

Cyber Risk Questionario

Sez.1		
DATI GENERALI CLIENTE E ATTIVITA' SVOLTA		
DATI ANAGRAFICI	Denominazione / Ragione sociale Contraente	Sogei S.p.A.
	Cod.Fiscale / Partita IVA Contraente	CF: 02327910580 P.IVA: 01043931003
	Denominazione / Ragione sociale Assicurato (se diverso)	
	Cod.Fiscale / Partita IVA Assicurato	CF: 02327910580 P.IVA: 01043931003
	Indirizzo ubicazione del rischio	Via Mario Carucci 99 Roma 00143
	Presenza di più ubicazioni <i>(In caso affermativo, allegare al presente questionario l'elenco delle altre ubicazioni)</i>	Via Mario Carucci 131 Roma 00143 Via Mario Carucci 85 Roma 00143 Via Aniene 14 Roma 00198 Viale Giacomo Matteotti 16 Firenze 50132 Viale dell'Innovazione 1/B Milano 20126 Via Roberto Bracco 20 Napoli 80133 Via Santa Maria 9 Torino 10122
	Indirizzo web	www.sogei.it

DATI ATTIVITÀ	Codice Ateco	62.90.09
	Data inizio attività	28/05/1976
	Numero totale dei dipendenti	2.735 al 31/12/2025 2.935 al 31/12/2026 (previsti da budget)
	Numero di dipendenti che non accedono alla rete aziendale	//
	Somme assicurate apparecchiature elettroniche	Si rimanda alle informazioni contenute nel Bilancio e documenti a corredo al sito www.sogei.it SE LE INFORMAZIONI NON FOSSERO SUFFICIENTI E' POSSIBILE RICHIEDERE IN SEDE DI RICHIESTE CHIARIMENTI
	Somma assicurata strumenti IoT e sistemi Scada unitamente ai sistemi fisici a cui si applicano	Si rimanda alle informazioni contenute nel Bilancio e documenti a corredo al sito www.sogei.it

	SE LE INFORMAZIONI NON FOSSERO SUFFICIENTI E' POSSIBILE RICHIEDERE IN SEDE DI RICHIESTE CHIARIMENTI
Profitto lordo ultimo esercizio <i>*Per profitto lordo s'intende: Utile netto di esercizio più le Spese generali fisse che continuerebbero a gravare sull'Assicurato in assenza dell'interruzione di Attività: Profitto Lordo = Utile netto di esercizio + Spese generali fisse</i>	L'ultimo Bilancio è disponibile sul sito www.sogei.it sul sito www.sogei.it
Fatturato ultimo esercizio (Allegare l'ultimo bilancio disponibile)	L'ultimo Bilancio è disponibile sul sito www.sogei.it
Indicare la distribuzione geografica del fatturato dell'ultimo esercizio (%)	Unione Europea ____ 100% ____ USA/Canada ____ Resto del mondo ____
Previsione di fatturato prossimo esercizio	€ 1.120.129.600,00
Indicare la distribuzione geografica del fatturato previsto per il prossimo esercizio (%)	Unione Europea ____ 100% ____ USA/Canada ____ Resto del mondo ____
Indicare eventuali società controllate/sedi estere (extra UE), specificando se si tratta di sedi commerciali e/o produttive	//
Nel caso in cui fossero presenti più sedi (incluse controllate extra UE), confermare che le informazioni contenute nel presente questionario siano da intendersi valide per tutte le società del Gruppo e che la gestione dell'infrastruttura informatica sia gestita centralmente dalla Contraente.	☐ sì ☒ no In caso contrario, specificare

DESCRIZIONE ATTIVITÀ	Descrivere nel dettaglio l'attività svolta
	Oggetto sociale

1. La Società, in quanto organismo di diritto pubblico/amministrazione aggiudicatrice e in quanto società interamente partecipata dal Ministero dell'economia e delle finanze, ha

per oggetto prevalente, per oltre l'80% del fatturato, la prestazione di servizi strumentali all'esercizio delle funzioni pubbliche attribuite al Ministero dell'economia e delle

finanze, alle Agenzie fiscali, in particolare:

a) ogni attività, ivi compresa l'attività industriale, finalizzata alla realizzazione, allo sviluppo, alla manutenzione ed alla conduzione tecnica del sistema informativo della fiscalità

per l'Amministrazione finanziaria;

b) ogni altra attività connessa, direttamente o indirettamente, con quella di cui sopra ivi comprese il supporto, l'assistenza e la consulenza all'Amministrazione finanziaria per lo

svolgimento delle funzioni statali ad essa spettanti;

c) le attività informatiche riservate allo Stato ai sensi del decreto legislativo n. 414 del 1997, e successivi provvedimenti di attuazione, nonché le attività di sviluppo e gestione

dei sistemi informatici ivi comprese le attività di supporto, assistenza e consulenza direttamente o indirettamente

collegate con le attività di cui sopra;

d) ogni altra attività di carattere informatico in aree di competenza del Ministero dell'economia e delle finanze;

e) l'elaborazione degli studi di settore, degli indici sintetici di affidabilità fiscale, la revisione e reingegnerizzazione integrata dei processi fiscali delle connesse procedure informatiche, da realizzare in collaborazione con le competenti Agenzie fiscali, nonché ogni altra attività di studio e ricerca in materia tributaria, ai sensi dell'articolo

10, comma 12, della legge 146/1998;

f) la predisposizione delle metodologie e la elaborazione dei dati per la definizione dei fabbisogni e dei costi standard delle funzioni e dei servizi resi, nei settori diversi dalla sanità, dalle regioni e dagli enti locali, svolgendo tutte le funzioni allo scopo previste dai decreti legislativi emanati in attuazione della legge 5 maggio 2009, n. 42, nonché

ogni altra attività necessaria;

g) ogni attività idonea a sviluppare innovative tecniche di elaborazione dei dati, a potenziare le attività di analisi per contrastare la sottrazione all'imposizione delle basi imponibili, anche di natura contributiva, aggiornare la mappa del rischio di evasione e individuare le relative aree territoriali e settoriali di intervento nonché, per favorire l'introduzione del concordato preventivo e l'implementazione dell'adempimento collaborativo di cui al decreto legislativo 5 agosto 2015, n. 128, a porre in essere le attività di progettazione, di sviluppo e di realizzazione dell'interoperabilità delle banche dati, relativamente agli aspetti metodologici.

2. La Società, infrastruttura nazionale cloud, al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa favorendo la digitalizzazione dei servizi e dei processi attraverso interventi di consolidamento delle infrastrutture, razionalizzazione dei sistemi informativi e interoperabilità tra le banche dati, può offrire, in conformità a specifiche disposizioni legislative e regolamentari, servizi informatici strumentali al raggiungimento degli obiettivi propri delle pubbliche amministrazioni e delle società pubbliche da esse

controllate.

3. *omissis*

4. In misura minoritaria e residuale, nel rispetto della normativa vigente, a condizione che permetta di conseguire economie di scala o altri recuperi di efficienza sul complesso

dell'attività principale, la Società può svolgere le ulteriori attività conferite in base a disposizioni legislative e regolamentari, per conto di Regioni, Enti Locali, società a partecipazione pubblica, anche indiretta, di organismi ed enti che svolgano attività di interesse pubblico o rilevanti nel settore pubblico, nonché di Istituzioni internazionali e sovranazionali e di Amministrazioni pubbliche estere, ivi comprese le attività verso l'Agenzia per l'Italia digitale.

5. *omissis*

6. Per conseguire la massima efficienza della sua azione e per l'acquisizione di risultati utili anche alla individuazione delle più idonee soluzioni dei problemi organizzativi

della Pubblica Amministrazione, la Società - nel quadro dell'obiettivo del costante aggiornamento tecnologico e professionale - potrà svolgere ricerca applicata e procedere

alla realizzazione ed allo sviluppo di prodotti in ogni area aperta dalla tecnologia informatica.

7. *omissis*

8. *omissis*

MODALITA' DI PAGAMENTO

Attività di vendita attraverso E-Commerce

☐ sì ☒ 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

☐ sì ☒ no

I pagamenti sono processati da terzi?

☐ sì tramite fornitore certificato PCI DSS

☐ sì tramite fornitore non soggetto allo standard PCI DSS che adotta misure di sicurezza simili e/o adeguate

☒ no, i pagamenti sono gestiti internamente

Con riferimento agli incassi, SOGEI non gestisce dati di carte di pagamento. Gli incassi avvengono tramite bonifico bancario e CBILL, attraverso il sistema bancario. Lo standard PCI DSS non è applicabile.

In caso affermativo, indicare:

Nominativi dei terzi

Volume delle transazioni per terzo all'anno

COMPLIANCE NORMATIVA	Con riferimento alla normativa italiana sulla cybersicurezza, l'organizzazione	☒ rientra nel perimetro del Dlgs 138/2024 (decreto NIS2) in qualità di soggetto essenziale ☐ rientra nel perimetro del Dlgs 138/2024 (decreto NIS2) in qualità di soggetto importante ☐ non rientra nel perimetro di applicazione del Dlgs 138/2024 (decreto NIS2) ☒ ha avviato un piano di adeguamento alla normativa cd. NIS2 ☐ è già conforme ai requisiti di sicurezza previsti dal Dlgs 138/2024 (decreto NIS2) ☐ non ha avviato un piano di adeguamento alla normativa cd. NIS2, anche se soggetta ☒ rientra nel perimetro del Dlgs 134/2024 di recepimento della direttiva (UE) 2022/2557 cd. CER (Critical Entities Resilience)
----------------------	--	---

SITUAZIONE ASSICURATIVA	Altre polizze in corso con il nostro gruppo ☐ sì ☐ no In caso affermativo, indicare:	
	Tipologia	Importo complessivo delle coperture in corso con il nostro gruppo

SITUAZIONE SINISTRI	Sinistri accaduti negli ultimi 3 anni ai sensi della polizza Cyber	☐ sì ☒ no Si specifica che ci sono stati Data breach di entità lieve riguardanti ANPR, per i quali non è stato necessario attivare la polizza
	In caso affermativo, la violazione ha riguardato: SI CHIEDE INOLTRE DI COMPILARE L'ALLEGATO 2	☐ Violazione della privacy, divulgazione non autorizzata o perdita di informazioni riservate ☐ Reclami/Segnalazioni da parte degli interessati ☐ Violazione del sistema informatico (attacchi informatici, intrusioni, violazioni della rete o simili) ☐ Interruzione di servizio non programmata Si specifica che ci sono stati Data breach di entità lieve riguardanti ANPR, per i quali non è stato necessario attivare la polizza

	L'organizzazione ha subito dei controlli e delle visite ispettive in materia privacy da parte dell'Autorità?	X si ☐ no SI RICHIEDE DI SPECIFICARE L'ANNO PER POTER FORNIRE INFORMAZIONI PIU' DETTAGLIATE In caso affermativo, indicare l'esito dell'ispezione: _____

MAPPAURA DEGLI ASSET AZIENDALI	Indicare il numero dei computer fissi	☐ <100 ☐ 101-1000 X >1001
	Indicare il numero dei device mobili utilizzati:	Tablet ☐ <100 ☐ 101-1000 ☐ >1001
		Smartphone ☐ <100 ☐ 101-1000 ☐ >1001
		Laptop ☐ <100 ☐ 101-1000 X >1001
	Indicare i sistemi operativi utilizzati sui client fissi/laptop	X Windows 11 X Windows 10 ☐ precedenti a Windows 10 X Mac ☐ Linux ☐ Altro, specificare
	Indicare i sistemi operativi utilizzati su tablet/smartphone	☐ Android ☐ IOS
	Indicare il numero dei server	☐ <10 <100 ☐ 101-1000 X >1001
Indicare le modalità di gestione dei data center	X in house X externalizzati in hosting/housing X in cloud	
Indicare i sistemi operativi utilizzati sui server	X precedenti o pari a Windows Server 2012 X Windows Server 2016 o superiore X Linux	

		☒ Altro, specificare z/OS, Unix:Solaris, Aix
	Nel caso in cui l'Organizzazione utilizzasse dei sistemi o software non più supportati dal produttore:	
	Fornire lista software/hardware end-of-life e relativo piano di dismissione e/o ragione dietro l'assenza di un piano di dismissione.	
	Indicare in quali processi sono coinvolti i sistemi legacy	
	L'organizzazione ha acquistato l'estensione del supporto per una versione precedente di Windows o altri OS?	☒ sì ☐ no Se sì, per quali sistemi? Windows 10
	I sistemi legacy sono isolati da internet e dal resto della rete aziendale?	☒ sì ☐ no Se sì, come? Sono attestati su rete interne, non esposte all'esterno. I sistemi non accedono ad internet direttamente ma solo attraverso proxy applicativi
	Viene effettuato monitoraggio proattivo? Ad esempio Endpoint Detection & Response (EDR)	☐ sì ☒ no
	L'EDR blocca/isola i sistemi in caso di alert?	☒ sì ☐ no Se no, quali azioni/procedure di escalation sono prese?

OUTSOURCERS	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?
	Nessuno di questi servizi è esternalizzato ma vengono svolti da Sogei con l'eventuale supporto di fornitori terzi.

	Attività	Fornitore
	☐ Desktop management	
	☐ Server management	
	☐ Network management	
	☐ Security management	
	☐ Data center hosting	
	☐ Data processing	
	☐ Application management	
	☐ Alert log monitoring	
	☐ Offsite backup e storage	
	☐ Co- location facility	
	☐ Application service provider (ASP)	
	☐ Call center/Service desk	
	☐ Operational business process	
	☐ Sistemi di pagamento	
	☐ Altro, specificare:	

OUTSOURCING SERVICE PROVIDER	Selezionare dall'elenco i principali fornitori di servizi informatici (selezione multipla)	☒ Accenture	☒ Almagora
		☐ Cedacri	☒ Cisco
		☒ Dell Technologies	☒ Engineering
		☒ IBM	☐ Insiel
		☐ Lepida	☐ Lutech
		☒ Microsoft	☒ Oracle
		☐ PagoPA	☐ Salesforce
		☐ SAP	☐ Sogei
		☐ TIM	☐ WIIT
		☐ Zucchetti	☒ Altro: <u>HITACHI/BROCADE</u>
☐ Non presente			

FORNITORE DI SERVIZI IN CLOUD	Selezionare dall'elenco i principali fornitori Cloud Provider (hosting services) (selezione multipla)	☐ Amazon web service(AWS)	☒ Microsoft Azure	
		☐ Aruba	☐ TIM	☐ Google Cloud Platform
		☐ Non presente		
		☐ Altro: _____		

REFERENTE CYBERSECURITY	Nel caso di un Ente Pubblico, si conferma la nomina di un Referente per la Cybersicurezza ex art. 8 L. 90/2024?	☒ sì, individuato in una figura interna all'Ente;
		☐ sì, individuato in una figura di altra Pubblica Amministrazione
		☐ no, anche se soggetta nomina in quanto rientrante tra i soggetti di cui all'art. 1 c. 1 della L. 90/2024.
		☐ no, perché non soggetta.

POLITICA DI SICUREZZA	Q.1	L'organizzazione ha ottenuto una certificazione ISO/IEC 27001?	Xsi ☐no In caso affermativo, indicare la data dell'ultimo aggiornamento e il perimetro a cui si applica la certificazione: Giugno 2025 Audit Perimetro: Conservazione Documenti Digitali (ISO 27001 + ISO 22301) Audit Servizio: Sistema di Interscambio Fatturazione Elettronica Audit Servizio: Piattaforma referendum Audit Servizio: SIA Audit Perimetro: Anagrafe Naz. Popolaz. Residente ANPR
	Q.2	La vostra organizzazione dispone di una politica formale per la sicurezza delle informazioni, documentata e regolarmente rivista e comunicata al personale?	Xsi ☐ no
	Q.3	Le regole espresse dalla Politica di Sicurezza delle Informazioni sono conosciute e accettate formalmente da tutto il personale?	Xsi ☐ no
	Q.4	È stato chiaramente identificato e formalizzato il ruolo di Responsabile della Sicurezza Informatica?	Xsi ☐ no
	Q.5	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?	Xsi ☐ no

RISORSE UMANE	Q.6	Quali strumenti adotta l'organizzazione per sensibilizzare i propri dipendenti in materia di sicurezza informatica?	X attacchi simulati antiphishing X corsi di formazione formali (Learning management system/Webinar) ☐ Microlearning (video/quiz interattivi) ☐ condivisione di articoli, segnalazioni/bollettini via mail ☐ nessuno
	Q.7	Durante la conclusione del rapporto di lavoro, l'organizzazione adotta quali di questi step?	X Notifica automatica a IT/HR per revoca accessi (account, VPN, badge) X Recupero asset fisici e credenziali (laptop, smartphone, token) ☐ Cancellazione o revoca di certificati

Q.8	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?	☒ si ☐ no
Q.9	L'organizzazione ha definito, formalizzato e condiviso con 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.)?	☒ si ☐ no
Q.10	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, patch management, password policy, MFA, aggiornamenti, cifratura, backup dei dati)?	☒ si ☐ no In caso affermativo, indicare i dispositivi sui quali sono applicate le misure di sicurezza ☒ laptop ☐ tablet ☐ smartphone
Q.11	L'organizzazione ha attivato modalità di lavoro agile /smart working?	☐ si, con BYOD ☒ si, senza BYOD ☐ no
Q.12	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)?	☐ si ☒ no
Q.13	L'organizzazione utilizza processi e tool differenti per distribuire software e policy su pc aziendali e device personali?	☐ si ☒ no
Q.14	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?	☒ si ☐ no
Q.15	Per le attivazioni su device aziendali, sono state implementate le seguenti misure di sicurezza:	☐ Full-disk Encryption ☐ Data Loss Prevention (DLP) endpoint ☒ Mobile device Management (MDM) ☒ Endpoint Detection & Response (EDR) / Antivirus ☒ Firewall ☒ Single-Sign-On + MFA per tutte le applicazioni aziendali
Q.16	Per le attivazioni in BYOD, sono state implementate le seguenti misure di sicurezza: NESSUNA DI QUESTE	☐ Antivirus /EDR mobile

			☐ revoca privilegi amministratore ☐ Verifica presenza antivirus ☐ Firewall ☐ Single-Sign-On + MFA per tutte le applicazioni aziendali
--	--	--	--

CONTROLLO DEGLI ACCESSI	Q.17	L'organizzazione definisce una politica di controllo degli accessi basata sul principio del privilegio minimo?	X si ☐ no
	Q.18	La politica di controllo accessi prevede una fase di riesame periodico dei diritti di accesso degli utenti e degli amministratori di sistema?	X si ☐ no
	Q.19	L'organizzazione provvede a fornire un identificativo univoco e vieta l'utilizzo di identificativi o utenze/app condivise (anche a livello di amministratore di sistema)?	X si ☐ no
	Q.20	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)?	X si ☐ no
	Q.21	L'organizzazione ha implementato e diffuso una password policy che garantisca e applichi un adeguato livello di complessità e robustezza?	X si ☐ no

CONTROLLI CRITTOGRAFICI	Q.22	Quali delle seguenti categorie di dati o dispositivi vengono protette tramite crittografia? (barrare tutte le voci applicabili)	☒ Dispositivi aziendali (PC, laptop, tablet, smartphone) e dispositivi rimovibili (chiavette USB, hard disk esterni) ☒ Dati "at rest" nelle banche dati, file system e sistemi di storage (inclusi NAS/SAN e object storage) ☒ Backup e archivi storici (inclusi backup off-site e su cloud) ☒ Dati "in transito" tra utenti, server e applicazioni (TLS/SSL, VPN, S/MIME, etc.) ☐ Nessuna delle precedenti
-------------------------	------	---	--

SICUREZZA FISICA	Q.23	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?	X si ☐ no
	Q.24	Sono previsti dei sistemi di verifica/registrazione/tracciatura in ingresso dei visitatori che accedono al building / struttura /	X si ☐ no

	impianto, anche attraverso l'esibizione di un documento di identità?	
Q.25	L'accesso ai locali del datacenter è permesso solo al personale autorizzato, dotato di credenziali / badge specifici?	Xsi ☐ no
Q.26	Sono presenti dei sistemi di controllo degli accessi al data center? Specificare quali.	X Apparatì CCTV ☐ Bussòle di accesso degli edifici con metal detector (sono presenti metal detector all'ingresso degli edifici del campus sogei e tornelli, le bussòle sono presenti sono in alcune aree) X Sensori anti-intrusione e dissuasori veicolari X Sistemi tecnologici anti-tailgating X Sensori volumetrici X Lettori badge / password / chiavi elettroniche (anche con doppi sistemi di autenticazione) ☐ Sistema di acquisizione delle impronte digitali con rilevamento di impronta falsa ☐ Altro, specificare _____
Q.27	Le operazioni di manutenzione da parte dei fornitori all'interno del data center in house sono sempre supervisionate da personale interno?	☐ sì Xno
Q.28	Esiste una procedura di revisione periodica degli accessi al building / infrastruttura / data center (log controllo accessi o revisione dei registri cartacei)?	☐ sì X no
Q.29	Caratteristiche del data center:	X rack e i server presenti all'interno del data center prevedono sempre una ridondanza delle linee elettriche X UPS X Gruppi elettrogeni di backup con avviamento automatico e test periodico programmato X il sistema di condizionamento è correttamente dimensionato e dotato di sistemi automatici di rilevamento e allerta di temperatura e umidità X sistemi di controllo antifumo e di rilevazione di sicurezza ambientale (es. sensori per pavimento flottante) X il sistema di cablaggio strutturato è conforme alle normative di settore ☐ Altro, specificare _____

SI CU RE	Q.30	[Change Management] Le fasi di change management prendono sempre in considerazione i requisiti di	Xsi ☐ no
----------------	------	---	---------------------------------

	sicurezza e i criteri di accettazione per nuove versioni o sistemi?	
Q.31	[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?	☒ si ☐ no
Q.32	[Anti-Malware] - È presente un sistema centralizzato di gestione antivirus/anti-malware (o EDR/XDR) con aggiornamento definito (minimo mensile, preferibilmente automatico giornaliero) che copre tutti gli endpoint, server e dispositivi mobili rientranti nella copertura assicurativa?	☒ si ☐ no
Q.33	[Anti-Malware] - L'organizzazione pianifica ed esegue scansioni periodiche su tutti gli asset informatici che sono oggetto della copertura assicurativa?	☒ si ☐ no
Q.34	[Anti-Malware] - Le impostazioni antivirus/anti-malware prevedono la scansione automatica di:	☒ Allegati di posta in ingresso e in uscita (gateway mail o client-side) ☒ Dispositivi di storage rimovibile (USB, dischi esterni) ☒ File decompressi (archivi ZIP, RAR, ISO) ☒ URL e download in web browsing ☐ Nessuno dei precedenti
Q.35	[Backup] – Con quale frequenza è eseguito il back up dei dati?	☒ Quotidiano ☐ Settimanale ☐ Mensile
Q.36	[Backup] Quale modalità di salvataggio e recupero dati fa parte della strategia di back up scelta dall'organizzazione?	☐ back up completo ☐ back up differenziale ☒ back up incrementale
Q.37	[Backup] - L'organizzazione si è dotata di una procedura di backup che identifica le informazioni critiche per il business?	☒ si ☐ no
Q.38	[Backup] - Dove sono salvate le copie di back up?	☒ supporti esterni (Server o NAS, chiavette USB, dischi esterni, etc.) ☐ Cloud
Q.39	[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?	☒ si ☐ no
Q.40	[Backup] - Vengono eseguiti periodicamente test di ripristino, in particolare dei database che sono oggetto della copertura assicurativa?	☒ si ☐ no

Q.41	[Backup] - Le copie di backup vengono protette in base al livello di confidenzialità delle informazioni che contengono?	☒ sì ☐ no
Q.42	[Backup]- Vengono eseguiti i backup delle configurazioni degli apparati di rete (es. router, firewall ecc.)?	☒ sì ☐ no
Q.43	Il sistema di backup prevede delle copie offline?	☒ sì ☐ no
Q.44	[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"?	☒ sì ☐ no
Q.45	[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)?	☒ sì ☐ no
Q.46	[Raccolta Log & Monitoraggio] - L'organizzazione si è dotata di sistema di correlazione e gestione dei log anche in ottica forense?	☒ sì ☐ no
Q.47	[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?	☒ sì ☐ no
Q.48	[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?	☒ sì ☐ no
Q.49	[Raccolta Log & Monitoraggio] - Quali misure di protezione sono state adottate dall'organizzazione per assicurare l'inalterabilità dei Log?	☒ accesso fisico controllato per le aree contenenti gli apparati di gestione dei log ☒ accesso logico ai dati tramite 2FA- two factor authentication ☒ crittografia dei file durante la conservazione ☐ Altro, specificare
Q.50	[Raccolta Log & Monitoraggio] - Indicare le tempistiche di conservazione dei file di log stabilite dall'organizzazione.	☐ < 6 mesi ☐ ≥ 6 mesi ☒ ≥ 12 mesi ☒ Altro, specificare Alcuni Log vengono mantenuti per un tempo definito dalle esigenze di business

Q.51	Sono attuate procedure per controllare l'installazione di software sui sistemi gestiti?	☒ sì ☐ no
Q.52	[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?	☒ sì ☐ no In caso affermativo, descrivere le principali criticità emerse
Q.53	Selezionare quali tra le seguenti misure sono implementate:	☒ antispam (soluzioni di filtraggio della posta elettronica che blocca gli allegati dannosi e file sospetti) ☒ Firewall ☒ Web application firewall ☒ SOC (Centro Operativo di sicurezza) ☒ SIEM (Security Information And Event Management) ☒ Webfiltering (soluzione di filtraggio web che impedisce ai dipendenti di visitare pagine web dannose o sospette note) ☐ DLP (Data Loss Prevention) ☒ autenticazione multifattoriale ☒ specifici sistemi di protezione contro attacchi DDOS ☒ specifici sistemi di protezione contro attacchi SLOW http ☐ sistemi di blocco delle porte USB
Q.54	In merito alle procedure di Patching Management adottate:	☒ le patch critiche sono aggiornate entro 30 giorni dal loro rilascio ☐ le patch non critiche vengono aggiornate entro 6 mesi dal loro rilascio ☐ non esiste una politica definita per la distribuzione delle patch (in questo caso, specificare modalità e tempistiche di aggiornamento adottate)
Q.55	È stata condotta un'approfondita analisi al fine di verificare se i sistemi non siano parte di una Botnet?	☐ sì ☒ no In caso affermativo, sono state adottate le opportune misure di bonifica? ☐ sì ☐ no

SICUREZZA DELLE RETI

Q.56	L'organizzazione dispone di sistemi firewall aggiornati ?	☒ si ☐ no
Q.57	E' attivo un monitoraggio in tempo reale sulle anomalie ?	☒ si ☐ no
Q.58	L'organizzazione si è dotata di sistemi di intrusion detection/prevention (IDS/IPS), costantemente aggiornati?	☒ si ☐ no
Q.59	Le connessioni di telecomunicazione adottano sistemi di ridondanza per garantire continuità operativa?	☒ si ☐ no
Q.60	In relazione alle informazioni scambiate su reti pubbliche (da e verso internet), viene garantito un adeguato livello di cifratura del canale o delle informazioni trasmesse (es. adozione di protocolli di tunnelling in VPN / SSL o SSH nelle ultime versioni disponibili)?	☒ si ☐ no
Q.61	L'organizzazione ha segregato la rete interna (LAN) in Virtual LAN (VLAN) o domini in base al livello di sicurezza dei processi e informazioni gestite?	☒ si ☐ no
Q.62	Se l'organizzazione fa parte di un gruppo con sedi estere, ha provveduto a segregare le reti delle sedi italiane dalle sedi estere?	☐ si ☐ no NON FA PARTE DI UN GRUPPO CON SEDI ESTERE
Q.63	Relativamente alle politiche di segmentazione implementate, selezionare ciò che si applica alla postura dell'organizzazione:	☐ l'organizzazione ha segmentato la rete in base all'area geografica (e.g.: il traffico tra uffici in luoghi diversi è negato a meno che non sia richiesto per supportare uno specifico requisito aziendale); ☐ l'organizzazione ha segmentato la rete in base alla funzione aziendale (ad esempio il traffico tra asset che supportano funzioni diverse, ad esempio HR e Finance, è negato a meno che non sia richiesto per supportare uno specifico requisito aziendale); ☐ l'organizzazione ha implementato regole del firewall host che impediscono l'uso di Remote Desktop Protocol - RDP per accedere alle workstation; ☐ l'organizzazione ha configurato tutti gli account di servizio per negare gli accessi interattivi; ☒ Nessuno dei precedenti.

FORNITORI
ESTERNI

Q.64	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?	☒ si ☐ no
------	---	--

	Q.65	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 ?	☐ sì, sono autorizzate connessioni remote via VPN ☒ sì, sono autorizzate connessioni remote con autenticazione multifattoriale ☐ Nessuna delle precedenti (specificare la modalità di accesso) ☐ no
	Q.66	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.)?	☐ sì ☒ no

ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEI SISTEMI INFORMATIVI	Q.67	L'azienda adotta controlli di adeguatezza, conformità e sicurezza rispetto a software/sistemi informativi sviluppati da terze parti?	☒ sì ☐ no
	Q.68	L'accesso agli ambienti di sviluppo, pre-produzione e produzione è consentito attraverso l'utilizzo di account diversi per ogni ambiente?	☒ sì ☐ no
	Q.69	Sono eseguite periodicamente le manutenzioni programmate richieste dalle specifiche dei produttori?	☒ sì ☐ no

CONTINUITA' OPERATIVA	Q.70	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?	☒ sì ☐ no
	Q.71	L'organizzazione si è dotata di un piano di ripristino o Business Continuity Plan (BCP) integrato con procedure operative e istruzioni di ripristino dettagliate?	☒ sì ☐ no
	Q.72	L'organizzazione identifica e definisce in un Disaster recovery Plan tutte le attività di ripristino tecnico?	☒ sì ☐ no
	Q.73	Sono testati regolarmente:	☐ il piano di business continuity ☒ il piano di disaster recovery
	Q.74	L'organizzazione ha adottato 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?	☒ sì ☐ no

	Q.75	Si coinvolgono i fornitori nei test di continuità operativa?	☐ si ☒ no (solo in caso di problemi)
	Q.76	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:	
		Attività (o settori)	Massimo periodo di interruzione prima di avere un impatto negativo
		(I tempi sono definiti dalle BIA effettuate su tutti i servizi. Vale quindi l'RTO lì definito)	☐ immediatamente ☐ >4ore ☐ >12ore ☐ >24ore ☐ >48 ore ☐ >5giorni ☐ mai
			☐ immediatamente ☐ >4ore ☐ >12ore ☐ >24ore ☐ >48 ore ☐ >5giorni ☐ mai
			☐ immediatamente ☐ >4ore ☐ >12ore ☐ >24ore ☐ >48 ore ☐ >5giorni ☐ mai
Q.77	Indicare, in caso di interruzione di rete o guasto di sistema, una stima della massima perdita finanziaria per ogni ora di interruzione	(La perdita in senso letterale si potrebbe avere non per noi ma per lo stato e solo in caso dei giochi per perdite di tasse o richiesta danni dei concessionari (va chiesto al mercato se esiste un massimale) Per altri servizi le perdite sono al limite identificabili con i lds e quindi vale la norma sul massimale delle penali su un contratto.)	

GESTIONE INCIDENTI	Q.78	L'organizzazione ha implementato un processo di Incident Management/Response (persone, ruoli, responsabilità)?	☒ si ☐ no
	Q.79	Esistono playbook (elenchi azioni predefinite) in funzione del tipo di incidente occorso (es. sospensione cautelativa del sistema colpito, cambio password, ecc.)?	☒ si ☐ no (Ovviamente sono limitati agli interventi di primo livello rilasciati alla Control Room)

	I dipendenti sanno come segnalare internamente un evento di sicurezza o una vulnerabilità?	☒ sì ☐ no
--	--	--

Sez.3

GESTIONE DEI DATI PERSONALI

GESTIONE DELLE ESPOSIZIONI PRIVACY	Q.80	Nell'esercizio della propria attività, che tipo di dati personali raccoglie, processa o conserva l'organizzazione?	
		Tipologia dei dati trattati	Volume dei dati trattati
		☒ dati finanziari (carte di credito/ debito/conto corrente)	☐ ≤100 ☐ ≤1.000 ☐ ≤100.000 ☐ ≤1.000.000 ☒ ≥1.000.000
		☒ dati personali di terzi Soggetti	☐ ≤100 ☐ ≤1.000 ☐ ≤100.000 ☐ ≤1.000.000 ☒ ≥1.000.000
		☒ Dati appartenenti a categorie particolari ai sensi dell'art. 9 GDPR (es. dati sanitari, dati biometrici, convinzioni religiose, appartenenza sindacale)	☐ ≤100 ☐ ≤1.000 ☐ ≤100.000 ☐ ≤1.000.000 ☒ ≥1.000.000
		Specificare quali ☐ proprietà intellettuale/copyrights/segrete commerciali	☒ ≤100 ☐ ≤1.000 ☐ ≤100.000 ☐ ≤1.000.000 ☐ ≥1.000.000
	Q.81	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>	☒ sì ☐ no
	Q.82	Indicare le misure organizzative implementate per l'adeguamento alla normativa nazionale ed europea in materia di trattamento dei dati	☒ aggiornamento informative (dipendenti, clienti, sito internet - inclusa Cookie Policy, ecc.) ☒ periodiche sessioni di formazione per dipendenti in materia privacy

		☒ processo di raccolta e gestione di consensi informati ☒ tutele rafforzate nel trattamento di categorie particolari di dati (es. informazioni sanitarie) ☒ redazione e aggiornamento registro dei trattamenti ☒ aggiornamento nomine per il trattamento dei dati (incaricati al trattamento, responsabili, amministratori di sistema, etc.) ☒ trasferimento dati extra UE nel rispetto delle condizioni dalla normativa (art. 44, 45 e 46 GDPR) ☐ Altro
Q.83	Quali delle seguenti Policy (nelle quali sono anche definiti ruoli e responsabilità) sono state adottate dall'organizzazione?	☒ Data Breach ☒ Data Retention (nella quale sono stati stabiliti i termini di conservazione e relativa cancellazione dei dati per tutti i trattamenti) ☒ Gestione delle richieste degli interessati in materia privacy ☒ Regolamento sul corretto utilizzo dei sistemi informatici aziendali ☐ Altro, specificare
Q.84	A chi è attribuita l'attività di gestione della privacy dell'organizzazione?	☐ Società di consulenza o studio legale ☒ Ufficio privacy all'interno dell'azienda (Privacy manager) ☐ Libero professionista
Q.85	L'organizzazione ha nominato un Responsabile della protezione dei dati (DPO)?	☒ sì ☐ no ☐ non soggetta
Q.86	L'organizzazione effettua i seguenti trattamenti:	☐ 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.) ☐ Decisioni automatizzate che producono significativi effetti giuridici sull'interessato (es. selezione candidati tramite algoritmo)

		☐ Utilizzo nuove soluzioni tecnologiche e organizzative (es. associazione di tecniche dattiloscopiche e riconoscimento del volto per il controllo degli accessi fisici) ☐ Monitoraggio regolare e sistematico (es. sorveglianza sistematica di un'area accessibile al pubblico) ☒ 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) ☒ 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.87	Sono previsti dei sistemi dai quali può derivare un controllo anche a distanza dei dipendenti?	☒ sì ☐ no In caso affermativo, indicare quali: ☐ sistemi di geolocalizzazione (veicoli) ☒ videosorveglianza ☒ monitoraggio della navigazione internet (sistema di log, etc.) ☐ altro _____
Q.88	Nel caso in cui l'organizzazione esegua uno dei trattamenti descritti nei due punti precedenti (Q.82 – Q.83), ha provveduto ad effettuare una valutazione d'impatto sulla protezione dei dati (DPIA) prima di procedere al trattamento?	☒ sì ☐ no

GESTIONE DELLA MULTIMEDIALITA'	Q.89	Di quale tipologia di canali digitali si avvale l'organizzazione?	☒ Social Network ☐ Blog ☐ Chatroom
	Q.90	Sul sito web aziendale, sono previste:	☒ procedure di doppio opt-in per la raccolta delle informazioni personali degli utenti (es. in fase di iscrizione al sito, newsletter, etc.) ☐ procedure di opt out, compreso l'inserimento del link per la disiscrizione al servizio (es. newsletter) ☐ procedure per la tracciabilità e/o profilazione degli utenti/visitatori (es. cookie, etc.)
	Q.90 bis	Il sito web aziendale utilizza cookie tecnici e/o di profilazione?	☐ sì, solo tecnici ☐ sì, anche di profilazione ☐ no In caso affermativo, è presente un banner informativo conforme alla normativa e una cookie policy aggiornata? ☐ sì ☐ no
	Q.91	L'organizzazione esternalizza tutta o solo in parte la propria pubblicità online a terze parti?	☒ viene esternalizzata tutta la pubblicità online ☐ viene esternalizzata solo una parte (indicare quale) ☐ no, la pubblicità viene gestita da un ufficio interno all'organizzazione
	Q.92	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?	☒ sì ☐ no In caso affermativo, descrivere quali (es. ricorso ad un legale qualificato, etc.) POLICY SOCIAL
	Q.93	La vagliatura dei contenuti pubblicati sui canali online dell'organizzazione, comprende:	☒ violazione del diritto alla riservatezza ☒ violazione del copyright ☐ lesione dell'altrui reputazione ☐ altro, specificare _____

Q.94

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?

☐ sì ☒ no

In caso affermativo, descrivere la procedura adottata

L'organizzazione dispone di un inventario aggiornato di tutti gli asset OT?	☒ si ☐ no
La contraente utilizza sistemi di controllo industriale (SCADA - supervisory control and data acquisition, DCS - distributed control systems, PLC - programmable logic controllers, embedded systems, ecc.)?	☐ sì, gestiti internamente ☐ sì, gestiti fornitori esterni ☒ no
L'accesso del personale alle aree di produzione è regolato da sistemi di controllo (es. badge, tornelli, autenticazione)?	☒ sì ☐ no
L'organizzazione applica patch regolari e controlli mensili sui dispositivi OT/SCADA?	☒ sì ☐ no
L'Organizzazione applica un controllo degli accessi basato sul principio del privilegio minimo sugli elementi ICS/SCADA/OT?	☐ sì ☐ no
L'organizzazione separa le reti OT e IT (es. tramite VLAN o firewall dedicati)?	☒ sì, tramite Firewall ☐ sì, tramite VLAN ☐ sì, tramite DMZ ☐ sì, tramite Gateway di sicurezza unidirezionali ☐ no
L'ambiente OT è separato da Internet?	☒ sì, tramite Firewall ☐ sì, tramite VLAN ☐ sì, tramite DMZ ☐ sì, tramite Gateway di sicurezza unidirezionali ☐ no
L'organizzazione esegue backup regolari dei programmi e delle configurazioni dei sistemi di automazione e supervisione?	☒ sì ☐ no
L'organizzazione dispone di un piano documentato di risposta agli incidenti per gli ambienti OT/SCADA?	☐ sì ☒ no

	L'organizzazione centralizza e analizza i principali eventi di sicurezza (accessi non autorizzati, errori critici) tramite un sistema SIEM o equivalente?	☐ si ☒ no
	L'organizzazione consente l'accesso remoto ai sistemi OT/SCADA solo tramite VPN o autenticazione multifattoriale?	☐ si tramite VPN ☐ si tramite un'autenticazione multifattoriale ☐ si tramite autenticazione a fattore singolo (utenza e password complessa) ☐ soltanto alcuni dipendenti sono autorizzati ad accedere da remoto ai dispositivi ICS/SCADA/OT ☒ no
	L'organizzazione eroga al personale operativo e manutentori OT una formazione di base sulla sicurezza almeno una volta all'anno?	☐ si ☒ no

INCIDENTE INFORMATICO

GESTIONE INCIDENTE

In relazione all'incidente occorso indicare:

Data di accadimento

Breve descrizione dell'incidente

Sfruttamento di una vulnerabilità "0 day" su MS Sharepoint.

Tempistiche di rilevazione dell'anomalia

☒ immediatamente

☐ >4ore ☐ >12ore ☐ >24ore ☐ >48 ore ☐ >5giorni

Altro, specificare

Qual è stato il vettore di ingresso dell'incidente

☐ sito internet

☐ E-mail

☐ Phone

☐ dispositivi aziendali

☐ dispositivi aziendali persi/rubati

☐ dispositivi personali dei dipendenti (BYOD)

☐ abuso Amministratori di Sistema

☐ Rete di terze parti

☒ Altro, specificare

Servizio esposto su internet

L'incidente ha colpito direttamente l'organizzazione o indirettamente attraverso un incidente informatico subito da un fornitore di servizi?	☒ direttamente ☐ indirettamente <i>(Indicare il provider di servizi)</i>
L'incidente subito dall'organizzazione ha colpito indirettamente sistemi e infrastrutture di Terzi?	☒ no ☐ si <i>(Indicare i nominativi dei Terzi coinvolti)</i>
Quali vulnerabilità sono state rilevate a seguito dell'incidente subito?	☒ gestione inadeguata delle patch ☐ installazione di software non autorizzato/ versione non aggiornata ☒ sistemi operativi non più aggiornabili (legacy) ☐ gestione inadeguata degli account con privilegi ☐ protezione inadeguata e-mail / browser web ☐ Difese antimalware inadeguate ☐ Configurazioni di sicurezza inadeguate per hardware e software su dispositivi, laptop, workstation, server ☐ Inadeguati sistemi di sicurezza per il controllo degli accessi alla struttura ☐ Controllo inadeguato di porte di rete, protocolli e servizi ☐ Resilienza e / o backup inadeguati di sistemi o file ☐ Dispositivi di rete non protetti (firewall, router, switch) ☐ Manutenzione e monitoraggio dei LOG inadeguati ☐ Penetration & Security Testing inadeguati ☐ Segmentazione di rete inadeguata ☐ Mancanza di consapevolezza/conoscenza del personale ☐ Bug del software ☐ Difetti hardware ☐ Questioni procedurali

	☐ Altro, specificare
Servizi e componenti interessati dall'incidente	☐ Endpoint / client (laptop, PC, sistemi operativi, applicazioni utente, ecc.) ☒ Applicazione / software utente correlato alle banche (vendita, negoziazione, credito, ecc.) ☐ Reti e telecomunicazioni (firewall, router, switch, PBX, ecc.) ☐ Gestione e archiviazione dei dati (file server, database, data warehouse, ecc.) ☐ Applicazioni software aziendali (SAP, Oracle, ecc.) ☒ Piattaforme Internet (server web, server di applicazioni, ecc.) ☐ Altro, specificare
Sistemi interessati dall'incidente	☒ Applicazioni/software ☐ Hardware ☐ Database ☐ Network/Infrastrutture ☐ Altro, specificare
Aree aziendali interessate dall'incidente	☐ Direzione ☐ Risorse Umane ☐ Amministrazione e controllo ☐ Contabilità ☐ Ricerca e Sviluppo ☐ Acquisti ☐ Logistica e Magazzino ☐ Commerciale e vendite ☐ Marketing

		☐ Affari legali e societari ☒ Gestione Tecnica ☐ Produzione ☐ Altro, specificare
	Indicare la durata dell'interruzione dell'attività aziendale conseguente all'incidente occorso	2 giorni
	Indicare l'impatto economico	Nessun impatto significativo
MISURE POST INCIDENTE	Indicare le principali azioni / misure correttive intraprese / pianificate per evitare che l'incidente si ripeta in futuro	Aggiornamento sistemi obsoleti

	E' stata fatta una root cause analysis?	Si
	La Società, a seguito dell'incidente occorso ha calendarizzato l'esecuzione di un vulnerability assessment o di un penetration test con il supporto di esperti informatici?	X si ☐ no

Dichiarazioni del Contraente

Il Contraente dichiara che:

- le dichiarazioni rese sono conformi a verità e dichiara di non aver omesso alcun elemento influente sulla valutazione del rischio, circostanza che potrebbe comportare l'inoperatività della garanzia assicurativa;
- la compilazione del presente Questionario di raccolta dati NON impegna alla stipulazione della Polizza di assicurazione.

Luogo e data della sottoscrizione

Titolo/Funzione dell'incaricato e Firma



CRISTINA
BARBARANELLI
Sogei S.p.A.
23.03.2026 16:54:32
GMT+01:00