Questionario Informativo Cyber Risk

1. Identificazione dell'azienda

Ragione sociale: LAZIO INNOVA SPA

Indirizzo: VIA MARCO AURELIO 26/A

Codice Fiscale/Partita IVA 05950941004

Sito/i Web: WWW.LAZIOINNOVA.IT

Numero di dipendenti: 277

Fatturato annuale: € 38.910.000,00

Margine netto annuo: 0.8%

Percentuale di Fatturato generato in:

USA/Canada: UK:

Unione Europea: 100% Resto del Mondo:

2. Profilo dell'azienda/delle aziende da assicurare

2.1 Attività dell'azienda

LAZIO INNOVA, società *in house* della Regione Lazio, partecipata anche, con quota di minoranza, dalla Camera di Commercio di Roma, è il risultato del processo di riordino delle società della Regione Lazio dedicate all'innovazione, al credito e allo sviluppo economico previsto dalla legge regionale n. 10/2013.

Opera a vantaggio delle imprese e della pubblica amministrazione locale nell'erogazione di incentivi a valere su risorse regionali, nazionali e/o europee; nel sostegno al credito e rilascio di garanzie; negli interventi nel capitale di rischio; nei servizi per l'internazionalizzazione, promozione delle reti d'impresa e delle eccellenze regionali; nei servizi per la nascita e lo sviluppo d'impresa; nelle misure per l'inclusione sociale.

Svolge anche funzioni di assistenza tecnica specialistica alla Regione Lazio, con particolare riferimento all'attuazione della programmazione europea e nazionale.

È inoltre responsabile per conto della Regione dell'attuazione di specifici progetti di sviluppo e internazionalizzazione.

È infine l'antenna regionale dei programmi Europei per l'innovazione attraverso l'analisi, l'ideazione di progetti di cooperazione e l'implementazione di servizi e attività a vantaggio del sistema innovativo laziale.

2.2 Società Controllate

[Si prega di fornire l'elenco delle società controllate da assicurare e descrizione dell'attività. Se l'azienda ha filiali al di fuori dell'UE, si prega di fornire i dettagli]

Nome	Sede	Attività

2.3 Criticità dei sistemi informativi

[Si prega di valutare il periodo di interruzione durante il quale l'azienda subirà un impatto significativo sulla sua attività.]

Settori (o Attività)	Massimo periodo di interruzione prima di avere un impatto negativo				
	Immediato	**> 12 h**	**> 24 h**	**> 48 h**	**> 5 giorni**

Lazio innova non genera alcun fatturato tramite i propri servizi esposti sul Web quindi un down dei sistemi non comporta mai un danno economico.

Esiste solo un tipo di servizio, il cosiddetto "bando a sportello" che prevede una sorta di "click day", in cui un eventuale malfunzionamento del servizio nei primi minuti di apertura del bando potrebbe, nel peggiore dei casi, portare a una richiesta di risarcimento danni da parte degli utenti.

Si sottolinea comunque che la tipologia di bando in questione è caratterizzata da una frequenza molto bassa (massimo 1-2 bandi all'anno) e che il periodo critico complessivo nel corso dell'anno è di pochi minuti, concentrati esclusivamente nel giorno di avvio del bando.

3. Sistemi informativi

Numero di utenti del sistema informativo:	275
Numero di Laptop:	170
Numero di Server:	140 (110 Virtuali + 30 Fisici)

Disponete/Siete proprietari di un servizio di e-commerce o di un sito web? SI [X] NO [ ]

In caso affermativo:
Qual è la quota di fatturato generata dal sito web? 0 (% o effettivo in €)

Lazio innova non genera alcun fatturato tramite i propri servizi esposti sul Web

4. Sistema di Sicurezza delle Informazioni (SSI)

4.1 Security policy e risk management		Sì	No
1	Una politica di SSI è stata formalizzata e approvata dalla direzione aziendale e/o sono state definite e comunicate a tutto lo staff regole di sicurezza approvate dai rappresentanti dello staff	X	
2	Sono formalizzati ed effettuati regolari training (almeno annuali) agli utenti sull'uso sicuro del sistema informativo		X
3	Sono identificati i rischi inerenti i sistemi informativi critici e sono implementati opportuni controlli per mitigarli → [è stato effettuato un assessment nel 2019 sulla sicurezza informatica e i miglioramenti identificati sono in corso di implementazione]	X	
4	Sono condotti audit regolari del SSI ed è assegnata priorità all'implementazione delle raccomandazioni risultanti → [è stato effettuato un VA a luglio 2020 e si stanno implementando le raccomandazioni]	X	
5	Le risorse informative sono classificate in accordo alla loro criticità e sensibilità	X	
6	I requisiti di sicurezza che si applicano alle risorse informative sono definiti in accordo alla loroclassificazione	X	

4.2 Protezione dei sistemi informativi		Sì	No
1	L'accesso ai sistemi informativi critici richiede un sistema di doppia autenticazione	X	
2	Agli utenti è richiesto di aggiornare regolarmente le password	X	
3	Le autorizzazioni di accesso al sistema si basano sui ruoli dei singoli utenti edesiste una procedura per la gestione delle autorizzazioni	X	
4	Sono definiti riferimenti di configurazione sicura per workstation, laptop, server [esclusi dispositivi mobili]	X	
5	È attuata la gestione centralizzata dei sistemi informatici e il monitoraggio delle configurazioni	X	
6	I laptop sono protetti da un personal firewall	X	
7	Un software antivirus è installato su tutti i sistemi e sono monitoratigli aggiornamenti	X	
8	Sono regolarmente distribuite ed installate le security patches	X	
9	Un DRP (Disaster Recovery Plan) è implementato eaggiornato regolarmente		X
10	I backup dei dati sono portati a termine quotidianamente, sono testati regolarmente e copie di essi sono depositate regolarmente in una località remota rispetto a quella ove risiedono i sistemi	X	

4.3 Sicurezza della rete e delle operazioni		Sì	No
1	È installato ed operativo un firewall per il filtraggio del traffico tra la rete interna e internet con un controllo aggiornato del flusso di informazioni in entrata ed in uscita	X	
2	Un IDS/IPS (Intrusion Detection/Prevention System) è implementato, aggiornato e monitorato regolarmente		X
3	Gli utenti interni all'azienda hanno accesso a Internet attraverso dispositivi di rete protetti da antivirus e sistemi di monitoraggio del traffico web → [non è previsto un sistema di monitoraggio della navigazione]	X	
4	È implementata la segmentazione della rete per separare le aree critiche dalle areenon critiche	X	
5	Sono effettuati regolarmente penetration test ed è implementato un remediation plan ove necessario		X
6	Sono effettuati regolarmente vulnerability assessment ed è implementato un remediation plan ove necessario [Effettuato VA a luglio 2020]	X	
7	Sono rese effettive procedure di incident management e change management → [In via di implementazione]		X
8	Eventi riguardanti la sicurezza, come rilevazioni di virus, tentativi di accesso, e simili, sono registrati (tramite log file) e monitorati regolarmente	X	

4.4 Sicurezza fisica della sala computer		Sì	N
1	I sistemi critici sono collocati in almeno una sala computer dedicata con accesso limitato e allarmi operativi funzionanti sono inviati ad una sede di monitoraggio	X	
2	I CED che ospitano sistemi critici hanno un'infrastruttura resiliente che include ridondanza dei sistemi di alimentazione, impianti di condizionamento e connessioni di rete	X	
3	I sistemi critici sono duplicati in funzione di un'architettura Active/Passive o Active/Active	X	
4	I sistemi critici sono duplicati in due sedi separate	X	
5	Sono implementati rilevatori antincendio e sistemi automatici di estinzione in aree critiche	X	
6	L'alimentazione è protetta da UPS e batterie, entrambi sottoposti a regolari programmi di manutenzione	X	
7	L'alimentazione è sostenuta da generatore elettrico soggetto a regolare contratto di manutenzionee testato regolarmente	X	

4.5 Outsourcing		Sì	No
[Si prega di compilare in caso una o più funzioni del sistema informativo è data in outsourcing]			
1	Il contratto di outsourcing include requisiti di sicurezza che devono essere osservati dall'outsourcer	X	
2	I Service Level Agreements (SLA) sono definiti con l'outsourcer al fine di gestire gli incidenti e vengono applicate penalità all'outsourcer in caso di non conformità con i SLA	X	
3	II/I comitato/i di direzione e controllo si coordina con il service provider per la gestione e il perfezionamento del servizio [coordinamento non effettivo per tutti i contratti]	X	
4	L'assicurato ha rinunciato al diritto di ricorso contro l'outsourcer nel contratto di outsourcing [Servizio Amm.ne]		

Quali sono le funzioni del sistema informativo date in outsourcing?

	Sì	No
Desktop management		X
Server management		X
Network management		X
Network security management		X
Application management		X
Utilizzo di cloud computing	X	

Se si, si prega di specificarne la natura

Software as a Service	X	
Platform as a Service	X	
Infrastructure as a Service	X	

Altro, si prega di specificare:

5	Il contratto di outsourcing contiene una disposizione che richiede al service provider di sostenere una polizza assicurativa coprente indennità professionale, errori e omissioni [Servizio Amm.ne]		

5. Dati personali trattenuti dall'azienda

5.1 Tipo e numero di record (archivi/documenti/registri)

Il numero di record contenenti informazioni personali trattenuti per l'attività da assicurare:

Totale: 50.000	Per nazione:	UK/I:
Europe (EU): 50.000	USA/Canada:	Resto del mondo:

Categorie di dati personali raccolti/trattati:	Sì	No	Quantità
Informazioni commerciali e di marketing	X		
Carte di credito o informazioni sulle transazioni finanziarie		X	
Informazioni di natura sanitaria [Relative ai dipendenti]	X		
Altro, si prega di specificare:			

I dati sono trattati: [X] Per fini propri [ ] Per conto di terze parti

5.2 Politica di protezione delle informazioni personali	Sì	No
1 E' stata formalizzata ed approvata dall'amministrazione una politica sulla privacy e/o sono definite e comunicate allo staff interessato regole per la sicurezza dei dati personali	X	
2 Sono forniti corsi di formazione e sensibilizzazione almeno annualmente al personale autorizzato ad accedere a o a trattare con dati personali	X	
3 È nominato un funzionario incaricato della protezione dei dati personali	X	
4 Viene firmato nel contratto di assunzione, da parte dello staff interessato, un accordo o una clausola di riservatezza	X	
5 Gli aspetti legali relativi alla politica sulla privacy sono convalidati da un avvocato o dalla divisionelegale	X	
6 Sono implementate misure di monitoraggio per garantire la conformità con le leggi e regolamentazioni per la protezione dei dati personali	X	
7 Le pratiche/prassi aziendali relative alle informazioni personali sono state sottoposte a auditing daun ispettore esterno negli ultimi due anni		X
8 Un Data Breach Response Plan è implementato e i ruoli sono stati comunicati con chiarezza ai membri della squadra operativa		X

5.3 Raccolta di dati personali	Sì	No
1 Avete notificato al Garante per la protezione dei dati personali il Responsabile del trattamento dei dati personali nominato in azienda e avete ottenuto la rispettiva autorizzazione	X	
Se non applicabile, si prega di spiegare:		
2 È stata pubblicata sul sito aziendale una politica sulla privacy revisionata da un legale/dipartimento legale	X	
3 È richiesto il consenso prima di raccogliere i dati personali e gli interessati possono accedere e, se necessario, correggere o cancellare i loro dati personali	X	
4 Ai proprietari è fornita in modo chiaro la possibilità di rinunciare ad operazioni mirate di marketing	X	
5 Trasferite i dati personali a terzi:	X	
Se si, si prega di rispondere alle seguenti:		
5.a I terzi sono contrattualmente obbligati a trattare i dati personali esclusivamente per conto vostro e secondo le vostre istruzioni	X	
5.b I terzi sono contrattualmente obbligati a implementare sufficienti misure di sicurezza per proteggere i dati personali	X	

5.4 Controlli per la protezione dei dati personali		Sì	No
1	L'accesso ai dati personali è limitato ai soli operatori che lo necessitano per svolgere il proprio incarico e le autorizzazioni di accesso sono revisionate regolarmente	X	
2	I dati personali sono criptati quando archiviati nei sistemi informatici, così come i relativi backup		X
3	I dati personali sono criptati quando trasmessi attraverso la rete		X
4	I dispositivi mobili e gli hard disk dei laptopsono criptati		X
5	La politica di sicurezza delle informazioni proibisce la copia di dati personali non criptati su dispositivi di archiviazione mobili o la trasmissione di tali dati via email [divieto di copia di dati personali]	X	

Se gli archivi di dati personali contengono dati relativi alle carte di credito, si prega di rispondere alle seguenti:

Il vostro livello PCI DSS è:

Livello 1: Livello 2: Livello 3: Livello 4:

	Sì	No
Chi tratta i pagamenti (voi stessi o terzi) rispetta il PCI DSS		
Se No:		
I dati relativi alle carte di credito sono archiviati criptati o solo una parte di essi è archiviata		
Il tempo di mantenimento dei dati relativi alle carte di credito non eccede la durata di pagamento e i requisiti legali/normativi		
Il trattamento dei dati relativi alle carte di credito è esternalizzata		
Se Si:		
È richiesto a chi si occupa del trattamento i pagamenti di indennizzarvi in caso di violazione della sicurezza		

Si prega di indicare il nome di chi si occupa del trattamento dei pagamenti, il tempo di mantenimento dei dati relativi alle carte di credito e ogni ulteriore misura di sicurezza:

5.5 Incidenti

Si prega di fornire una descrizione di qualunque incidente relativo alla sicurezza informatica o alla privacy accaduto nei precedenti 36 mesi. Gli incidenti includono qualunque accesso non autorizzato a qualunque computer, sistema informatico o database, intrusione o attacco, impossibilità d'utilizzo di qualunque computer o sistema, interruzione premeditata, corruzione, o distruzione di dati, programmi, o applicazioni, qualunque evento di cyber estorsione; o qualunque altro incidente simile ai precedenti, inclusi quelli che hanno generato una richiesta di risarcimento, azione amministrativa, o procedimento da parte di un'autorità di vigilanza.

Data: 07/05/2019

Descrizione dell'incidente:

La notte tra i giorni 7 e 8 maggio è avvenuta la violazione probabilmente attraverso password violation.

I dati violati sono i dati di rendicontazione relativi a persone giuridiche e in alcuni casi persone fisiche, beneficiari di finanziamenti in relazione a specifici bandi e azioni gestiti da Lazio Innova. Tra i suddetti dati possono figurare:

(i) i dati anagrafici e il codice fiscale di persone fisiche che prestano la propria attività lavorativa per il beneficiario del finanziamento i cui costi sono rimborsati tramite i fondi erogati da Lazio Innova ovvero, in alcuni casi, dati anagrafici di fornitori persone fisiche del beneficiario le cui fatture sono rimborsate tramite i fondi erogati da Lazio Innova;

(ii) gli importi rimborsati.

Non è possibile individuare, neanche approssimativamente, il numero di interessati coinvolti, mentre il numero approssimativo di registrazioni di dati violati si aggira sui 3,5 milioni.

Esiti e remediation

Lazio Innova ha provveduto a informare il Garante nonché le persone interessate. Ha avviato, inoltre, un assessment sulla sicurezza e l'hardening dei sistemi informativi.

Commenti:

Nessun individuo o ente per cui è richiesta copertura è a conoscenza di alcun fatto, circostanza, o situazione, che ha ragione di suppore possa causare alcuna richiesta di risarcimento **(claim)** che possa ricadere nell'ambito della copertura proposta.

☐ Nessuno

o, tranne: nessuno tranne l'incidente descritto al punto 5.5