

Sez.1

DATI GENERALI CLIENTE E ATTIVITA' SVOLTA

DATI ANAGRAFICI	Denominazione / Ragione sociale Contraente	Sogei S.p.A.
	Cod.Fiscale / Partita IVA Contraente	01043931003
	Denominazione / Ragione sociale Assicurato (se diverso)	
	Cod.Fiscale / Partita IVA Assicurato	
	Indirizzo ubicazione del rischio	Via Carucci 99, 00143 Roma(RM)
	Presenza di più ubicazioni (In caso affermativo, allegare al presente questionario l'elenco delle altre ubicazioni)	Via Carucci 85, 00143 Roma(RM) Via Atanasio Soldati 80, 00155 Roma(RM)
	Indirizzo web	www.sogei.it

DATI ATTIVITÀ	Codice Ateco	62.09.09
	Data inizio attività	1976
	Numero totale dei dipendenti	2228
	Numero di dipendenti che non accedono alla rete aziendale	0
	Somme assicurate apparecchiature elettroniche	€ 230.877.356,60
	Somma assicurata strumenti IoT e sistemi Scada unitamente ai sistemi fisici a cui si applicano	Al momento non disponiamo di una disaggregazione di somme per tali strumenti elettronici.
	Profitto lordo ultimo esercizio <i>*Per profitto lordo s'intende: la differenza fra l'ammontare del Volume di affari annuo addizionato alle rimanenze finali e l'ammontare delle rimanenze iniziali addizionato agli altri costi variabili di esercizio non assicurati. Le rimanenze iniziali e quelle finali devono essere determinate secondo i normali metodi contabili dell'Assicurato. Ove possibile, compilare l'allegato prospetto analitico denominato "determinazione del Profitto lordo ai fini assicurativi".</i>	€ 40.913.000,00
	Fatturato ultimo esercizio (Allegare l'ultimo bilancio disponibile)	€584.933.823,00. Allegato scaricabile da www.sogei.it (ultimo bilancio disponibile relativo all'esercizio 2019). Il bilancio 2020 è ancora in attesa di approvazione da parte dell'assemblea dei soci.
	Indicare la distribuzione geografica del fatturato dell'ultimo esercizio (%)	Unione Europea _____ 100% USA/Canada _____ Resto del mondo _____
	Previsione di fatturato prossimo esercizio	€ 625.665.000,00
	Indicare la distribuzione geografica del fatturato previsto per il prossimo esercizio (%)	Unione Europea _____ 100% USA/Canada _____ Resto del mondo _____

DESCRIZIONE ATTIVITÀ	Descrivere nel dettaglio l'attività svolta
	Realizzazione di servizi informatici in grado di governare la complessità del sistema pubblico, come il Sistema informativo della fiscalità e l'automazione dei processi operativi e gestionali del Ministero, Corte dei conti, Agenzie fiscali e altre pubbliche amministrazioni.

MODALITÀ DI PAGAMENTO		
	Attività di vendita attraverso E-Commerce	<input type="checkbox"/> sì <input checked="" type="checkbox"/> no In caso affermativo, indicare il fatturato (%) derivante da vendite effettuate tramite E-commerce negli ultimi 12 mesi

	Accettati pagamenti con carta di credito per beni e servizi	<input type="checkbox"/> sì <input checked="" type="checkbox"/> no
	Conformità Payment Card Industry Data Security Standards – PCI DSS	<input type="checkbox"/> soggetta <input checked="" type="checkbox"/> non soggetta <input type="checkbox"/> conforme
	Sono processati pagamenti per conto terzi, comprese transazioni E-commerce? <input type="checkbox"/> sì <input checked="" type="checkbox"/> no In caso affermativo, indicare:	
	<i>Nominativi dei terzi</i>	<i>Volume delle transazioni per terzo all'anno</i>

SITUAZIONE ASSICURATIVA	Altre polizze in corso con il nostro gruppo <input type="checkbox"/> sì <input checked="" type="checkbox"/> no In caso affermativo, indicare:	
	<i>Tipologia</i>	<i>Importo complessivo delle coperture in corso con il nostro gruppo</i>

SITUAZIONE SINISTRI	Sinistri accaduti negli ultimi 3 anni ai sensi della polizza Cyber	<input type="checkbox"/> sì <input checked="" type="checkbox"/> no
	In caso affermativo, la violazione ha riguardato:	
	Violazione della privacy, divulgazione non autorizzata o perdita di informazioni riservate <input type="checkbox"/> sì <input checked="" type="checkbox"/> no In caso affermativo, indicare:	
	<i>Tipologia</i>	<i>Impatto economico</i>
	Reclami/Segnalazioni da parte degli interessati <input type="checkbox"/> sì <input checked="" type="checkbox"/> no In caso affermativo, indicare:	
	<i>Tipologia</i>	<i>Impatto economico</i>
	Violazione del sistema informatico (attacchi informatici, intrusioni, violazioni della rete o simili) <input type="checkbox"/> sì <input checked="" type="checkbox"/> no In caso affermativo, indicare:	
	<i>Tipologia</i>	<i>Impatto economico</i>
	Interruzione di servizio non programmata <input checked="" type="checkbox"/> sì <input type="checkbox"/> no	

In caso affermativo, indicare:	
Durata di ogni singola interruzione	Impatto economico
L'organizzazione ha subito dei controlli e delle visite ispettive in materia privacy da parte dell'Autorità?	<input checked="" type="checkbox"/> sì <input type="checkbox"/> no In caso affermativo, indicare l'esito dell'ispezione: _____ Negativo _____

MAPPAURA DEGLI ASSET AZIENDALI	Indicare il numero dei computer fissi	<input type="checkbox"/> <100 <input type="checkbox"/> 101-1000 <input checked="" type="checkbox"/> >1001
	Indicare il numero dei device mobili utilizzati:	Tablet <input type="checkbox"/> <100 <input checked="" type="checkbox"/> 101-1000 <input type="checkbox"/> >1001
		Smartphone <input type="checkbox"/> <100 <input type="checkbox"/> 101-1000 <input checked="" type="checkbox"/> >1001
		Laptop <input type="checkbox"/> <100 <input type="checkbox"/> 101-1000 <input checked="" type="checkbox"/> >1001
	Indicare i sistemi operativi utilizzati sui client fissi/laptop	<input type="checkbox"/> precedenti a Windows 10 <input checked="" type="checkbox"/> Windows 10 <input checked="" type="checkbox"/> Mac <input type="checkbox"/> Linux <input type="checkbox"/> Altro
	Indicare i sistemi operativi utilizzati su tablet/smartphone	<input checked="" type="checkbox"/> Android <input checked="" type="checkbox"/> IOS
	Indicare il numero dei server	<input type="checkbox"/> <10 <input type="checkbox"/> <100 <input type="checkbox"/> 101-1000 <input checked="" type="checkbox"/> >1001
	Indicare le modalità di gestione dei data center	<input checked="" type="checkbox"/> in house <input type="checkbox"/> externalizzati in hosting/housing <input type="checkbox"/> in cloud
Indicare i sistemi operativi utilizzati sui server	<input checked="" type="checkbox"/> precedenti a Windows Server 2019 <input checked="" type="checkbox"/> Windows Server 2019 <input checked="" type="checkbox"/> Linux <input checked="" type="checkbox"/> Altro	

Quali processi relativi alla gestione delle operazioni e/o della sicurezza dei dispositivi e dei sistemi di rete sono esternalizzati a provider esterni di servizi?	
Attività	Fornitore
<input type="checkbox"/> Desktop management	
<input type="checkbox"/> Server management	
<input type="checkbox"/> Network management	
<input type="checkbox"/> Security management	
<input type="checkbox"/> Data center hosting	
<input type="checkbox"/> Data processing	
<input type="checkbox"/> Application management	
<input type="checkbox"/> Alert log monitoring	
<input type="checkbox"/> Offsite backup e storage	
<input type="checkbox"/> Co- location facility	
<input type="checkbox"/> Application service provider (ASP)	
<input checked="" type="checkbox"/> Call center/Service desk	
<input type="checkbox"/> Operational business process	
<input type="checkbox"/> Sistemi di pagamento	
<input type="checkbox"/> Altro, specificare:	

SERVIZI IN CLOUD	Sono utilizzati dei servizi in Cloud? <input checked="" type="checkbox"/> sì <input type="checkbox"/> no		
	In caso affermativo, indicare:		
	Partner	Servizi	Nazione in cui sono conservati i dati
	Microsoft	Servizi di collaboration su Office365	UE

Sez.2

SICUREZZA DEI SISTEMI, DELLA RETE E DELLE INFORMAZIONI

POLITICA DI SICUREZZA	Q.1	L'organizzazione ha ottenuto una certificazione ISO/IEC 27001?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no In caso affermativo, indicare la data dell'ultimo aggiornamento: Maggio 2020
	Q.2	La Direzione Aziendale ha definito, approvato e pubblicato una Politica di Sicurezza delle Informazioni?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.3	Le regole espresse dalla Politica di Sicurezza delle Informazioni sono conosciute e accettate formalmente da tutto il personale?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.4	La Politica di sicurezza è periodicamente riesaminata ed aggiornata?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.5	È stato chiaramente identificato e formalizzato il ruolo di Responsabile della Sicurezza Informatica?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.6	L'organizzazione si è dotata di una funzione interna di Audit che si occupa di verificare e garantire la corretta implementazione dei presidi di sicurezza informatica, comprese le Policy adottate dall'azienda?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
RISORSE UMANE	Q.7	L'organizzazione prevede dei cicli di formazione specifici sui temi di Information Security (con cadenza almeno annuale) per garantire la consapevolezza, l'istruzione e l'addestramento dei collaboratori in relazione al ruolo che ricopriranno in azienda?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.8	E' presente una procedura che, durante le fasi di conclusione del rapporto lavorativo, preveda un immediato recupero degli elementi di sicurezza (chiavi, tessere etc.), la restituzione degli asset in dotazione e una contestuale disabilitazione delle utenze?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no (HR)
GESTIONE DEGLI ASSET, REMOTE CONTROL E SMART WORKING	Q.9	L'organizzazione ha implementato un processo di Ict Asset Management, che identifichi tutti gli asset informativi (client, server, apparati di rete, Scada, IoT, device mobili, applicazioni/dati, etc.) oggetto della copertura assicurativa, nonché l'ownership e le relative responsabilità?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.10	L'organizzazione ha definito, formalizzato e condiviso con i tutti i suoi collaboratori, delle specifiche istruzioni per un corretto utilizzo degli asset aziendali (es. email, internet, social media, supporti rimovibili, regole di comunicazione telefonica, regole di utilizzo laptop in ambienti pubblici, utilizzo di servizi di rete, etc.)?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.11	L'organizzazione ha implementato, sui dispositivi aziendali utilizzabili all'esterno dell'azienda, misure di sicurezza equivalenti a quelle degli asset presenti nel perimetro aziendale (es. antivirus, aggiornamenti, cambio password, cifratura, backup dei dati)?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no In caso affermativo, indicare i dispositivi sui quali sono applicate le misure di sicurezza <input checked="" type="checkbox"/> laptop <input checked="" type="checkbox"/> tablet

			<input checked="" type="checkbox"/> smartphone
Q.12	L'organizzazione ha attivato modalità di lavoro agile /smart working?		<input checked="" type="checkbox"/> si, con BYOD <input type="checkbox"/> si, senza BYOD <input type="checkbox"/> no
Q.13	Esistono procedure per verificare preventivamente i requisiti e le configurazioni di sicurezza degli asset informatici personali nel caso in cui un collaboratore utilizzi un proprio dispositivo all'interno del perimetro aziendale (BYOD)?		<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.14	L'organizzazione adotta modalità di deployment differenziando le attivazioni su pc aziendali da quelle in BYOD?		<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.15	L'organizzazione ha reso ai propri collaboratori delle specifiche istruzioni sulle modalità di lavoro in smart working in cui sono dettagliate le basi della sicurezza nel lavoro da remoto?		<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.16	Per le attivazioni su device aziendali, sono state implementate le seguenti misure di sicurezza:		<input checked="" type="checkbox"/> disk Encryption <input type="checkbox"/> DLP <input checked="" type="checkbox"/> MDM (Mobile device Management) <input checked="" type="checkbox"/> AV con firewall <input checked="" type="checkbox"/> Connessione con VPN con 2FA (OTP/authenticator) ovvero altra modalità di connessione attivata (es.accesso a bolla citrix o altra piattaforma di disintermediazione su pagina crittografata (https) ovvero soluzione di virtual desktop)
Q.17	Per le attivazioni in BYOD, sono state implementate le seguenti misure di sicurezza:		<input checked="" type="checkbox"/> rilascio di agent sulle macchine degli users <input type="checkbox"/> revoca privilegi amministratore <input type="checkbox"/> Verifica presenza AV con firewall con preventiva scansione <input checked="" type="checkbox"/> Rilascio di soluzione di connessione con VPN con 2FA (OTP/authenticator) ovvero altra modalità di connessione attivata (es.accesso a bolla citrix o altra piattaforma di disintermediazione su pagina crittografata (https) ovvero soluzione di virtual desktop)

CONTROLLO DEGLI ACCESSI	Q.18	L'organizzazione definisce una politica di controllo degli accessi basata sul principio del privilegio minimo?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.19	La politica di controllo accessi prevede una fase di riesame periodico dei diritti di accesso degli utenti e degli amministratori di sistema?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.20	L'organizzazione provvede a fornire un identificativo univoco e vieta l'utilizzo di identificativi o utenze condivise (anche a livello di amministratore di sistema)?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.21	L'organizzazione si è dotata di un processo formale per l'assegnazione e revoca dei diritti di accesso per tutte le tipologie di utenze e per tutti i sistemi e servizi (inclusi i diritti di accesso privilegiato)?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.22	L'organizzazione ha implementato e diffuso una password policy che garantisca e applichi un adeguato livello di complessità e robustezza?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no

CONTROLLI CRITTOGRAFICI	Q.23	L'organizzazione ha implementato delle soluzioni crittografiche e adottato una policy relativa alla definizione dei requisiti minimi di sicurezza e di controllo delle tecnologie adottate (es. uso, protezione e durata delle chiavi di crittografia)?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no

SICUREZZA FISICA	Q.24	Il perimetro fisico dell'impianto / uffici è chiaramente delimitato e ogni singolo varco è presidiato da operatori di sicurezza e/o impianti di rilevazione accessi?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.25	Sono previsti dei sistemi di verifica/registrazione/tracciatura in ingresso dei visitatori che accedono al building / struttura / impianto, anche attraverso l'esibizione di un documento di identità?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.26	Gli accessi sono chiusi e presidiati al di fuori dell'orario di lavoro?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.27	L'accesso ai locali del datacenter è permesso solo al personale autorizzato, dotato di credenziali / badge specifici?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.28	Sono presenti dei sistemi di controllo degli accessi al data center? Specificare quali.	<input checked="" type="checkbox"/> Apparecchi CCTV <input checked="" type="checkbox"/> Bussole di accesso degli edifici con metal detector <input type="checkbox"/> Sensori anti-intrusione e dissuasori veicolari <input type="checkbox"/> Sistemi tecnologici anti-tailgating <input type="checkbox"/> Sensori volumetrici <input checked="" type="checkbox"/> Lettori badge / password / chiavi elettroniche (anche con doppi sistemi di autenticazione) <input type="checkbox"/> Sistema di acquisizione delle impronte digitali con rilevamento di impronta falsa <input type="checkbox"/> Altro, specificare _____
	Q.29	Le operazioni di manutenzione da parte dei fornitori all'interno del data center in house sono sempre supervisionate da personale interno?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.30	Esiste una procedura di revisione periodica degli accessi al building / infrastruttura / data center (log controllo accessi o revisione dei registri cartacei)?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.31	Caratteristiche del data center:	<input checked="" type="checkbox"/> rack e i server presenti all'interno del data center prevedono sempre una ridondanza delle linee elettriche <input checked="" type="checkbox"/> il sistema di condizionamento è correttamente dimensionato e dotato di sistemi automatici di rilevamento e allerta di temperatura e umidità <input checked="" type="checkbox"/> sistemi di controllo antifumo e di rilevazione di sicurezza ambientale (es. sensori per pavimento flottante) <input checked="" type="checkbox"/> UPS <input checked="" type="checkbox"/> il sistema di cablaggio strutturato è conforme alle normative di settore <input type="checkbox"/> Altro, specificare _____

	Q.32	Il sistema di condizionamento è correttamente dimensionato e dotato di sistemi automatici di rilevamento e allerta di temperatura e umidità?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.33	Il datacenter prevede sistemi di controllo antifumo e di rilevazione di sicurezza ambientale (es. sensori per pavimento flottante)?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.34	Esiste un processo di "sanitizzazione" che garantisca la cancellazione o la sovrascrittura sicura dei dati presenti sugli apparati informatici prima della dismissione/riutilizzo?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no

SICUREZZA DELLE ATTIVITA' OPERATIVE	Q.35	[Change Management] Le fasi di change management prendono sempre in considerazione i requisiti di sicurezza e i criteri di accettazione per nuove versioni o sistemi?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.36	[Change Management] Gli ambienti di sviluppo, test e produzione sono separati per ridurre il rischio di accesso o cambiamenti non autorizzati all'ambiente di produzione?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.37	[Anti-Malware] - L'organizzazione si è dotata di un sistema centralizzato, regolarmente aggiornato (almeno mensile), per la gestione dei sistemi antivirus/anti-Malware che copre tutti gli asset rientranti della copertura assicurativa?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.38	[Anti-Malware] - L'organizzazione pianifica ed esegue scansioni periodiche su tutti gli asset informatici che sono oggetto della copertura assicurativa?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.39	[Anti-Malware] - Le impostazioni del software antivirus / Anti-Malware sono impostate per scansionare anche gli allegati di posta e il contenuto delle pen drive quando utilizzate?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.40	[Backup] – Con quale frequenza è eseguito il back up dei dati?	<p>Possiamo affermare che a seconda dei dati trattati, abbiamo le seguenti frequenze di backup:</p> <p>1. BACKUP IMMAGINI SISTEMI VIRTUALI: backup effettuato più volte al giorno. I dati vengono conservati per un periodo di 30 giorni;</p> <p>2. BACKUP BASE INFORMATIVA ORACLE, SQL SERVER, ecc. (dati strutturati): Salvataggio dei log contenenti la registrazione degli aggiornamenti dei DB (Archive-log per Oracle), sono eseguiti più volte al giorno al superamento di valori predefiniti e sono mantenuti per un periodo di 8 settimane; Salvataggio full dei DB con cadenza bisettimanale, è schedato in orari e giorni stabiliti ed è mantenuto per un periodo di 8 settimane;</p> <p>3. BACKUP BASE INFORMATIVA SU FILE PIATTO: Per la base informativa applicativa è previsto un salvataggio totale settimanale ed un salvataggio incrementale giornaliero, il dato è mantenuto 1 mese per alcune tipologie di dati, 2 mesi per altre. Per la base informativa di sistema, che comprende le configurazioni ed i prodotti installati non soggetti a modifiche frequenti, è previsto un salvataggio totale mensile, il dato è mantenuto 3 mesi.</p>

Q.41	[Backup] Quale modalità di salvataggio e recupero dati fa parte della strategia di back up scelta dall'organizzazione?	<input checked="" type="checkbox"/> back up completo <input type="checkbox"/> back up differenziale <input type="checkbox"/> back up incrementale
Q.42	[Backup] - L'organizzazione si è dotata di una procedura di backup che identifica le informazioni critiche per il business?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.43	[Backup] - Dove sono salvate le copie di back up?	<input checked="" type="checkbox"/> supporti esterni o asportabili <input checked="" type="checkbox"/> supporti interni fissi <input type="checkbox"/> Cloud
Q.44	[Backup] – Le copie di back up salvate su supporti esterni, sono conservate in siti alternativi / secondari per garantire l'efficacia dei processi di Disaster Recovery?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.45	[Backup] - Vengono eseguiti periodicamente test di ripristino, in particolare dei database che sono oggetto della copertura assicurativa?	<input type="checkbox"/> si <input checked="" type="checkbox"/> no
Q.46	[Backup] - Le copie di backup vengono protette in base al livello di confidenzialità delle informazioni che contengono?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.47	[Backup]- Vengono eseguiti i backup delle configurazioni degli apparati di rete (es. router, firewall ecc.)?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.48	[Raccolta Log & Monitoraggio] - L'organizzazione definisce a priori quali log sono ritenuti essenziali per identificare eventuali anomalie e/o evidenziare potenziali attacchi e/o azioni malevole sui propri applicativi e infrastrutture "mission critical"?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.49	[Raccolta Log & Monitoraggio] - Per garantire una corretta registrazione degli eventi, l'orario interno dei sistemi è sincronizzato con i time server tramite protocollo NTP (Network Time Protocol)?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.50	[Raccolta Log & Monitoraggio] - L'organizzazione si è dotata di sistema di correlazione e gestione dei log che supporta le funzioni interne / security nell'identificazione e nell'analisi degli eventi ritenuti critici, anche in ottica forense?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.51	[Raccolta Log & Monitoraggio] - L'accesso ai file di log è consentito solo a soggetti individuati nel rispetto del principio "need to know" prevedendo, con granularità, i profili delle utenze che possono accedere e i relativi privilegi?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.52	[Raccolta Log & Monitoraggio] – L'organizzazione si è dotata di un sistema di Log Management in grado di monitorare gli accessi eseguiti dagli amministratori e dagli operatori di sistema sui sistemi aziendali?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.53	[Raccolta Log & Monitoraggio] – Quali misure di protezione sono state adottate dall'organizzazione per assicurare l'inalterabilità dei Log?	<input type="checkbox"/> accesso fisico controllato per le aree contenenti gli apparati di gestione dei log <input type="checkbox"/> accesso logico ai dati tramite 2FA- two factor authentication <input type="checkbox"/> crittografia dei file durante la conservazione <input checked="" type="checkbox"/> Altro, specificare (processo formale)

	Q.54	[Raccolta Log & Monitoraggio] – Indicare le tempistiche di conservazione dei file di log stabilite dall'organizzazione.	<input type="checkbox"/> < 6 mesi <input type="checkbox"/> ≥ 6 mesi <input checked="" type="checkbox"/> ≥ 12 mesi <input type="checkbox"/> Altro, specificare
	Q.55	Sono attuate procedure per controllare l'installazione di software sui sistemi gestiti?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.56	[Gestione vulnerabilità tecniche] – L'organizzazione effettua, su tutti gli asset rientranti nel perimetro, dei test di sicurezza periodici (es. Vulnerability Assessment, penetration test) e attività di Risk Analysis?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no In caso affermativo, descrivere le principali criticità emerse

SICUREZZA DELLE RETI	Q.57	L'organizzazione dispone di sistemi firewall aggiornati?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.58	È attivo un monitoraggio in tempo reale sulle anomalie?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.59	L'organizzazione si è dotata di sistemi di intrusion detection/prevention (IDS/IPS), costantemente aggiornati?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.60	Le connessioni di telecomunicazione adottano sistemi di ridondanza per garantire continuità operativa?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.61	In relazione alle informazioni scambiate su reti pubbliche, viene garantito un adeguato livello di cifratura del canale (es. adozione di protocolli di tunnelling in SSL o SSH) o delle informazioni trasmesse?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.62	Data per scontata la segregazione della rete interna effettuata con VLAN o metodi analoghi, essa coinvolge anche le reti su cui si attestano eventuali smart-meter e sensori?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no

	Q.63	L'organizzazione si è dotata di un sistema di selezione dei fornitori che valuti, oltre alla loro solidità finanziaria, anche le loro politiche di cyber security e di trattamento dei dati, e che includa una verifica periodica sul mantenimento dei requisiti richiesti in ingresso?	<input type="checkbox"/> si <input checked="" type="checkbox"/> no
	Q.64	Per i fornitori esiste una procedura di autorizzazione all'accesso diretto o da remoto ai sistemi, che prevede una verifica periodica e una revoca superato un periodo di tempo prestabilito?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.65	I fornitori di servizi cloud sono in possesso di certificazioni professionali (esempio CCSP Certified Cloud Security Professional, EXIN Cloud Computing Foundation, EC Council CAST 618 Designing and Implementing Cloud Security, ecc.)?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no

ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEI SISTEMI INFORMATIVI	Q.66	L'azienda adotta controlli di adeguatezza, conformità e sicurezza rispetto a software/sistemi informativi sviluppati da terze parti?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.67	L'accesso agli ambienti di sviluppo, pre-produzione e produzione è consentito attraverso l'utilizzo di account diversi per ogni ambiente?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.68	Sono eseguite periodicamente le manutenzioni programmate richieste dalle specifiche dei produttori?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no

CONTINUITÀ OPERATIVA	Q.69	L'organizzazione ha implementato un processo documentato di Business Impact Analysis (BIA) regolarmente aggiornato che identifichi gli impatti in termini di tempi di interruzione, danni (es. patrimoniali diretti e indiretti) e relativi tempi di ripristino?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
----------------------	------	--	--

	Q.70	L'organizzazione si è dotata di un piano di ripristino o Business Continuity Plan (BCP) integrato con procedure operative e istruzioni di ripristino dettagliate?	<input checked="" type="checkbox"/> sì <input type="checkbox"/> no
	Q.71	L'organizzazione identifica e definisce in un Disaster recovery Plan tutte le attività di ripristino tecnico?	<input checked="" type="checkbox"/> sì <input type="checkbox"/> no I DRP non include le procedure di ripristino che sono definite separatamente
	Q.72	Sono testati regolarmente:	<input checked="" type="checkbox"/> il piano di business continuity <input type="checkbox"/> il piano di disaster recovery
	Q.73	L'organizzazione ha adottato di una procedura di valutazione degli impatti che eventuali cambiamenti all'organizzazione, ai processi di business, alle strutture di elaborazione delle informazioni e ai sistemi, possono avere sulla sicurezza delle informazioni?	<input checked="" type="checkbox"/> sì <input type="checkbox"/> no
	Q.74	Si coinvolgono i fornitori nei test di continuità operativa?	<input checked="" type="checkbox"/> sì <input type="checkbox"/> no
	Q.75	Si prega di valutare, in caso di interruzione di rete o di guasto del sistema, dopo quanto tempo, l'impossibilità di accedere ai sistemi informatici, genererebbe un impatto significativo sull'attività dell'organizzazione:	
		<i>Attività (o settori)</i>	<i>Massimo periodo di interruzione prima di avere un impatto negativo</i>
		Gestione rete	immediatamente <input type="checkbox"/> <input checked="" type="checkbox"/> >4ore <input type="checkbox"/> >12ore <input type="checkbox"/> >24ore <input type="checkbox"/> >48 ore <input type="checkbox"/> >5giorni <input type="checkbox"/> mai
		Gestione sistemi	<input type="checkbox"/> immediatamente <input checked="" type="checkbox"/> >4ore <input type="checkbox"/> >12ore <input type="checkbox"/> >24ore <input type="checkbox"/> >48 ore <input type="checkbox"/> >5giorni <input type="checkbox"/> mai
		Gestione sistemi di sicurezza	<input checked="" type="checkbox"/> immediatamente <input type="checkbox"/> >4ore <input type="checkbox"/> >12ore <input type="checkbox"/> >24ore <input type="checkbox"/> >48 ore <input type="checkbox"/> >5giorni <input type="checkbox"/> mai
Q.76	Indicare, in caso di interruzione di rete o guasto di sistema, una stima della massima perdita finanziaria per ogni ora di interruzione	± € 66.800,00	

GESTIONE INCIDENTI	Q.77	L'organizzazione ha implementato un processo di Incident Management/Response (persone, ruoli, responsabilità)?	<input checked="" type="checkbox"/> sì <input type="checkbox"/> no
	Q.78	Esistono playbook (elenchi azioni predefinite) in funzione del tipo di incidente occorso (es. sospensione cautelativa del sistema colpito, cambio password, ecc.)?	<input checked="" type="checkbox"/> sì <input type="checkbox"/> no

Sez.3

GESTIONE DEI DATI PERSONALI

GESTIONE DELLE ESPOSIZIONI PRIVACY	Q.79	Nell'esercizio della propria attività, che tipo di dati personali raccoglie, processa o conserva l'organizzazione?	
		<i>Tipologia dei dati trattati</i>	<i>Volume dei dati trattati</i>
		<input checked="" type="checkbox"/> dati finanziari (carte di credito/ debito/conto corrente)	<input type="checkbox"/> ≤100 <input type="checkbox"/> ≤1.000 <input type="checkbox"/> ≤100.000 <input type="checkbox"/> ≤1.000.000 <input checked="" type="checkbox"/> ≥1.000.000
		<input checked="" type="checkbox"/> dati personali di terzi Soggetti	<input type="checkbox"/> ≤100 <input type="checkbox"/> ≤1.000 <input type="checkbox"/> ≤100.000 <input type="checkbox"/> ≤1.000.000 <input checked="" type="checkbox"/> ≥1.000.000
		<input checked="" type="checkbox"/> Informazioni sanitarie	<input type="checkbox"/> ≤100 <input type="checkbox"/> ≤1.000 <input type="checkbox"/> ≤100.000 <input type="checkbox"/> ≤1.000.000 <input checked="" type="checkbox"/> ≥1.000.000

	<input checked="" type="checkbox"/> proprietà intellettuale/copyrights/segrete commerciali	<input type="checkbox"/> ≤100 <input type="checkbox"/> ≤1.000 <input type="checkbox"/> ≤100.000 <input type="checkbox"/> ≤1.000.000 <input type="checkbox"/> ≥1.000.000
Q.80	L'organizzazione ha implementato un sistema di gestione dei dati adempiendo alle prescrizioni previste dalla normativa nazionale ed europea in materia di trattamento dei dati e nel rispetto dei diritti degli interessati? <i>*Si intendono incluse le misure che soddisfino i principi di privacy by design e privacy by default, quali ad esempio: ridurre al minimo il trattamento dei dati, offrire trasparenza per quanto riguarda i trattamenti (es. prevedendo delle informative conformi da rendere prima di raccogliere i dati), raccolta del consenso informato prima di procedere a determinati trattamenti (es. marketing), etc.</i>	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.81	L'organizzazione ha previsto tutele rafforzate nel trattamento di categorie particolari di dati (es. informazioni sanitarie)?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.82	Sul sito web aziendale sono presenti informative aggiornate (inclusa l'informativa sui cookies) rispetto alla normativa in vigore ed ai trattamenti effettuati?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.83	A chi è attribuita l'attività di gestione della privacy dell'organizzazione?	<input type="checkbox"/> Società di consulenza o studio legale <input checked="" type="checkbox"/> Ufficio privacy all'interno dell'azienda (Privacy manager) <input type="checkbox"/> Libero professionista
Q.84	Il personale è stato informato in merito alle procedure sul trattamento dei dati adottate dall'organizzazione (informative, regolamenti, etc.)?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.85	L'organizzazione prevede delle periodiche sessioni di formazione e aggiornamento (almeno su base annuale) in materia privacy per il personale che, a vario titolo, ha accesso ai dati personali trattati dall'azienda?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.86	È presente un documento, costantemente aggiornato, contenente un'analisi dei rischi sui trattamenti effettuati dall'azienda e applicabile a tutti i processi, le applicazioni, le classi d'informazione e/o asset, al fine di prevedere e mitigare gli inevitabili impatti sull'organizzazione in termini di riservatezza, integrità e disponibilità delle informazioni?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.87	L'organizzazione ha nominato un Responsabile della protezione dei dati (DPO)?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no <input type="checkbox"/> non soggetta
Q.88	Sono state utilizzate delle specifiche clausole o modelli contrattuali per individuare e nominare gli amministratori di sistema e/o i responsabili del trattamento dei dati esterni all'organizzazione?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.89	È stata adottata e portata a conoscenza del personale, una procedura per la gestione di eventuali violazioni dei dati (Data Breach), al cui interno sono stati definiti ruoli e responsabilità?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
Q.90	E' stata definita una Data Retention Policy nella quale sono stati stabiliti i termini di conservazione e relativa cancellazione dei dati per tutti i trattamenti, nonché il soggetto interno preposto a tale attività?	La data retention è definita per ogni trattamento. In corso di definizione una policy complessiva

	Q.91	L'organizzazione effettua i seguenti trattamenti:	<input type="checkbox"/> Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive (es. screening dei propri clienti utilizzando database di rischio creditizio/lotta alle frodi/riciclaggio e finanziamento del terrorismo (AML/CTF), creazione di profili comportamentali /marketing a partire dalla navigazione sul proprio sito, etc.) <input type="checkbox"/> Decisioni automatizzate che producono significativi effetti giuridici sull'interessato (es. selezione candidati tramite algoritmo) <input type="checkbox"/> Utilizzo nuove soluzioni tecnologiche e organizzative (es. associazione di tecniche dattiloscopiche e riconoscimento del volto per il controllo degli accessi fisici) <input checked="" type="checkbox"/> Monitoraggio regolare e sistematico (es. sorveglianza sistematica di un'area accessibile al pubblico) <input checked="" type="checkbox"/> Trattamento di dati su larga scala (da valutare in base al numero degli interessati coinvolti, il volume dei dati trattati, la durata delle attività di trattamento o l'estensione geografica del trattamento) <input type="checkbox"/> Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).
	Q.92	Sono previsti dei sistemi di monitoraggio dei dipendenti?	<input type="checkbox"/> sì <input checked="" type="checkbox"/> no In caso affermativo, indicare quali: <input type="checkbox"/> sistemi di geolocalizzazione (veicoli) <input type="checkbox"/> videosorveglianza <input type="checkbox"/> monitoraggio della navigazione internet (sistema di log, etc.) <input type="checkbox"/> altro _____
	Q.93	Nel caso in cui l'organizzazione esegua uno dei trattamenti descritti nei due punti precedenti (), ha provveduto ad effettuare una valutazione d'impatto sulla protezione dei dati (DPIA) prima di procedere al trattamento?	<input type="checkbox"/> sì <input checked="" type="checkbox"/> no
	Q.94	L'organizzazione trasferisce dati al di fuori dell'Unione Europea nel rispetto delle condizioni previste dagli artt. 44, 45 e 46 del GDPR (es. Accordi internazionali come Privacy Shield, trasferimento sulla base di decisioni di adeguatezza, data transfer agreement)?	<input type="checkbox"/> sì <input checked="" type="checkbox"/> no
	Q.95	L'organizzazione ha adottato delle procedure per rispondere tempestivamente alle richieste, riguardanti i trattamenti dei dati, da parte degli interessati?	<input checked="" type="checkbox"/> sì <input type="checkbox"/> no

Sez.4

CONTENUTI MULTIMEDIALI

GESTIONE DELLA MULTIMEDIALITA'	Q.96	Di quale tipologia di canali digitali si avvale l'organizzazione?	<input checked="" type="checkbox"/> Social Network <input type="checkbox"/> Blog <input type="checkbox"/> Chatroom
	Q.97	Sul sito web aziendale, sono previste:	<input type="checkbox"/> procedure di doppio opt-in per la raccolta delle informazioni personali degli utenti (es. in fase di iscrizione al sito, newsletter, etc.) <input type="checkbox"/> procedure di opt out, compreso l'inserimento del link per la disiscrizione al servizio (es. newsletter) <input checked="" type="checkbox"/> procedure per la tracciabilità e/o profilazione degli utenti/ visitatori (es. cookie, etc.)
	Q.98	L'organizzazione esternalizza tutta o solo in parte la propria pubblicità online a terze parti?	<input type="checkbox"/> viene esternalizzata tutta la pubblicità online <input type="checkbox"/> viene esternalizzata solo una parte (indicare quale) <hr/> <input checked="" type="checkbox"/> no, la pubblicità viene gestita da un ufficio interno all'organizzazione.
	Q.99	L'organizzazione ha adottato delle procedure per impedire la pubblicazione di contenuti diffamatori, illegali o in violazione al diritto alla privacy di terzi sui propri canali online?	<input checked="" type="checkbox"/> sì <input type="checkbox"/> no In caso affermativo, descrivere quali (es. ricorso ad un legale qualificato, etc.) Esistono diverse procedure e regolamenti aziendali che definiscono le linee guida e i comportamenti per l'uso corretto degli strumenti dei social.
	Q.100	La vagliatura dei contenuti pubblicati sui canali online dell'organizzazione, comprende:	<input checked="" type="checkbox"/> violazione del diritto alla riservatezza <input checked="" type="checkbox"/> violazione del copyright <input checked="" type="checkbox"/> lesione dell'altrui reputazione <input checked="" type="checkbox"/> altro, specificare _____
	Q.101	L'organizzazione dispone di una procedura per rispondere ad eventuali reclami sui contenuti creati e pubblicati, considerati calunniosi, illegali o in violazione al diritto alla privacy di terzi?	<input type="checkbox"/> sì <input checked="" type="checkbox"/> no In caso affermativo, descrivere la procedura adottata <hr/>

Luogo e Data

Roma, 7 Maggio 2021

Titolo/Funzione dell'incaricato

RES.INR – Carmelo Parrotta