

**GARA EUROPEA A PROCEDURA TELEMATICA APERTA AI SENSI DELL'ART 71 DEL D.LGS. N. 36/2023 PER  
L'AFFIDAMENTO DEI "SERVIZI ASSICURATIVI DELL'ERSU"**

Lotto 1 – CIG B3FAF5D7A8 - RIF. APP. 58LP/2024	Servizio di copertura assicurativa della "Responsabilità Civile verso terzi e Prestatori d'opera" (RCT/RCO)
Lotto 2 – CIG B3FAF5E87B - RIF. APP. 59LP/2024	Servizio di copertura assicurativa per la "Responsabilità civile patrimoniale"
Lotto 3 – CIG B3FAF5F94E - RIF. APP. 60LP/2024	Servizio di copertura assicurativa "All Risks patrimonio mobiliare ed immobiliare"
Lotto 4 –CIG B3FAF60A21 - RIF. APP. 61LP/2024	Servizio di copertura assicurativa "Cyber Risks"

**QUESTIONARIO CYBER**

## Sez.1

## DATI GENERALI CLIENTE E ATTIVITA' SVOLTA

DATI ANAGRAFICI	Denominazione / Ragione sociale Contraente	Ente Regionale per il Diritto allo Studio Universitario di Cagliari (ERSU di Cagliari)
	Cod.Fiscale / Contraente	C.F. 80018410920
	Denominazione / Ragione sociale Assicurato (se diverso)	
	Cod.Fiscale / Partita IVA Assicurato	P. Iva 01031570920
	Indirizzo ubicazione del rischio	Corso Vittorio Emanuele II, n. 65 – CAP 09124 Cagliari
	Presenza di più ubicazioni <i>(In caso affermativo, allegare al presente questionario l'elenco delle altre ubicazioni)</i>	Vedi elenco allegato
	Indirizzo web	<a href="https://ersucagliari.it">https://ersucagliari.it</a>

DATI ATTIVITÀ	Codice Ateco	56.29.10
	Data inizio attività	
	Numero totale dei dipendenti	76
	Numero di dipendenti che non accedono alla rete aziendale	0
	Somme assicurate apparecchiature elettroniche	10.131
	Somma assicurata strumenti IoT e sistemi Scada unitamente ai sistemi fisici a cui si applicano	
	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>	
	Fatturato ultimo esercizio <i>(Allegare l'ultimo bilancio disponibile)</i>	2.834.103
	Indicare la distribuzione geografica del fatturato dell'ultimo esercizio (%)	Unione Europea      Interamente UE USA/Canada          _____ Resto del mondo      _____
	Previsione di fatturato prossimo esercizio	2.733.240
	Indicare la distribuzione geografica del fatturato previsto per il prossimo esercizio (%)	Unione Europea      _____ 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	<input type="checkbox"/> sì <input type="checkbox"/> no

## Questionario Polizza Cyber Risk

	Gruppo e che la gestione dell'infrastruttura informatica sia gestita centralmente dalla Contraente.	In caso contrario, specificare

DESCRIZIONE ATTIVITÀ	Descrivere nel dettaglio l'attività svolta

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
	I pagamenti sono processati da terzi?	<input type="checkbox"/> sì tramite fornitore certificato PCI DSS <input type="checkbox"/> sì tramite fornitore non soggetto allo standard PCI DSS che adotta misure di sicurezza simili e/o adeguate <input checked="" type="checkbox"/> no, i pagamenti sono gestiti internamente
	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 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:  <b>SI CHIEDE INOLTRE DI COMPILARE L'ALLEGATO 3</b>	<input type="checkbox"/> Violazione della privacy, divulgazione non autorizzata o perdita di informazioni riservate <input type="checkbox"/> Reclami/Segnalazioni da parte degli interessati <input type="checkbox"/> Violazione del sistema informatico (attacchi informatici, intrusioni, violazioni della rete o simili) <input type="checkbox"/> Interruzione di servizio non programmata
	L'organizzazione ha subito dei controlli e delle visite ispettive in materia privacy da parte dell'Autorità?	<input type="checkbox"/> sì <input checked="" type="checkbox"/> no In caso affermativo, indicare l'esito dell'ispezione:

MAPPATURA DEGLI ASSET AZIENDALI	Indicare il numero dei computer fissi	<input type="checkbox"/> <100 <input checked="" type="checkbox"/> 101-1000 <input type="checkbox"/> >1001
	Indicare il numero dei device mobili utilizzati:	Tablet <input checked="" type="checkbox"/> <100 <input type="checkbox"/> 101-1000 <input type="checkbox"/> >1001 Smartphone <input checked="" type="checkbox"/> <100 <input type="checkbox"/> 101-1000 <input type="checkbox"/> >1001 Laptop <input checked="" type="checkbox"/> <100 <input type="checkbox"/> 101-1000 <input 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 -11 <input type="checkbox"/> Mac <input type="checkbox"/> Linux <input type="checkbox"/> Altro, specificare
	Indicare i sistemi operativi utilizzati su tablet/smartphone	<input checked="" type="checkbox"/> Android <input type="checkbox"/> iOS
	Indicare il numero dei server	<input checked="" type="checkbox"/> <10 <input type="checkbox"/> <100 <input type="checkbox"/> 101-1000 <input type="checkbox"/> >1001
	Indicare le modalità di gestione dei data center	<input checked="" type="checkbox"/> in house <input checked="" type="checkbox"/> externalizzati in hosting/housing <input type="checkbox"/> in cloud
	Indicare i sistemi operativi utilizzati sui server	<input checked="" type="checkbox"/> precedenti o pari a Windows Server 2008 R2 <input type="checkbox"/> Windows Server 2016 o superiore <input type="checkbox"/> Linux <input type="checkbox"/> Altro, specificare
	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?	<input type="checkbox"/> sì <input checked="" type="checkbox"/> no Se sì, per quali sistemi?
	I sistemi legacy sono isolati da internet e dal resto della rete aziendale?	<input type="checkbox"/> sì <input checked="" type="checkbox"/> no Se sì, come?
	Viene effettuato monitoraggio proattivo? Ad esempio Endpoint Detection & Response (EDR)	<input type="checkbox"/> sì <input checked="" type="checkbox"/> no
L'EDR blocca/isola i sistemi in caso di alert?	<input type="checkbox"/> sì <input checked="" type="checkbox"/> 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?	
	Attività	Fornitore
	<input type="checkbox"/> Desktop management	
	<input checked="" type="checkbox"/> <input type="checkbox"/> Server management	SERVER-PLAN
	<input type="checkbox"/> Network management	
	<input type="checkbox"/> Security management	
	<input type="checkbox"/> Data center hosting	
	<input type="checkbox"/> Data processing	
	<input checked="" type="checkbox"/> <input type="checkbox"/> Application management	MAGGIOLI – IN4MATIC
	<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 type="checkbox"/> Call center/Service desk	
	<input type="checkbox"/> Operational business process	
<input checked="" type="checkbox"/> <input type="checkbox"/> Sistemi di pagamento	SIBEAR RAS - PAGOPA	
<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	
Maggioli Spa	Protocollo/determinazioni/conservazione sostituiva	ITALIA	

## 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 type="checkbox"/> si <input checked="" type="checkbox"/> no  In caso affermativo, indicare la data dell'ultimo aggiornamento e il perimetro a cui si applica la certificazione:
	Q.2	La Direzione Aziendale ha definito, approvato e pubblicato una Politica di Sicurezza delle Informazioni?	<input type="checkbox"/> si <input checked="" type="checkbox"/> no
	Q.3	Le regole espresse dalla Politica di Sicurezza delle Informazioni sono conosciute e accettate formalmente da tutto il personale?	<input type="checkbox"/> si <input checked="" type="checkbox"/> no
	Q.4	La Politica di sicurezza è periodicamente riesaminata ed aggiornata?	<input type="checkbox"/> si <input checked="" type="checkbox"/> no
	Q.5	È stato chiaramente identificato e formalizzato il ruolo di Responsabile della Sicurezza Informatica?	<input type="checkbox"/> si <input checked="" 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 type="checkbox"/> si <input checked="" type="checkbox"/> no

RISORSE UMANE	Q.7	Quali strumenti adotta l'organizzazione per sensibilizzare i propri dipendenti in materia di sicurezza informatica?	<input type="checkbox"/> attacchi simulati antiphishing <input type="checkbox"/> corsi di formazione <input type="checkbox"/> condivisione di articoli, segnalazioni/bollettini via mail <input checked="" type="checkbox"/> nessuno
	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 type="checkbox"/> si <input checked="" type="checkbox"/> no

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 type="checkbox"/> si <input checked="" 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 type="checkbox"/> si <input checked="" 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 type="checkbox"/> si <input checked="" type="checkbox"/> no  In caso affermativo, indicare i dispositivi sui quali sono applicate le misure di sicurezza <input type="checkbox"/> laptop <input type="checkbox"/> tablet <input type="checkbox"/> smartphone
	Q.12	L'organizzazione ha attivato modalità di lavoro agile /smart working?	<input type="checkbox"/> si, con BYOD <input checked="" type="checkbox"/> si, senza BYOD <input type="checkbox"/> no

## Questionario Polizza Cyber Risk

	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 type="checkbox"/> si <input checked="" type="checkbox"/> no
	Q.14	L'organizzazione adotta modalità di deployment differenziando le attivazioni su pc aziendali da quelle in BYOD?	<input type="checkbox"/> si <input checked="" 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 type="checkbox"/> si <input checked="" type="checkbox"/> no
	Q.16	Per le attivazioni su device aziendali, sono state implementate le seguenti misure di sicurezza:	<input type="checkbox"/> disk Encryption <input type="checkbox"/> DLP <input type="checkbox"/> MDM (Mobile device Management) <input checked="" type="checkbox"/> AV con firewall <input 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 checked="" type="checkbox"/> revoca privilegi amministratore <input checked="" 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 type="checkbox"/> si <input checked="" 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 type="checkbox"/> si <input checked="" 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 type="checkbox"/> si <input checked="" 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 type="checkbox"/> si <input checked="" 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 type="checkbox"/> si <input checked="" type="checkbox"/> no

CONTROLLI CRITTOGRAFICI	Q.23	L'organizzazione ha adottato i seguenti sistemi crittografici:	<input type="checkbox"/> sistemi crittografici per i dispositivi, inclusi quelli rimovibili, in dotazione ai dipendenti <input type="checkbox"/> sistemi crittografici per i dati custoditi all'interno delle banche dati informatiche <input checked="" type="checkbox"/> sistemi crittografici per i back up <input type="checkbox"/> Nessuna delle precedenti
-------------------------	------	--	---

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"/> Apparati CCTV <input 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 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 type="checkbox"/> si <input checked="" 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 _____

SICUREZZA DELLE ATTIVITA' OPERATIVE	Q.32	[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 type="checkbox"/> si <input checked="" type="checkbox"/> no
	Q.33	[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 type="checkbox"/> si <input checked="" type="checkbox"/> no
	Q.34	[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 type="checkbox"/> si <input checked="" type="checkbox"/> no
	Q.35	[Anti-Malware] - L'organizzazione pianifica ed esegue scansioni periodiche su tutti gli asset informatici che sono oggetto della copertura assicurativa?	<input type="checkbox"/> si <input checked="" type="checkbox"/> no



Q.36	[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"/> sì <input type="checkbox"/> no
Q.37	[Backup] – Con quale frequenza è eseguito il back up dei dati?	GIORNALIERO
Q.38	[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 SETTIMANALE <input type="checkbox"/> back up differenziale <input checked="" type="checkbox"/> back up incrementale GIORNALIERO
Q.39	[Backup] - L'organizzazione si è dotata di una procedura di backup che identifica le informazioni critiche per il business?	<input type="checkbox"/> sì <input checked="" type="checkbox"/> no
Q.40	[Backup] - Dove sono salvate le copie di back up?	<input checked="" type="checkbox"/> supporti esterni (Server o NAS, chiavette USB, dischi esterni, etc.) <input checked="" type="checkbox"/> Cloud
Q.41	[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 type="checkbox"/> sì <input checked="" type="checkbox"/> no
Q.42	[Backup] - Vengono eseguiti periodicamente test di ripristino, in particolare dei database che sono oggetto della copertura assicurativa?	<input checked="" type="checkbox"/> sì <input type="checkbox"/> no
Q.43	[Backup] - Le copie di backup vengono protette in base al livello di confidenzialità delle informazioni che contengono?	<input checked="" type="checkbox"/> sì <input type="checkbox"/> no
Q.44	[Backup]- Vengono eseguiti i backup delle configurazioni degli apparati di rete (es. router, firewall ecc.)?	<input checked="" type="checkbox"/> sì <input type="checkbox"/> no
Q.44.1	Il sistema di backup prevede delle copie offline?	<input type="checkbox"/> sì <input checked="" type="checkbox"/> no
Q.45	[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 type="checkbox"/> sì <input checked="" type="checkbox"/> no
Q.46	[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 type="checkbox"/> sì <input checked="" type="checkbox"/> no
Q.47	[Raccolta Log & Monitoraggio] - L'organizzazione si è dotata di sistema di correlazione e gestione dei log anche in ottica forense?	<input type="checkbox"/> sì <input checked="" type="checkbox"/> no
Q.48	[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 type="checkbox"/> sì <input checked="" type="checkbox"/> no
Q.49	[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 type="checkbox"/> sì <input checked="" type="checkbox"/> no
Q.50	[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 checked="" type="checkbox"/> crittografia dei file durante la conservazione <input type="checkbox"/> Altro, specificare
Q.51	[Raccolta Log & Monitoraggio] – Indicare le tempistiche di conservazione dei file di log stabilite dall'organizzazione.	<input checked="" type="checkbox"/> < 6 mesi <input type="checkbox"/> ≥ 6 mesi

		<input type="checkbox"/> ≥ 12 mesi <input type="checkbox"/> Altro, specificare
Q.52	Sono attuate procedure per controllare l'installazione di software sui sistemi gestiti?	<input type="checkbox"/> si <input checked="" type="checkbox"/> no
Q.53	[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 type="checkbox"/> si <input checked="" type="checkbox"/> no In caso affermativo, descrivere le principali criticità emerse
Q.53.1	Selezionare quali tra le seguenti misure sono implementate:	<input type="checkbox"/> soluzioni di filtraggio della posta elettronica che blocca gli allegati dannosi e file sospetti (antispam) <input checked="" type="checkbox"/> application firewall <input type="checkbox"/> SOC (Centro Operativo di sicurezza) <input type="checkbox"/> SIEM (Security Information And Event Management) <input type="checkbox"/> soluzione di filtraggio web che impedisce ai dipendenti di visitare pagine web dannose o sospette note (url/content filtering) <input type="checkbox"/> autenticazione multifattoriale <input type="checkbox"/> specifici sistemi di protezione contro attacchi DDOS <input type="checkbox"/> specifici sistemi di protezione contro attacchi SLOW http <input type="checkbox"/> sistemi di blocco delle porte USB
Q.53.2	In merito alle procedure di Patching Management adottate:	<input type="checkbox"/> le patch critiche sono aggiornate entro 30 giorni dal loro rilascio <input type="checkbox"/> le patch non critiche vengono aggiornate entro 6 mesi dal loro rilascio <input checked="" type="checkbox"/> non esiste una politica definita per la distribuzione delle patch (in questo caso, specificare modalità e tempistiche di aggiornamento adottate) _____
Q.53.3	È stata condotta un'approfondita analisi al fine di verificare se i sistemi non siano parte di una Botnet?	<input type="checkbox"/> si <input type="checkbox"/> no  In caso affermativo, sono state adottate le opportune misure di bonifica? <input type="checkbox"/> si <input type="checkbox"/> no

SICUREZZA DELLE RETI	Q.54	L'organizzazione dispone di sistemi firewall aggiornati ?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.55	E' attivo un monitoraggio in tempo reale sulle anomalie ?	<input type="checkbox"/> si <input checked="" type="checkbox"/> no
	Q.56	L'organizzazione si è dotata di sistemi di intrusion detection/prevention (IDS/IPS), costantemente aggiornati?	<input type="checkbox"/> si <input checked="" type="checkbox"/> no
	Q.57	Le connessioni di telecomunicazione adottano sistemi di ridondanza per garantire continuità operativa?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.58	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)?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
	Q.59	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?	<input type="checkbox"/> si <input type="checkbox"/> no

	Q.59.1	Se l'organizzazione fa parte di un gruppo con sedi estere, ha provveduto a segregare le reti delle sedi italiane dalle sedi estere?	<input type="checkbox"/> sì <input type="checkbox"/> no <b>Non fa parte</b>
	Q.59.2	Relativamente alle politiche di segmentazione implementate, selezionare ciò che si applica alla postura dell'organizzazione:	<input type="checkbox"/> 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); <input type="checkbox"/> 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); <input type="checkbox"/> l'organizzazione ha implementato regole del firewall host che impediscono l'uso di Remote Desktop Protocol - RDP per accedere alle workstation; <input type="checkbox"/> l'organizzazione ha configurato tutti gli account di servizio per negare gli accessi interattivi; <b>X</b> <input type="checkbox"/> Nessuno dei precedenti.

FORNITORI ESTERNI	Q.60	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"/> sì <b>X</b> <input type="checkbox"/> no
	Q.61	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 type="checkbox"/> sì, sono autorizzate connessioni remote via VPN <input type="checkbox"/> sì, sono autorizzate connessioni remote con autenticazione multifattoriale <input type="checkbox"/> Nessuna delle precedenti (specificare la modalità di accesso) <b>X</b> <input type="checkbox"/> no
	Q.62	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.)?	<b>X</b> <input type="checkbox"/> sì <input type="checkbox"/> no

ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEI SISTEMI	Q.63	L'azienda adotta controlli di adeguatezza, conformità e sicurezza rispetto a software/sistemi informativi sviluppati da terze parti?	<input type="checkbox"/> sì <b>X</b> <input type="checkbox"/> no
	Q.64	L'accesso agli ambienti di sviluppo, pre-produzione e produzione è consentito attraverso l'utilizzo di account diversi per ogni ambiente?	<input type="checkbox"/> sì <b>X</b> <input type="checkbox"/> no
	Q.65	Sono eseguite periodicamente le manutenzioni programmate richieste dalle specifiche dei produttori?	<input type="checkbox"/> sì <b>X</b> <input type="checkbox"/> no

CONTINUITÀ OPERATIVA	Q.66	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 type="checkbox"/> sì <b>X</b> <input type="checkbox"/> no
	Q.67	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 type="checkbox"/> sì <b>X</b> <input type="checkbox"/> no
	Q.68	L'organizzazione identifica e definisce in un Disaster recovery Plan tutte le attività di ripristino tecnico?	<input type="checkbox"/> sì <b>X</b> <input type="checkbox"/> no
	Q.69	Sono testati regolarmente:	<input type="checkbox"/> il piano di business continuity

			<input type="checkbox"/> il piano di disaster recovery
	Q.70	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 type="checkbox"/> si <input checked="" type="checkbox"/> no
	Q.71	Si coinvolgono i fornitori nei test di continuità operativa?	<input type="checkbox"/> si <input checked="" type="checkbox"/> no
	Q.72	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
			<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
			<input 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
			<input 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.73	Indicare, in caso di interruzione di rete o guasto di sistema, una stima della massima perdita finanziaria per ogni ora di interruzione	???	

GESTIONE INCIDENTI	Q.74	L'organizzazione ha implementato un processo di Incident Management/Response (persone, ruoli, responsabilità)?	<input type="checkbox"/> si <input checked="" type="checkbox"/> no
	Q.75	Esistono playbook (elenchi azioni predefinite) in funzione del tipo di incidente occorso (es. sospensione cautelativa del sistema colpito, cambio password, ecc.)?	<input type="checkbox"/> si <input checked="" type="checkbox"/> no

## Sez.3

## GESTIONE DEI DATI PERSONALI

GESTIONE DELLE ESPOSIZIONI PRIVACY	Q.76	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 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 type="checkbox"/> ≥1.000.000
		<input 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 type="checkbox"/> ≥1.000.000
		<input 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 type="checkbox"/> ≥1.000.000
		<input type="checkbox"/> proprietà intellettuale/copyrights/segreti 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.77	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 type="checkbox"/> sì <input type="checkbox"/> no
	Q.78	Indicare le misure organizzative implementate per l'adeguamento alla normativa nazionale ed europea in materia di trattamento dei dati	<input checked="" type="checkbox"/> <input type="checkbox"/> aggiornamento informative (dipendenti, clienti, sito internet - inclusa Cookie Policy, ecc.) <input type="checkbox"/> periodiche sessioni di formazione per dipendenti in materia privacy <input type="checkbox"/> processo di raccolta e gestione di consensi informati <input type="checkbox"/> tutele rafforzate nel trattamento di categorie particolari di dati (es. informazioni sanitarie) <input checked="" type="checkbox"/> <input type="checkbox"/> redazione e aggiornamento registro dei trattamenti <input checked="" type="checkbox"/> <input type="checkbox"/> aggiornamento nomine per il trattamento dei dati (incaricati al trattamento, responsabili, amministratori di sistema, etc.) <input type="checkbox"/> trasferimento dati extra UE nel rispetto delle condizioni dalla normativa (art. 44, 45 e 46 GDPR)  <input type="checkbox"/> Altro
	Q.79	Quali delle seguenti Policy (nelle quali sono anche definiti ruoli e responsabilità) sono state adottate dall'organizzazione?	<input type="checkbox"/> Data Breach <input type="checkbox"/> Data Retention (nella quale sono stati stabiliti i termini di conservazione e relativa cancellazione dei dati per tutti i trattamenti) <input checked="" type="checkbox"/> <input type="checkbox"/> Gestione delle richieste degli interessati in materia privacy <input type="checkbox"/> Regolamento sul corretto utilizzo dei sistemi informatici aziendali  <input type="checkbox"/> Altro, specificare
	Q.80	A chi è attribuita l'attività di gestione della privacy dell'organizzazione?	<input type="checkbox"/> Società di consulenza o studio legale <input type="checkbox"/> Ufficio privacy all'interno dell'azienda (Privacy manager) <input type="checkbox"/> Libero professionista
Q.81	L'organizzazione ha nominato un Responsabile della protezione dei dati (DPO)?	<input checked="" type="checkbox"/> <input type="checkbox"/> sì <input type="checkbox"/> no <input type="checkbox"/> non soggetta	
Q.82	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	

		<p>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.)</p> <p><input type="checkbox"/> Decisioni automatizzate che producono significativi effetti giuridici sull'interessato (es. selezione candidati tramite algoritmo)</p> <p><input type="checkbox"/> Utilizzo nuove soluzioni tecnologiche e organizzative (es. associazione di tecniche dattiloscopiche e riconoscimento del volto per il controllo degli accessi fisici)</p> <p><input checked="" type="checkbox"/> <input type="checkbox"/> Monitoraggio regolare e sistematico (es. sorveglianza sistematica di un'area accessibile al pubblico)</p> <p><input 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)</p> <p><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).</p>
<b>Q.83</b>	Sono previsti dei sistemi dai quali può derivare un controllo anche a distanza dei dipendenti?	<p><input type="checkbox"/> sì    <input type="checkbox"/> no</p> <p>In caso affermativo, indicare quali:</p> <p><input type="checkbox"/> sistemi di geolocalizzazione (veicoli)</p> <p><input type="checkbox"/> videosorveglianza</p> <p><input type="checkbox"/> monitoraggio della navigazione internet (sistema di log, etc.)</p> <p><input type="checkbox"/> altro _____</p>
<b>Q.84</b>	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?	<p><input type="checkbox"/> sì    <input type="checkbox"/> no</p>

## Sez.4

## CONTENUTI MULTIMEDIALI

GESTIONE DELLA MULTIMEDIALITA'	Q.85	Di quale tipologia di canali digitali si avvale l'organizzazione?	<input type="checkbox"/> Social Network <input type="checkbox"/> Blog <input type="checkbox"/> Chatroom
	Q.86	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 type="checkbox"/> procedure per la tracciabilità e/o profilazione degli utenti/visitatori (es. cookie, etc.)
	Q.87	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 type="checkbox"/> no, la pubblicità viene gestita da un ufficio interno all'organizzazione
	Q.88	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 type="checkbox"/> sì <input type="checkbox"/> no In caso affermativo, descrivere quali (es. ricorso ad un legale qualificato, etc.) <hr/>
	Q.89	La vagliatura dei contenuti pubblicati sui canali online dell'organizzazione, comprende:	<input type="checkbox"/> violazione del diritto alla riservatezza <input type="checkbox"/> violazione del copyright <input type="checkbox"/> lesione dell'altrui reputazione <input type="checkbox"/> altro, specificare _____
	Q.90	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 type="checkbox"/> no In caso affermativo, descrivere la procedura adottata <hr/>

## Allegato 1.

## VULNERABILITA' NOTA LOG4SHELL

RILEVAMENTO E GESTIONE VULNERABILITA'	L'organizzazione esegue o utilizza sistemi vulnerabili a (CVE-2021-44228)?	<input type="checkbox"/> si <input type="checkbox"/> no
	In caso negativo, è stato confermato dal fornitore di servizi IT?	<input type="checkbox"/> si <input type="checkbox"/> no
	In caso affermativo, i sistemi sono stati aggiornati o implementate mitigazioni/controlli compensativi a breve termine?	<input type="checkbox"/> si <input type="checkbox"/> no
	A quale % di applicazioni vulnerabili è stata applicata la patch?	
	Qual è il piano di mitigazione previsto? (Specificare se è disponibile una cronologia)	
	L'organizzazione ha scansionato i sistemi IT vulnerabili alla ricerca di Indicatori di Compromissione (IoC) e successivamente sono state intraprese eventuali contromisure?	<input type="checkbox"/> si <input type="checkbox"/> no
	Quali misure di rilevamento avete messo in atto?	
	Sono state identificate le terze parti critiche che potrebbero essere vulnerabili?	<input type="checkbox"/> si <input type="checkbox"/> no
	Sono stati aggiornati i Firewall per impedire il possibile testo di injection?	<input type="checkbox"/> si <input type="checkbox"/> no
	È stato implementato uno degli strumenti di scansione log4j?	<input type="checkbox"/> si <input type="checkbox"/> no



## Allegato 2.

## ICS/SCADA/OT

## EFFICACIA DEI CONTROLLI

Quali misure di sicurezza sono adottate dall'Organizzazione contro i malware sugli elementi ICS/SCADA/OT?

- ☐ sistemi di analisi comportamentale
- ☐ Sistemi di prevenzione delle intrusioni basati su host o basati sulla rete
- ☐ sicurezza del firmware

Quali delle seguenti misure sono implementate dall'Organizzazione sui sistemi ICS/SCADA/OT

- ☐ gestione di una configurazione sicura per ciascun ICS/SCADA/OT, comprese le attività di aggiornamento del software, correzione delle vulnerabilità, disabilitazione di servizi non necessari e rafforzamento delle configurazioni dopo ogni valutazione mensile dei rischi
- ☐ controllo degli accessi basata sul principio del privilegio minimo
- ☐ il Richiedente utilizza password sicure per tutti gli account amministratore dei dispositivi
- ☐ I sistemi critici ICS/SCADA/OT hanno configurazioni ridondanti o capacità di failover per evitare danni materiali o interruzione dell'attività
- ☐ sono implementati piani documentati (e collaudati) di Risposta agli incidenti e di Disaster Recovery
- ☐ è in vigore un piano ufficiale di manutenzione fisica per sistemi ICS/SCADA/OT, che comprende un programma di sostituzione regolare e procedure per la prevenzione proattiva (in relazione a corrosione, usura, ecc.)
- ☐ tutti i sistemi critici ICS/SCADA/OT del Richiedente hanno un rilevamento automatico di guasti, integrità e/o perdite che aziona un processo automatico di failover o shut-off per evitare danni materiali e pecuniari
- ☐ Gli amministratori, gli sviluppatori e gli operatori ICS/SCADA/OT seguono una formazione annuale obbligatoria che comprende formazione sul ciclo di vita della sicurezza, consigli per evitare possibilità di aggirare i controlli sulla sicurezza e buone prassi in materia di sicurezza degli elementi ICS/SCADA/OT
- ☐ utilizzo di tecnologia che monitora tutti i dispositivi ICS/SCADA/OT per poter aggiornare l'inventario hardware e rimuovere i dispositivi non autorizzati
- ☐ i log dei dispositivi ICS/SCADA/OT sono aggregati ed analizzati tramite un Sistema Security Information Event Management (SIEM)
- ☐ I dispositivi ICS/SCADA/OT sono registrati all'interno di un sistema di directory aziendale (quale, ad esempio, Active Directory o LDAP)?
- ☐ sono effettuati trimestralmente test di penetrazione dei dispositivi ICS/SCADA/OT e/o esercitazioni red team e per testare la risposta agli incidenti

Il Richiedente separa gli elementi ICS/SCADA/OT in una rete (o reti) isolata(e) dal resto dell'organizzazione?

- ☐ sì ☐ no

	<p>Il Richiedente consente connessioni remote a dispositivi ICS/SCADA/OT per finalità di monitoraggio o controllo?</p>	<p> <input type="checkbox"/> Si tramite VPN  <input type="checkbox"/> Si tramite un'autenticazione multifattoriale  <input type="checkbox"/> si tramite autenticazione a fattore singolo (utenza e pwd complessa)  <input type="checkbox"/> Soltanto alcuni dipendenti sono autorizzati ad accedere da remoto ai dispositivi ICS/SCADA/OT  <input type="checkbox"/> No         </p>
	<p>Il Richiedente effettua i seguenti test per stabilire se tutti i dispositivi ICS/SCADA/OT sono vulnerabili, per migliorare il monitoraggio e la risposta agli incidenti?</p>	<p> <input type="checkbox"/> Test di penetrazione trimestrale che simula metodi di attacco noti a ICS/SCADA/OT  <input type="checkbox"/> Simulazione annuale di attacchi DoS per riprodurre un'eventuale interruzione  <input type="checkbox"/> Simulazione annuale di interruzione dell'alimentazione elettrica         </p>

## Allegato 3.

## INCIDENTE INFORMATICO

GESTIONE INCIDENTE	In relazione all'incidente occorso indicare:	
	Data di accadimento	
	Breve descrizione dell'incidente	
	Tempistiche di rilevazione dell'anomalia	<input type="checkbox"/> immediatamente <input type="checkbox"/> >4ore <input type="checkbox"/> >12ore <input type="checkbox"/> >24ore <input type="checkbox"/> >48 ore <input type="checkbox"/> >5giorni Altro, specificare _____
	Qual è stato il vettore di ingresso dell'incidente	<input type="checkbox"/> sito internet <input type="checkbox"/> E-mail <input type="checkbox"/> Phone <input type="checkbox"/> dispositivi aziendali <input type="checkbox"/> dispositivi aziendali persi/rubati <input type="checkbox"/> dispositivi personali dei dipendenti (BYOD) <input type="checkbox"/> abuso Amministratori di Sistema <input type="checkbox"/> Rete di terze parti <input type="checkbox"/> Altro, specificare _____
	L'incidente ha colpito direttamente l'organizzazione o indirettamente attraverso un incidente informatico subito da un fornitore di servizi?	<input type="checkbox"/> direttamente <input type="checkbox"/> indirettamente ( <i>Indicare il provider di servizi</i> )
	L'incidente subito dall'organizzazione ha colpito indirettamente sistemi e infrastrutture di Terzi?	<input type="checkbox"/> no <input type="checkbox"/> sì ( <i>Indicare i nominativi dei Terzi coinvolti</i> )
Quali vulnerabilità sono state rilevate a seguito dell'incidente subito?	<input type="checkbox"/> gestione inadeguata delle patch <input type="checkbox"/> installazione di software non autorizzato/ versione non aggiornata <input type="checkbox"/> sistemi operativi non più aggiornabili (legacy) <input type="checkbox"/> gestione inadeguata degli account con privilegi <input type="checkbox"/> protezione inadeguata e-mail / browser web <input type="checkbox"/> Difese antimalware inadeguate <input type="checkbox"/> Configurazioni di sicurezza inadeguate per hardware e software su dispositivi, laptop, workstation, server <input type="checkbox"/> Inadeguati sistemi di sicurezza per il controllo degli accessi alla struttura <input type="checkbox"/> Controllo inadeguato di porte di rete, protocolli e servizi <input type="checkbox"/> Resilienza e / o backup inadeguati di sistemi o file <input type="checkbox"/> Dispositivi di rete non protetti (firewall, router, switch) <input type="checkbox"/> Manutenzione e monitoraggio dei LOG inadeguati <input type="checkbox"/> Penetration & Security Testing inadeguati	

	<input type="checkbox"/> Segmentazione di rete inadeguata <input type="checkbox"/> Mancanza di consapevolezza/conoscenza del personale <input type="checkbox"/> Bug del software <input type="checkbox"/> Difetti hardware <input type="checkbox"/> Questioni procedurali <input type="checkbox"/> Altro, specificare
Servizi e componenti interessati dall'incidente	<input type="checkbox"/> Endpoint / client (laptop, PC, sistemi operativi, applicazioni utente, ecc.) <input type="checkbox"/> Applicazione / software utente correlato alle banche (vendita, negoziazione, credito, ecc.) <input type="checkbox"/> Reti e telecomunicazioni (firewall, router, switch, PBX, ecc.) <input type="checkbox"/> Gestione e archiviazione dei dati (file server, database, data warehouse, ecc.) <input type="checkbox"/> Applicazioni software aziendali (SAP, Oracle, ecc.) <input type="checkbox"/> Piattaforme Internet (server web, server di applicazioni, ecc.) <input type="checkbox"/> Altro, specificare
Sistemi interessati dall'incidente	<input type="checkbox"/> Applicazioni/software <input type="checkbox"/> Hardware <input type="checkbox"/> Database <input type="checkbox"/> Network/Infrastrutture <input type="checkbox"/> Altro, specificare
Aree aziendali interessate dall'incidente	<input type="checkbox"/> Direzione <input type="checkbox"/> Risorse Umane <input type="checkbox"/> Amministrazione e controllo <input type="checkbox"/> Contabilità <input type="checkbox"/> Ricerca e Sviluppo <input type="checkbox"/> Acquisti <input type="checkbox"/> Logistica e Magazzino <input type="checkbox"/> Commerciale e vendite <input type="checkbox"/> Marketing <input type="checkbox"/> Affari legali e societari <input type="checkbox"/> Gestione Tecnica <input type="checkbox"/> Produzione <input type="checkbox"/> Altro, specificare
Indicare la durata dell'interruzione dell'attività aziendale conseguente all'incidente occorso	
Indicare l'impatto economico	

MISURE POST INCIDENTE	Indicare le principali azioni / misure correttive intraprese / pianificate per evitare che l'incidente si ripeta in futuro	
	E' stata fatta una root cause analysis?	
	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?	<input type="checkbox"/> si <input type="checkbox"/> no

DICHIARAZIONI	
	La firma del presente questionario non impegna il sottoscrittore, cioè il proponente, né la Compagnia Assicuratrice alla stipulazione della polizza di assicurazione
	Il sottoscritto, in forza dei poteri di sottoscrizione e di rappresentanza disgiunta della società, qui di seguito dichiara che tutte le dichiarazioni e le informazioni rese con il presente questionario sono vere e che non sussistono fatti materiali errati o sottaciuti. Per fatto materiale si intende un qualsiasi accadimento che potrebbe influenzare l'accettazione o la valutazione del rischio.
	Il sottoscritto accetta che il presente questionario, qualsiasi allegato allo stesso o informazione fornita con lo stesso, e tutte le altre informazioni rese e/o richieste, potrebbero costituire la base di un eventuale e futuro contratto di assicurazione. Il sottoscritto conseguentemente si obbliga ad informare l'Assicuratore di qualsiasi modifica materiale di qualsiasi informazione, dichiarazione, rappresentazione o fatto presentati in questo questionario, che si verifichino prima o dopo la data di decorrenza della copertura assicurativa.

Luogo e Data

\_\_\_\_\_

Titolo/Funzione dell'incaricato e Firma

\_\_\_\_\_