SOA - Statement of Applicability - DICHIARAZIONE DI APPLICABILITA' ISO /IEC 27001:2022 - Annex A

Lo scopo di questo documento è definire, in relazione alla SICUREZZA DELLE INFORMAZIONI, quali controlli sono adeguati per essere implementati in DELLORTO SPA, gli obiettivi di tali controlli e come vengono implementati.
Questo documento include tutti i controlli elencati nell'Allegato A della norma ISO 27001. I controlli sono applicabili all'intero ambito del Sistema di GESTIONE INTEGRATO, con particolare riferimento al Sistema di Gestione della Sicurezza delle Informazioni .

Area	Id Controllo	Titolo	Applicabilità (YES/NO)	Giustificazione in caso di "NO"	Metodo di implementazione
	A.5.1	Politiche per la sicurezza delle informazioni	YES		Tutte le Policy e tutta la documentazione per la sicurezza delle informazioni sono gestite attraverso il SGI - Sistema di Gestione Integrato DELLORTO
	A.5.2	Ruoli e responsabilità della sicurezza delle informazioni	YES		DELLORTO ha nominato il responsabile per la sicurezza delle informazioni e il Referente Privacy interno.
	A.5.3	Separazione dei compiti	YES		I compiti associati alla sicurezza delle informazioni seguono flussi di approvazione a più livelli
	A.5.4	Responsabilità della Direzione	YES		Il Managment di DELLORTO sostiene attivamente la sicurezza delle informazioni attraverso la verifica che il SGI sia implementato e attivo
	A.5.5	Contatti con le autorità	YES		DELLORTO ha adottato ed efficacemente attuato il modello organizzativo Dlgs 231/2001. P.DG.02 - Principi del modello organizzativo 231 P.DG. 07 - Valutazione del Rischio e gestione delle emergenza per la business continuity P.DG.03 - Procedura Whistleblowing P.DG.11 - Procedura Gestione Data Breach
	A.5.6	Contatti con gruppi specialistici	YES		P.ICT.06 ProceduraInformationSecurity P.ICT.01 Incident management
	A.5.7	Monitoraggio delle minacce (Threat Intelligence)	YES		P.ICT.06 ProceduraInformationSecurity P.ICT.01 Incident management
	A.5.8	Sicurezza delle informazioni nella gestione dei progetti	YES		P.ICT.05 ChangeManagement P.ICT.10 - Sviluppo Sicuro
	A.5.9	Inventario delle informazioni e di altri assets associati	YES		DELLORTO dispone di tools specifici per l'inventario degli asset associati alla sicurezza delle informazioni
	A.5.10	Uso accettabile delle informazioni e di altri beni associati	YES		DELLORTO ha definito un regolamento aziendale associato all'utilizzo degli strumenti informatici ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali Lettere di incarico
	A.5.11	Restituzione degli asset	YES		DELLORTO ha definito un regolamento aziendale associato all'utilizzo degli strumenti informatici ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali I.ICT 04 Rev.00_DimissioneUtenza I.ICT 05 Rev.00_RItiroDismissioneHardware M.ICT 01 Rev.00_ConsegnaRestituzioneDotazioni
	A.5.12	Classificazione delle informazioni	YES		DELLORTO ha classifica differenti livelli di riservatezza delle informazioni in funzione del potenziale impatto sulla business continuity P.DG.09 - Gestione Documentazione
	A.5.13	Etichettatura delle informazioni	YES		DELLORTO identifica differenti livelli di riservatezza delle informazioni in funzione del potenziale impatto sulla business continuity P.DG.09 - Gestione Documentazione
	A.5.14	Trasferimento di informazioni	YES		DELLORTO identifica differenti metodologie di trasferimento delle informazione in base al grado di riservatezza identificato P.DG.09 - Gestione Documentazione
	A.5.15	Controllo degli accessi	YES		DELLORTO mette in atto procedure finalizzate a garantire il controllo di accessi fisici e informatici alle informazioni ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali P.ICT.06 ProceduraInformationSecurity P.ICT.07 misure di Sicurezza Fisica ICT P.FHS.01 Gestione accessi personale interno P.FHS.02 Gestione accessi personale esterno
	A.5.16	Identity management	YES		DELLORTO mette in atto procedure finalizzate a garantire l'accesso alle informazione solo a personale autorizzato I.ICT 03 rev.00 - Nuova postazione di lavoro I.ICT 04 rev.00 - Dismissione utenza I.ICT 05 Rev.00 - RItiro Dismissione Hardware I.ICT 06 rev.00 - Cambio ruolo ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali P.ICT.06 ProceduraInformationSecurity(5.6);
	A.5.17	Informazioni sull'autenticazione	YES		DELLORTO mette in atto procedure finalizzate a garantire l'accesso alle informazione solo a personale autorizzato I.ICT 03 rev.00 - Nuova postazione di lavoro I.ICT 04 rev.00 - Dismissione utenza I.ICT 05 Rev.00 - RItiro Dismissione Hardware I.ICT 06 rev.00 - Cambio ruolo ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali P.ICT.06 ProceduraInformationSecurity(5.6);

A.5 Organizzazione	A.5.18	Diritti di Accesso	YES	DELLORTO mette in atto procedure finalizzate a garantire l'accesso alle informazione solo a personale autorizzato I.ICT 03 rev.00 - Nuova postazione di lavoro I.ICT 04 rev.00 - Dismissione utenza I.ICT 05 Rev.00 - RItiro Dismissione Hardware I.ICT 06 rev.00 - Cambio ruolo ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali P.ICT.06 ProceduraInformationSecurity(5.6);
	A.5.19	Sicurezza delle informazioni nei rapporti con i fornitori	YES	DELLORTO implementa procedure atte a ridurre il rischio legato al trasferimento delle proprie informazioni lungo la catena di fornitura attraverso strumenti di scambio dati sicuri, Procedure del proprio SGI e richiedendo NDA specifici. P.PPD.03-NDA Non Disclosure Agreement PPD-06-Gestione Vendor List P.DG.13 - Manuale di conservazione Incarichi amministratori di sistema PDG 09- Gestione della documentazione P.QA.06 - Supplier Quality Manual
	A.5.20	Gestione della sicurezza delle informazioni all'interno degli accordi con i fornitori	YES	DELLORTO implementa procedure atte a ridurre il rischio legato al trasferimento delle proprie informazioni lungo la catena di fornitura attraverso strumenti di scambio dati sicuri, Procedure del proprio SGI e richiedendo NDA specifici. P.PPD.03-NDA Non Disclosure Agreement PPD-06-Gestione Vendor List P.DG.13 - Manuale di conservazione Incarichi amministratori di sistema PDG 09- Gestione della documentazione P.QA.06 - Supplier Quality Manual
	A.5.21	Gestione della sicurezza delle informazioni nella catena di fornitura in ambito ICT.	YES	DELLORTO implementa procedure atte a ridurre il rischio legato al trasferimento delle proprie informazioni lungo la catena di fornitura attraverso strumenti di scambio dati sicuri, Procedure del proprio SGI e richiedendo NDA specifici. P.PPD.03-NDA Non Disclosure Agreement PPD-06-Gestione Vendor List P.DG.13 - Manuale di conservazione Incarichi amministratori di sistema PDG 09- Gestione della documentazione P.QA.06 - Supplier Quality Manual
	A.5.22	Monitoraggio, revisione e gestione del cambiamento dei servizi dei fornitori	YES	DELLORTO implementa procedure atte a ridurre il rischio legato al trasferimento delle proprie informazioni lungo la catena di fornitura attraverso strumenti di scambio dati sicuri, Procedure del proprio SGI e richiedendo NDA specifici. P.PPD.03-NDA Non Disclosure Agreement PPD-06-Gestione Vendor List P.DG.13 - Manuale di conservazione Incarichi amministratori di sistema PDG 09- Gestione della documentazione P.QA.06 - Supplier Quality Manual P.ICT.05 ChangeManagement
	A.5.23	Sicurezza delle informazioni per l'utilizzo dei servizi cloud	YES	DELLORTO implementa procedure atte a ridurre il rischio legato al trasferimento delle proprie informazioni lungo la catena di fornitura attraverso strumenti di scambio dati sicuri, Procedure del proprio SGI e richiedendo NDA specifici. Si avvale inoltre dei servizi Cloud per il proprio Backup su DataCenter certificati TIER IV P.PPD.03-NDA Non Disclosure Agreement PPD-06-Gestione Vendor List P.DG.13 - Manuale di conservazione Incarichi amministratori di sistema PDG 09- Gestione della documentazione P.QA.06 - Supplier Quality Manual P.ICT.02 Procedura di Backup
	A.5.24	Pianificazione e preparazione della gestione degli incidenti di sicurezza delle informazioni	YES	DELLORTO attua, sulla base della valutazione del rischio,opportuni piani per la gestione degli incidenti, prevedendo procedure per la minimizzazione dell'impatto sulla sicurezza delle informazioni P.DG. 07 - Valutazione del Rischio e gestione delle emergenza per la business continuity ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali P.ICT.01 Incident management P.ICT.02 Procedura di Backup P.ICT.03 Disaster Recovery P.ICT.06 ProceduraInformationSecurity P.DG.03 - Procedura Whistleblowing P.DG.11 - Procedura Gestione Data Breach M.ICT 04- Pianificazione-RegistroTest_Incident
	A.5.25	Valutazione e decisione su eventi di sicurezza informatica	YES	DELLORTO attua, sulla base della valutazione del rischio,opportuni piani per la gestione degli incidenti, prevedendo procedure per la minimizzazione dell'impatto sulla sicurezza delle informazioni P.DG. 07 - Valutazione del Rischio e gestione delle emergenza per la business continuity ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali P.ICT.01 Incident management P.ICT.02 Procedura di Backup P.ICT.03 Disaster Recovery P.ICT.06 ProceduraInformationSecurity P.DG.03 - Procedura Whistleblowing P.DG.11 - Procedura Gestione Data Breach M.ICT 04- Pianificazione-RegistroTest_Incident

	A.5.26	Risposta agli incidenti di sicurezza delle informazioni	YES		DELLORTO attua, sulla base della valutazione del rischio,opportuni piani per la gestione degli incidenti, prevedendo procedure per la minimizzazione dell'impatto sulla sicurezza delle informazioni P.DG. 07 - Valutazione del Rischio e gestione delle emergenza per la business continuity ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali P.ICT.01 Incident management P.ICT.02 Procedura di Backup P.ICT.03 Disaster Recovery P.ICT.06 ProceduraInformationSecurity P.DG.03 - Procedura Whistleblowing P.DG.11 - Procedura Gestione Data Breach M.ICT 04- Pianificazione-RegistroTest_Incident
	A.5.27	Imparare dagli incidenti di sicurezza delle informazioni	YES		DELLORTO riesamina periodicamente i piani di emergenza e gli incidenti ed attua le oppurtune azioni preventive e di sistema secondo la logica del miglioramento continuo. P.DG. 08 - Miglioramento continuo P.DG. 07 - Valutazione del Rischio e gestione delle emergenza per la business continuity ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali P.ICT.01 Incident management P.ICT.02 Procedura di Backup P.ICT.03 Disaster Recovery P.ICT.06 ProceduraInformationSecurity P.DG.03 - Procedura Whistleblowing P.DG.11 - Procedura Gestione Data Breach M.ICT 04- Pianificazione-RegistroTest_Incident
	A.5.28	Raccolta di evidenze	YES		DELLORTO riesamina periodicamente le registrazioni per preventive o verificare gli eventi di sicurezza delle informazioni secondo la logica del miglioramento continuo. P.DG. 08 - Miglioramento continuo P.DG. 07 - Valutazione del Rischio e gestione delle emergenza per la business continuity ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali P.ICT.01 Incident management P.ICT.02 Procedura di Backup P.ICT.03 Disaster Recovery P.ICT.06 ProceduraInformationSecurity P.DG.03 - Procedura Whistleblowing P.DG.11 - Procedura Gestione Data Breach M.ICT 04- Pianificazione-RegistroTest_Incident P.ICT.09 - Gestione LOG
	A.5.29	Sicurezza delle informazioni durante l'interruzione	YES		DELLORTO ha definito un piano di reazione agli incidenti per rispondere al meglio alle richieste di Business continuity aziendale P.ICT.03 Disaster Recovery P.ICT.07 misure di Sicurezza Fisica ICT M.ICT 04- Pianificazione-RegistroTest_Incident
	A.5.30	Prontezza ICT per la continuità operativa	YES		DELLORTO ha definito un piano di reazione agli incidenti per rispondere al meglio alle richieste di Business continuity aziendale P.ICT.03 Disaster Recovery P.ICT.07 misure di Sicurezza Fisica ICT M.ICT 04- Pianificazione-RegistroTest_Incident
	A.5.31	Requisiti legali, statutari, regolamentari e contrattuali	YES		DELLORTO gestisce i legal e contractual requirement attraverso software informatici
	A.5.32	Diritti di proprietà intellettuale	YES		DELLORTO gestisce e protegge i propri brevetti attraverso il processo interno di Innovazione
	A.5.33	Protezione dei record	YES		DELLORTO ha implementato delle politiche di gestione per le verifiche periodiche del LOG di sistema e delle politiche per uno sviluppo del software P.ICT.09 - Gestione LOG P.ICT.10 - Sviluppo Sicuro
	A.5.34	Privacy e protezione delle informazioni personali identificabili (PII)	YES		DELLORTO ha nominato un Referente interno Privacy ed rispetta la normativa GDPR Regolamento (UE) 2016/679
	A.5.35	Riesame indipendente della sicurezza delle informazioni	YES		DELLORTO si sottopone ad audit periodici da parte di Enti di Certificazione secondo lo standard ISO 27001 P.QA - 09 Gestione Audit Audit Esterni Privacy, Audit dell'organismo di vigilanza secondo DLgs231 Riesame della direzione
	A.5.36	Conformità a politiche, regole e standard per la sicurezza delle informazioni	YES		DELLORTO si sottopone ad audit periodici da parte di Enti di Certificazione secondo lo standard ISO 27001 P.QA - 09 Gestione Audit Audit Esterni Privacy, Audit dell'organismo di vigilanza secondo DLgs231 Riesame della direzione
	A.5.37	Procedure operative documentate	YES		DELLORTO dispone di un Sistema di Gestione Integrato secondo gli standard IATF16949, ISO 9001, ISO 14001, ISO 27001 che viene periodicamente revisionato e la cui applicazione viene auditata.
	A.6.1	Screening	YES		DELLORTO si avvale di procedure interne per la selezione del proprio personale, avvalendosi anche di referenze se disponibili. P.HR.01: Procedura ricerca, selezione del personale. P.DG.01: Codice Etico P.DG.02: Modello di ordganizzazione e controllo ai sensi del D.Lgs. 231/01
	A.6.2	Termini e condizioni di impiego	YES		P.HR.04: Gestione del personale con rapporto di lavoro subordinato P.HR.05: Gestione del personale in stage/borsisti P.HR.06: Gestione del personale con contratto di collaborazione coordinata e continuativa coordinata e continuativa

A.6 Persone	A.6.3	Sensibilizzazione, istruzione e formazione sulla sicurezza delle informazioni	YES		DELLORTO pianifica e somministra la formazione in relazione alla sicurezza delle informazioni avvalendosi di procedure interne e di una piattaforma di E-Learning per la formazione capillare. L'efficacia della formazione è valutata attraverso oppuortuni test. P.HR.02 - Procedura Formazione motivazione e consapevolezza test Phishing P.ICT.06 ProceduraInformationSecurity
	A.6.4	Processo disciplinare	YES		All'atto dell'assunzione DELLORTO sottopone clausule legate alla riservatezza delle informazioni applicazione CCNL ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali
	A.6.5	Responsabilità dopo il licenziamento o il cambio di rapporto di lavoro	YES		All'atto dell'assunzione DELLORTO sottopone clausule legate alla riservatezza delle informazioni; in casi specifici vengono stiulati accordi di non concorrenza. applicazione CCNL ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali
	A.6.6	Accordi di riservatezza o non divulgazione	YES		All'atto dell'assunzione DELLORTO sottopone clausule legate alla riservatezza delle informazioni; in casi specifici vengono stiulati accordi di non concorrenza. applicazione CCNL ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali
	A.6.7	Remote working	YES		DELLORTO si avvale di connessioni VPN sicure per lavori da remoto
	A.6.8	Segnalazione di eventi di sicurezza delle informazioni	YES		DELLORTO ha definito le procedure interne per la segnalazione degli eventi di sicurezza delle informazioni P.DG.11 - Procedura Gestione Data Breach P.DG.03 - Procedura Whistleblowing Pianificazione-RegistroTest_Incident P.ICT.06 ProceduraInformationSecurity ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali
A.7 Controlli fisici	A.7.1	Perimetri di sicurezza fisica	YES		DELLORTO protegge il perimetro fisico con zone ad accesso limitato tramite badge autorizzato. E' protetta da sistemi di videorsorveglianza e antintrusione. Sono presenti sistemi antincendio, protezione elettrica e contro il calore. Il monitoraggio avviene tramite sensoristica Software e Hardware. P.FHS.01 - Gestione accessi personale interno P.FHS.02 - Gestione accessi personale esterno P.ICT.07 - Misure di Sicurezza Fisica ICT
	A.7.2	Ingresso fisico	YES		DELLORTO ha implementato delle procedure per regolamentare l'accesso fisico del personale dipendente ed esterni. P.FHS.01 - Gestione accessi personale interno P.FHS.02 - Gestione accessi personale esterno P.ICT.07 - Misure di Sicurezza Fisica ICT
	A.7.3	Messa in sicurezza di uffici, locali e strutture	YES		DELLORTO ha implementato delle procedure per regolamentare l'accesso fisico del personale dipendente ed esterni. P.FHS.01 - Gestione accessi personale interno P.FHS.02 - Gestione accessi personale esterno P.ICT.07 - Misure di Sicurezza Fisica ICT
	A.7.4	Monitoraggio della sicurezza fisica	YES		DELLORTO ha implementato delle procedure per regolamentare l'accesso fisico del personale dipendente ed esterni.Ogni accesso viene registrato all'interno dei software di gestione delle presenze. P.FHS.01 - Gestione accessi personale interno P.FHS.02 - Gestione accessi personale esterno P.ICT.07 - Misure di Sicurezza Fisica ICT
	A.7.5	Protezione contro le minacce fisiche e ambientali	YES		DELLORTO protegge il perimetro fisico con zone ad accesso limitato tramite badge autorizzato. E' protetta da sistemi di videorsorveglianza e antintrusione. Sono presenti sistemi antincendio, protezione elettrica e contro il calore. Il monitoraggio avviene tramite sensoristica Software e Hardware. P.FHS.01 - Gestione accessi personale interno P.FHS.02 - Gestione accessi personale esterno P.ICT.07 - Misure di Sicurezza Fisica ICT
	A.7.6	Lavorare in aree sicure	YES		DELLORTO protegge il perimetro fisico con zone ad accesso limitato tramite badge autorizzato. E' protetta da sistemi di videorsorveglianza e antintrusione. Sono presenti sistemi antincendio, protezione elettrica e contro il calore. Il monitoraggio avviene tramite sensoristica Software e Hardware. P.FHS.01 - Gestione accessi personale interno P.FHS.02 - Gestione accessi personale esterno P.ICT.07 - Misure di Sicurezza Fisica ICT
	A.7.7	Clear desk and clear screen	YES		DELLORTO definisce le linee guida per ridurre il rischio di violazioni di sicurezza delle informazioni presenti nelle postazioni di lavoro P.DG.12 - Procedura clear desk e clear screen
	A.7.8	Ubicazione e protezione delle apparecchiature	YES		DELLORTO protegge i datacenter aziendali con protezioni fisiche di antintrusione, antincendio, condizionamento. P.FHS.01 - Gestione accessi personale interno P.ICT.07 - Misure di Sicurezza Fisica ICT
	A.7.9	Sicurezza degli assets fuori sede	YES		DELLORTO definisce le linee guida per ridurre il rischio di violazioni di sicurezza delle informazioni quando i device sono all'esterno dell'azienda P.ICT.06 ProceduraInformationSecurity ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali I.ICT 05_RItiroDismissioneHardware
	A.7.10	Supporti di memorizzazione	YES		DELLORTO definisce le linee guida per ridurre il rischio di violazioni di sicurezza delle informazioni sull'utilizzo di supporti di memorizzazione e la rimozione sicura dei dati prima dello smaltimento P.ICT.06 ProceduraInformationSecurity ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali I.ICT 05_RItiroDismissioneHardware
	A.7.11	Utilità di supporto	YES		DELLORTO ha predisposto delle utilità di supporto per la continuità operativa. P.DG. 07 - Valutazione del Rischio e gestione delle emergenza per la business continuity P.ICT.07 Misure di Sicurezza Fisica ICT

	A.7.12	Sicurezza del cablaggio	YES		I cavi elettrici e dati sono installati all'interno di armadi protetti dell'organizzazione e, ove ciò non sia possibile, sono protetti da pressacavi e/o canaline protette
	A.7.13	Manutenzione degli apparati	YES		La manutenzione dei sistemi necessari al corretto funzionamento del DATA CENTER sono gestiti da un fornitori esterni e un planning di manutenzione che DELLORTO gestisce attraverso un software dedicato. La registrazione dell'intervento e il suo esito vengono archiviati dal dipartimento FHS
	A.7.14	Smaltimento sicuro o riutilizzo delle apparecchiature	YES		DELLORTO definisce le linee guida per ridurre il rischio di violazioni di sicurezza delle informazioni sull'utilizzo di supporti di memorizzazione e la rimozione sicura dei dati prima dello smaltimento P.ICT.06 ProceduraInformationSecurity ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali I.ICT 05_RItiroDismissioneHardware
A.8 Controlli tecnologici	A.8.1	User end point devices	YES		ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali P.ICT.06 ProceduraInformationSecurity
	A.8.2	Diritti di accesso privilegiati	YES		ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali P.ICT.06 ProceduraInformationSecurity
	A.8.3	Restrizione all'accesso alle informazioni	YES		ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali P.ICT.06 ProceduraInformationSecurity
	A.8.4	Accesso al codice sorgente	YES		Il codice sorgente del programma viene preservato e solo l'ICT e il responsabile del gruppo ICT hanno i diritti di accesso P.ICT.10 rev.00 - Sviluppo Sicuro
	A.8.5	Autenticazione sicura	YES		Esiste un processo di accesso sicuro per tutti i computer della rete P.ICT.06 ProceduraInformationSecurity ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali
	A.8.6	Capacity management	YES		DELLORTO si avvale di KPI per il monitoraggio della capacità dei cluster. L'ICT è responsabile del monitoraggio dell'uso delle risorse ICT e della pianificazione della capacità richiesta
	A.8.7	Protezione contro i malware	YES		DELLORTO utilizza vari sistemi di protezione contro i malware. Sono presenti Firewall, EndPoint e sistemi di Backup. Effettua Phishing testpiù volte l'anno ai dipendenti per mantenere alta l'attenzione su rischi P.ICT.06 ProceduraInformationSecurity P.ICT.04 Gestione patching P.ICT.02 Procedura di Backup
	A.8.8	Gestione delle vulnerabilità tecniche	YES		DELLORTO attua una politica di costante aggiornamento su tutti i sistemi P.ICT.04 Gestione patching
	A.8.9	Configuration management	YES		DELLORTO attua una politica di costante aggiornamento su tutti i sistemi il servizio ICT annualmente effettua una verifica sull'obsolescenza dei sistemi informatizi presenti in azienda e presenta un piano di miglioramento al RIesame della Direzione P.ICT.04 Gestione patching
	A.8.10	Cancellazione delle informazioni	YES		DELLORTO definisce le linee guida per ridurre il rischio di violazioni di sicurezza delle informazioni sull'utilizzo di supporti di memorizzazione e la rimozione sicura dei dati prima dello smaltimento P.ICT.06 ProceduraInformationSecurity ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali I.ICT 05_RItiroDismissioneHardware Data Retention Policy
	A.8.11	Mascheramento dei dati (Data masking)	YES		L'anonimizzazione e il mascheramento dei dati rispetta la normativa GDPR Regolamento (UE) 2016/679
	A.8.12	Prevenzione della fuga di dati	YES		All'atto dell'assunzione DELLORTO sottopone clausule legate alla riservatezza delle informazioni; in casi specifici vengono stiulati accordi di non concorrenza. applicazione CCNL. Viene inotre regolamnetata l'utilizzo di supporti di memorizzazione di massa, navigazione siti WebMail, siti Scambio Dati. Lettere di incarico per i dati trattati Classificazione delle informazioni ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali GDPR Regolamento (UE) 2016/679
	A.8.13	Backup delle informazioni	YES		DELLORTO attua politiche di backup multi sede avendo definito opportuni target RTO/RPO. P.ICT.02 Procedura di Backup P.ICT.06 ProceduraInformationSecurity M.ICT 04- Pianificazione-RegistroTest_Incident
	A.8.14	Ridondanza delle strutture di elaborazione delle informazioni	YES		P.ICT.07 misure di Sicurezza Fisica ICT M.ICT 04- Pianificazione-RegistroTest_Incident P.DG. 07 - Valutazione del Rischio e gestione delle emergenza per la business continuity P.ICT.02 Procedura di Backup P.ICT.03 Disaster Recovery
	A.8.15	Gestione dei Log	YES		DELLORTO attua una procedura che prevede il monitoraggio giornaliero dei LOG P.ICT.09 - Gestione LOG
	A.8.16	Attività di monitoraggio	YES		DELLORTO monitora tutti i processi attraverso opportuni KPI. Attua inoltre una procedura che prevede il monitoraggio giornaliero dei LOG P.ICT.09 Gestione LOG P.ICT.06 ProceduraInformationSecurity I.ICT 11 KPI
	A.8.17	Sincronizzazione dell'orologio	YES		Tutti gli orologi sei sistemi sono sincronizzati con il Domani Controller P.ICT.06 ProceduraInformationSecurity
	A.8.18	Utilizzo di programmi di utilità privilegiati	YES		Solo il personale ICT e il responsabile ICT hanno il diritto di utilizzare utilità privilegiate. Il codice sorgente del programmi viene preservato e solo l'ICT e il responsabile ICT hanno i diritti di accesso ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali P.ICT.10 - Sviluppo Sicuro
	A.8.19	Installazione di software su sistemi operativi	YES		DELLORTO ha adottato un Regolamento Aziendale per fornire le linee guida sull'utilizzo degli strumenti informatici. Non è consentito, se non con autorizzazione del servizio ICT, l'installazione di software su qualsiasi dispositivo aziendale ALL 6_SIC.DATI_Regolamento aziendale e norme comportamentali

A.8.20	Sicurezza delle reti	YES		DELLORTO ha implementato sistemi di sicurezza per proteggere e monitorare la Rete aziendale e tutti i servizi pubblicati. P.ICT.06 ProceduraInformationSecurity
A.8.21	Sicurezza dei servizi di rete	YES		DELLORTO ha implementato sistemi di sicurezza per proteggere e monitorare la Rete aziendale e tutti i servizi pubblicati. P.ICT.06 ProceduraInformationSecurity
A.8.22	Segregazione delle reti	YES		DELLORTO ha implementato sistemi di sicurezza per proteggere e monitorare la Rete aziendale e tutti i servizi pubblicati. P.ICT.06 ProceduraInformationSecurity
A.8.23	Web filtering	YES		DELLORTO ha implementato sistemi di sicurezza per proteggere e monitorare la Rete aziendale e tutti i servizi pubblicati. P.ICT.06 ProceduraInformationSecurity
A.8.24	Uso della crittografia	YES		DELLORTO utilizza il sistema di crittografia per proteggere i propri dati aziendali P.ICT.06 ProceduraInformationSecurity
A.8.25	Ciclo di vita dello sviluppo sicuro	YES		DELLORTO applica degli standard e delle regole generali di programmazione al fine di garantire la sicurezza delle informazione e Privacy BY Design P.ICT.10 - Sviluppo Sicuro
A.8.26	Requisiti di sicurezza dell'applicazione	YES		DELLORTO applica degli standard e delle regole generali di programmazione al fine di garantire la sicurezza delle informazione e Privacy BY Design P.ICT.10 - Sviluppo Sicuro
A.8.27	Architettura di sistema sicura e principi ingegneristici	YES		DELLORTO applica degli standard e delle regole generali di programmazione al fine di garantire la sicurezza delle informazione e Privacy BY Design P.ICT.10 - Sviluppo Sicuro
A.8.28	Codifica sicura	YES		DELLORTO applica degli standard e delle regole generali di programmazione al fine di garantire la sicurezza delle informazione e Privacy BY Design P.ICT.10 - Sviluppo Sicuro
A.8.29	Test di sicurezza in fase di sviluppo e accettazione	YES		DELLORTO applica degli standard e delle regole generali di programmazione al fine di garantire la sicurezza delle informazione e Privacy BY Design P.ICT.10 - Sviluppo Sicuro
A.8.30	Sviluppo in outsourcing	YES		DELLORTO applica degli standard e delle regole generali di programmazione al fine di garantire la sicurezza delle informazione e Privacy BY Design P.ICT.10 - Sviluppo Sicuro
A.8.31	Separazione degli ambienti di sviluppo, test e produzione	YES		DELLORTO applica degli standard e delle regole generali di programmazione al fine di garantire la sicurezza delle informazione e Privacy BY Design P.ICT.10 - Sviluppo Sicuro
A.8.32	Change management	YES		Ad ogni cambiamento significativo di procedure e/o servizi, viene utilizzato un processo di Change Managment per analizzare anche gli aspetti delle sicurezza delle informazione e Privacy P.ICT.05 ChangeManagement
A.8.33	Informazione sui Test	YES		DELLORTO applica degli standard e delle regole generali di programmazione al fine di garantire la sicurezza delle informazione e Privacy BY Design P.ICT.10 - Sviluppo Sicuro
A.8.34	Protezione dei sistemi informativi durante le attività di audit/test	YES		DELLORTO applica degli standard e delle regole generali di programmazione al fine di garantire la sicurezza delle informazione e Privacy BY Design P.ICT.10 - Sviluppo Sicuro