e ora.*
8.18	Utilizzo di programmi di utilità privilegiati	**Controllo** L'uso di programmi di utilità che possono essere in grado di ignorare i controlli del sistema e delle applicazioni deve essere limitato e strettamente controllato. (9.4.4)	☒	☐	*16 M_Mod_Consegna_riconsegna device par. 4 Politica aziendale e responsabilità del dipendente.* *Prevista l'installazione di software provvisti di firma.*
8.19	Installazione del software sui sistemi in esercizio	**Controllo** Devono essere attuate procedure e misure per gestire in modo sicuro l'installazione del software sui sistemi in esercizio. (12.5.1)	☒	☐	*16 M_Mod_Consegna_riconsegna device par. 4 Responsabilità del dipendente.* *Prevista l'installazione di software provvisti di firma.* *Tutti i software installati sono dotati di licenza originale.*

					L'ADS si occupa dell'installazione, e della scelta del software più adatto alle esigenze dell'azienda, in accordo con la Direzione.
8.20	Sicurezza delle reti	**Controllo** Le reti e i dispositivi di rete devono essere protetti, gestiti e controllati per proteggere le informazioni nei sistemi e nelle applicazioni.	☒	☐	*16 M_Mod_Consegna_riconsegna device par. 4 Responsabilità del dipendente.*
8.21	Sicurezza dei servizi di rete	**Controllo** I meccanismi di sicurezza, i livelli di servizio e i requisiti dei servizi di rete devono essere identificati, attuati e monitorati. (13.1.1)	☒	☐	*16 M_Mod_Consegna_riconsegna device par. 4 Responsabilità del dipendente.*
8.22	Segregazione delle reti	**Controllo** I gruppi di servizi informativi, di utenti e di sistemi informativi devono essere segregati nelle reti dell'organizzazione. (13.1.3)	☒	☐	*16 M_Mod_Consegna_riconsegna device par. 4 Responsabilità del dipendente.*
8.23	Web filtering	**Controllo** L'accesso a siti web esterni deve essere gestito per ridurre l'esposizione a contenuti dannosi.	☒	☐	*La protezione dalla navigazione verso siti malevoli è affidata ai meccanismi di sicurezza integrati nei sistemi operativi (Microsoft Defender SmartScreen su Windows, le protezioni integrate di macOS e del browser su Mac) e al modulo di web protection dell'antivirus installato, che bloccano l'accesso a siti di phishing e malware noti. Non è applicato un filtraggio per categorie di contenuti, in quanto non sono definite categorie di siti non consentite.*
8.24	Uso della crittografia	**Controllo** Per l'uso efficace della crittografia devono essere definite e attuate regole, inclusa la gestione delle chiavi crittografiche. (10.1.1 – 10.1.2)	☒	☐	*Sui singoli device è attivata la crittografia dell'intero disco (full-disk encryption) fornita nativamente dal sistema operativo: BitLocker su Windows e FileVault su macOS.*
8.25	Ciclo di vita dello sviluppo sicuro	**Controllo** Devono essere stabilite e applicate regole per lo sviluppo sicuro di software e sistemi. (14.2.1)	☒	☐	*Le regole/requisiti sono indicate nei documenti contrattuali con il cliente.* *In fase di sviluppo vengono analizzati i requisiti di sicurezza come previsto dalla procedura PRO Progettazione e sviluppo (integrata con Sistema ISO9001).*
8.26	Requisiti di sicurezza delle applicazioni	**Controllo** I requisiti di sicurezza delle informazioni devono essere identificati, specificati e approvati durante lo sviluppo o l'acquisizione di applicazioni.	☒	☐	*I requisiti di sicurezza sono identificati all'interno dei documenti tecnici richiesti dal cliente ed approvati nella fase contrattuale.*

8.27	Sicurezza dell'architettura dei sistemi e dei principi di ingegnerizzazione	**Controllo** I principi per l'ingegnerizzazione di sistemi sicuri devono essere stabiliti, documentati, mantenuti e applicati a qualsiasi attività di sviluppo dei sistemi informativi.	☒	☐	*Elaborato documento di analisi funzionale nel quale vengono stabiliti, documenti i principi di ingegnerizzazione per la sicurezza dei sistemi progettati e prodotti.* *Vedi 20_STARTUP GENERATOR Documento di Analisi Funzionale*
8.28	Sviluppo sicuro	**Controllo** I principi di sviluppo sicuro devono essere applicati allo sviluppo del software. (14.2.1)	☐	☒	*L'organizzazione applica la regola "Sicurezza by design" pertanto lo sviluppo del software avviene in maniera sicura*
8.29	Test di sicurezza in fase di sviluppo e di accettazione	**Controllo** I processi di test di sicurezza devono essere definiti e attuati nel ciclo di vita dello sviluppo. (14.28 – 14.2.9)	☒	☐	*1-9_M_6.1.3_All. Penetration Test* *L'ADS verifica l'esecuzione della procedura, che deve essere effettuata annualmente.*
8.30	Sviluppo affidato all'esterno	**Controllo** L'organizzazione deve dirigere, monitorare e riesaminare le attività di sviluppo dei sistemi affidate all'esterno. (14.2.7)	☒	☐	*Le attività di sviluppo e monitoraggio dei processi vengono coordinate con Cloudbits, attraverso lo scambio di mail.*
8.31	Separazione degli ambienti di sviluppo, test e produzione	**Controllo** Gli ambienti di sviluppo, test e produzione devono essere separati e protetti. (12.1.4)	☒	☐	*Lo sviluppo e la produzione vengono eseguiti da Cloudbits,* *mentre Carraro Lab esegue i test sugli sviluppi.* *La separazione degli ambienti viene garantita anche nel caso di sviluppi e test per cliente finale.*
8.32	Gestione dei cambiamenti	**Controllo** I cambiamenti alle strutture di elaborazione delle informazioni e ai sistemi informativi devono essere soggetti a procedure di gestione dei cambiamenti. (12.1.2)	☒	☐	*Istituito a livello di sistema un modulo di registrazione che consente di poter effettuare un'analisi relativa a qualunque tipologia di cambiamento che potrebbe comportare un impatto sul sistema di gestione o sulla sicurezza delle informazioni.* *Vedi 24_M_Gestione del cambiamento*
8.33	Dati di test	**Controllo** I dati di test devono essere scelti, protetti e gestiti opportunamente. (14.3.1)	☒	☐	*I dati di test vengono gestiti direttamente dal fornitore esterno Cloudbits e messi a disposizione in caso di richiesta da parte di Carraro Lab.*

8.34	Protezione dei sistemi informativi durante il test di audit	**Controllo** Il test di audit e le altre attività di garanzia che prevedono la valutazione dei sistemi di produzione devono essere pianificati e concordati tra chi li effettua e l'appropriato livello manageriale. (14.3.1)	☒	☐	*Gli audit tecnici (vulnerability scan, security review) sono pianificati e gestiti per garantire la protezione dei sistemi durante il test. Sarà definita finestra programmata fuori orario di punta, comunicazione preventiva al team, backup pre-test, rollback plan predisposto. I report dei vulnerability assessment vengono archiviati su GoogleDrive* *1-9_M_6.1.3_All. 8.29_ Penetration Test*