Misure tecniche e organizzative adottate.

Misure Organizzative		
	Esiste una policy interna sulla gestione della privacy (policy by design)?	La maggior parte delle procedure relative alla gestione della privacy sono affrontate nelle procedure di gestione della qualità e della sicurezza (ISO 9001 e ISO 27001). Ad esempio, i principi di privacy by design e by default del GDPR sono di fatto previsti nella norma ISO 27001 in quanto alcune clausole di tale norma richiedono uno studio del contesto dei dati raccolti ed elaborati e raccomandano di eseguire periodiche valutazioni dei rischi al fine di assicurare l'efficacia della loro gestione e sicurezza. Il discorso può essere esteso a tutti gli argomenti che sono in comune con i due standard, come la riservatezza l'integrità dei dati, la valutazione del rischio, etc. Pertanto per quanto riguarda le procedure interne si fa riferimento alla certificazione ISO 27001
	Esiste un Organigramma con assegnazione delle funzioni in ambito GDPR?	Si, è previsto. E' composto dal Rappresentante Legale (Oscar Pitzanti), quale Titolare del Trattamento e Amministratore di Sistema, DPO (avv. Fausto Di Marcantonio), autorizzati divisi nelle varie Aree (Sistemistica, Sviluppo, Produzione, etc..)
	È stato nominato un DPO dal Titolare?	Si – avv. Fausto Di Marcantonio - privacy@digitalpa.it
	È stato individuato e nominato un Amministratore di Sistema?	SI – Fabrizio Nicosia
	I Dipendenti ricevono una specifica informativa relativamente alle norme comportamentali e le responsabilità connesse con l'accesso alle informazioni (Lettera di incarico)?	Per i lavoratori dipendenti, viene data specifica informativa tramite lettera di incarico nella quale vengono riportate le istruzioni relativamente alla privacy delle informazioni trattate in riferimento alla mansione svolta. Vengono specificati i permessi e le responsabilità relative alle varie tipologie di dato.
	Esiste un registro dei trattamenti (art. 30) eseguiti per conto dei TITOLARI o di altre società?	SI, è previsto.
	Esiste un Regolamento interno e/o una Policy sull'utilizzo degli strumenti informatici (Pc, email, ecc.)?	Si, è previsto nelle procedure della certificazione ISO-IEC 27001
	Esiste ed è mantenuto aggiornato un inventario dei dispositivi e applicazioni informatiche in uso presso la società?	Si, è previsto nelle procedure della certificazione ISO-IEC 27001
	Quali sono le procedure e gli strumenti adottati in caso di accesso non autorizzato ai dati, diffusione non consentita o alterazione degli stessi, anche qualora si trattasse di un semplice sospetto in ambito	È prevista una procedura di gestione e notifica di data breach redatta dal DPO, basata sul Regolamento Europeo 2016/679 (GDPR). Le disposizioni che vengono indicate nella procedura, partono dall'analisi degli eventi, la valutazione di eventuale violazione, classificazione, comunicazione titolare (entro 24 ore) e gestione con compilazione del registro degli eventi. Queste azioni vengono eseguite dall'Incident response team che può variare in base anche applicativo oggetto della violazione.

	Information Security e/o violazione dati?	
	È previsto ed aggiornato un inventario dei dispositivi, software, servizi e applicazioni informatiche in uso?	Si, è previsto per Server e Desktop e apparati di Rete secondo procedure della certificazione ISO-IEC 27001
	È presente l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP?	Apparati di rete, Server, VM, Desktop e altri dispositivi vengono registrati per IP e MAC Address.
	Vengono eseguite regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato?	Si, è previsto nelle procedure della certificazione ISO-IEC 27001
	Viene verificato che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio?	Si, è previsto nelle procedure della certificazione ISO-IEC 27001
	È definito un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, portatili, etc.).	Si, è previsto nelle procedure della certificazione ISO-IEC 27001
	Viene attribuito, alle azioni per la risoluzione delle vulnerabilità, un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche?	Si, è previsto nelle procedure della certificazione ISO-IEC 27001
	I privilegi di amministrazione sono limitati ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi?	Previsto. Per ogni reparto, solo gli utenti autorizzati possono accedere ai sistemi di propria competenza utilizzando credenziali personali.
	Le utenze amministrative sono utilizzate solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato?	Gli accessi ai sistemi sono tracciati tramite audit log e vengono registrati su dispositivi WORM per almeno 180 gg
	Esiste l'inventario di tutte le utenze amministrative, per	Si, è previsto.

	garantire che ciascuna di esse sia debitamente e formalmente autorizzata?	
	Le credenziali delle utenze amministrative sono sostituite con sufficiente frequenza (password aging)?	Nel nostro sistema IdM (Identification Manager) è presente una password policy distinta per gruppi, che impone il cambio password almeno ogni 90 gg per i dipendenti. Password policy più restrittive sono adottate in caso di incaricati non dipendenti.
	È prevista una storicizzazione delle password in modo tale che non sia possibile riutilizzare le credenziali a breve distanza di tempo (password history)?	Nel nostro sistema IdM è presente una password policy distinta per gruppi, che impone il cambio password almeno ogni 90 gg per i dipendenti, con history di 5 password salvate. Password policy più restrittive sono adottate in caso di incaricati non dipendenti.
	Tutte le utenze, in particolare quelle amministrative, sono nominative e riconducibili ad una sola persona?	Ogni dipendente/incaricato detiene una sola user personale nel sistema IdM.
	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, sono utilizzate solo per le situazioni di emergenza e le relative credenziali sono gestite in modo da assicurare l'imputabilità di chi ne fa uso?	Le credenziali amministrative anonime, sono detenute in Vault aziendale, accessibili previa autenticazione dell'utente tramite IdM o Active Directory, e depositate in uno spazio condiviso e backuppato ai soli amministratori.
	Sono adottate policy di Data Protection basate sui principi di Privacy by Design e by Default, e responsabilizzazione?	Tutti i software sviluppati dalla DigitalPA sono conformi alle indicazioni previste dal Regolamento Generale sulla Protezione dei Dati (GDPR). Sono previste delle linee guida sullo sviluppo relativamente alla ISO 27001.
	È previsto un piano di continuità operativa / piano di disaster recovery?	Si, è previsto nelle procedure della certificazione ISO 22301:2019
	È previsto un programma di valutazione del rischio per identificare in modo proattivo la sicurezza delle informazioni e i rischi di continuità operativa?	Si, è previsto nelle procedure della certificazione ISO 22301:2019
	Misure Tecniche	
	Come viene assicurato che l'accesso alle informazioni sia riservato solo a quei collaboratori che ne hanno necessità per poter erogare il servizio richiesto e soddisfare le esigenze specificate dal CLIENTE?	I nostri server sono dotati di sistema centralizzato delle autenticazioni, Identity Management (IdM), che permette l'accesso puntuale ai singoli incaricati, che in genere vengono gestiti in gruppi di autorizzazione. Ad ogni gruppo vengono applicate delle Policy autorizzative organizzate in genere per Host-Base Access Conotrol (HBAC) e password policy specifiche.
	Quali strumenti tecnici e di controllo periodico sono utilizzati per assicurare che l'accesso alle informazioni del CLIENTE sia limitato esclusivamente a quanto	Gli accessi ai server sono registrati come da regolamento UE, e in base alla normativa Italiana, su dispositivo Write-Once Read-Many (WORM) e criptati. I log in questo modo possono essere analizzati per le verifiche programmate. Periodo di conservazione predefinito: 181 giorni

	richiesto nell'ambito del servizio e che i dati non vengano usati per scopi diversi da quelli di un eventuale accordo?	
	Come è organizzata l'infrastruttura? Dove è localizzato il Data Center nel quale eventualmente potrebbero essere conservati dati di cui il CLIENTE è Titolare (indicare esatta ubicazione)? Quali sono le misure di protezione che applicate?	Il datacenter si trovano in Italia, per ulteriori dettagli, vedere documento "Modelli di erogazione in SaaS".
	Quali strumenti, sistemi di controllo applica DigtitalPA per prevenire il verificarsi di incidenti di Information Security e Data Protection?	I nostri server sono protetti da firewall, IPS, Web Application Firewall (WAF). L'IPS analizza i log dei servizi esposti di un server e si interfaccia con il firewall per bloccare gli IP, che stanno eseguendo delle azioni illecite, es. brute force attack. Il WAF viene costantemente aggiornato alle regole recenti, per identificare exploit del codice applicativo. Ad esempio rileva le azioni di SQL Injection e Cross Site Scripting.
	Quali procedure e strumenti di controllo assicurano la tempestiva applicazione degli aggiornamenti software e hardware (attività di patching, vulnerability Management) tali da eliminare o ridurre al minimo il rischio di incidenti che possano coinvolgere i dati e/o l'infrastruttura del CLIENTE ed in generale tutti i dati trattati da DigitalPA?	I server configurati sono dotati di watchdog, che consente di dare evidenza di nuovi aggiornamenti dei software di sistema, e del patching distribuito. Una volta evidenziati i pacchetti da installare vengono sottoposti a valutazione le release note ai vari reparti, per valutare l'impatto sul software installato. In seguito vengono installati su server di test, con stesse caratteristiche dei server di produzione, e i software vengono sottoposti a test, da parte del reparto Tester. Alcuni applicativi/appliance come Antivirus, IPS, e WAF sono aggiornati in modalità automatica per disporre delle ultime funzionalità sempre presenti.
	Le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature vengono eseguite per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri)?	Viene utilizzato almeno il protocollo TLS 1.2 per tutti i data in transit.
	Gli strumenti di scansione delle vulnerabilità utilizzati sono regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza?	I Web Application Firewall eseguono il check di aggiornamento giornalmente. Settimanalmente gli antivirus e antispyware.
	Come vengono installate le patch e gli aggiornamenti software del sistema operativo e delle applicazioni?	Le patch di sicurezza sui server vengono dapprima testate su ambienti di test, ed in seguito al testing, se non impattanti per il software, vengono installati in produzione. Per i desktop viene verificata l'usabilità del Sistema Operativo su un gruppo limitato di Desktop per poi essere aggiornati tutti i sistemi. Gli apparati di rete vengono backuppati ed in seguito aggiornati.

	Quali misure di sicurezza vengono adottate per i locali ove sono contenuti i dati personali (es. anti-incendio e anti-intrusione, impianto di videosorveglianza dei locali, etc.)	• Doppio portoncino blindato • Antifurto a sensore di apertura porte e sensore volumetrico/infrarosso a doppia tecnologia e dispositivo di alert sms ed email e app mobile. • Videosorveglianza full hd interna ed esterna ai locali 24h*365 con riversamento su NAS dedicato • L'accesso ai locali è profilato attraverso le chiavi antifurto personale in dotazione ai soli responsabili con diverse abilitazioni e fasce orarie di accesso. • L'accesso ai locali durante gli orari lavorativi è consentito tramite inserimento di codice da digitare su tastiera posta all'ingresso • È vietato l'accesso non autorizzato al di fuori degli orari lavorativi. Gli accessi ai responsabili muniti di chiavi di accesso vengono monitorati dai log di accesso ai locali tramite chiave personalizzata dell'antifurto. • Presenza di estintori a polvere revisionati Per ulteriori dettagli, consultare il documento "Modelli di erogazione in SaaS"