REGIONE LAZIO

REGIONE LAZIO

RESP. PREVENZIONE DELLA CORRUZIONE E TRASPARENZA

Area:

DETERMINAZIONE *(con firma digitale)*

N. F00004 **del** 24/01/2024 **Proposta n.** 2921 **del** 24/01/2024

Oggetto:

Utilizzo dei servizi predisposti da Whistleblowing Solutions Impresa Sociale s.r.l. Designazione del responsabile del trattamento ai sensi dell'art 28 del GDPR e approvazione della documentazione in tema di protezione dati

Proponente:

Estensore	COLETTI MARIA CHIARA	_____*firma elettronica*_____
Responsabile del procedimento	COLETTI MARIA CHIARA	_____*firma elettronica*_____
Responsabile dell' Area		_____
Responsabile	M.C. COLETTI	_____*firma digitale*_____

Firma di Concerto

Richiesta di pubblicazione sul BUR: SI

OGGETTO: utilizzo dei servizi predisposti da Whistleblowing Solutions Impresa Sociale s.r.l. Designazione del responsabile del trattamento ai sensi dell'art 28 del GDPR e approvazione della documentazione in tema di protezione dati.

IL RESPONSABILE DELLA PREVENZIONE DELLA CORRUZIONE E DELLA TRASPARENZA

VISTO lo Statuto della Regione Lazio;

VISTA la Legge regionale 18 febbraio 2002, n. 6 e s.m.i. concernente: "Disciplina del sistema organizzativo della Giunta e del Consiglio e disposizioni relative alla dirigenza e al personale regionale";

VISTO il Regolamento regionale 6 settembre 2002, n. 1 e s.m.i. "Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale";

VISTA la Legge 6 novembre 2012, n. 190 e s.m.i. avente ad oggetto "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione";

VISTO il Piano Nazionale Anticorruzione (P.N.A), approvato con delibera 11 settembre 2013, n. 72 e i suoi successivi aggiornamenti;

VISTO il Decreto Legge 24 giugno 2014, n. 90 coordinato con la legge di conversione 11 agosto 2014, n. 114 recante "Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari" ed, in particolare, l'art. 19, comma 15, il quale stabilisce che "Le funzioni del Dipartimento della funzione pubblica della Presidenza del Consiglio dei Ministri in materia di trasparenza e prevenzione della corruzione di cui all'art. 1, commi 4, 5 e 8, della legge 6 novembre 2012 n. 190, e le funzioni di cui all'art. 48 del decreto legislativo 14 marzo 2013, n. 33, sono trasferite all'Autorità nazionale anticorruzione";

CONSIDERATO che in linea con le indicazioni contenute nella Determinazione n. 6 del 28 aprile 2015 - ANAC "Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower)", l'Amministrazione si è dotata di un sistema informatico per la segnalazione criptata di illeciti da parte dei dipendenti della Giunta regionale il cui link è stato pubblicato sulla pagina intranet regionale, unitamente alla procedura esplicativa;

VISTO il D.Lgs. 25 maggio 2016, n. 97 «Recante revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche»;

VISTA la Deliberazione della Giunta regionale n. 455 del 25 luglio 2017 avente ad oggetto "Modifica della Deliberazione della Giunta Regionale del 14 febbraio 2017, n. 58 concernente "Adozione del Piano Triennale di Prevenzione della Corruzione per gli anni 2017-2019" con la quale si è stabilito di introdurre un sistema di segnalazione di illeciti per le seguenti categorie di soggetti: consulenti e collaboratori della Giunta regionale; imprese fornitrici di beni o servizi e che realizzano opere in favore della Giunta regionale; dipendenti delle società in house che prestano servizio presso le strutture della Giunta Regionale; imprese partecipanti a procedure di gara per lavori, servizi e forniture; persone giuridiche e liberi professionisti destinatari di provvedimenti di

autorizzazione e concessione, garantendo a tali soggetti misure di tutela della riservatezza analoghe a quelle previste per i dipendenti e demandando al Responsabile della Prevenzione della Corruzione di "porre in essere gli atti necessari e conseguenti all'adozione della presente deliberazione";

VISTA altresì la Legge n. 179 del 30 novembre 2017 "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato" che ha, tra l'altro, modificato l'art. 54-bis del decreto legislativo 30 marzo 2001, n. 165 ampliando l'ambito soggettivo di applicazione della norma estendendolo anche ai lavoratori e ai collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica;

VISTA la Determinazione n. F00002 del 3 giugno 2022 con la quale sono state estese le tutele previste dall'art. 54-bis del d.lgs. 165/2001, come modificato dall'art. 1 della L. 179/2017;

VISTA la Deliberazione della Giunta regionale n. 42 del 31 gennaio 2023 concernente "adozione del Piano Integrato di Attività e Organizzazione (PIAO) 2023 - 2025 ai sensi dell'art. 6 del decreto-legge 9 giugno 2021, n. 80, convertito, con modificazioni, dalla legge 6 agosto 2021, n. 113";

VISTA la Determinazione n. F00002 del 13 aprile 2023 e successive modifiche e integrazioni con cui è stata adottata la Ricognizione dei processi della Regione Lazio per il triennio 2023-2025;

VISTA la Delibera dell'Autorità Nazionale Anticorruzione n. 311 del 12 luglio 2023 concernente "*Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali – procedure per la presentazione e gestione delle segnalazioni esterne*";

VISTA la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione;

VISTO il Decreto Legislativo 10 marzo 2023, n. 24 recante "Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali";

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

VISTO il decreto legislativo 30 giugno 2003, n. 196 «*Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*», e successive modifiche;

VISTO il decreto legislativo 23 giugno 2011, n. 118, recante: "Disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli enti locali e dei loro organismi, a norma degli articoli 1 e 2 della legge 5 maggio 2009, n. 42" e relativi principi applicativi, come modificato dal decreto legislativo 10 agosto 2014, n. 126;

VISTA la legge regionale 12 agosto 2020, n. 11, recante: "Legge di contabilità regionale";

VISTO il regolamento regionale 9 novembre 2017, n. 26, recante: "Regolamento regionale di contabilità" che, ai sensi dell'articolo 56, comma 2, della l.r. n. 11/2020, fino alla data di entrata in vigore del regolamento di contabilità di cui all'articolo 55 della citata l.r. n. 11/2020, continua ad applicarsi il r.r. n. 26/2017, in quanto compatibile con le disposizioni di cui alla medesima l.r. n. 11/2020;

VISTA la Legge Regionale del 29.12.2023 n.23 recante "Legge di Stabilità Regionale 2024";

VISTA la Legge Regionale del 29.12.2023 n. 24 recante "Bilancio di previsione finanziario della Regione Lazio 2024-2026";

VISTA la deliberazione della Giunta regionale 28 dicembre 2023 n. 980 concernente: "Bilancio di previsione finanziario della Regione Lazio 2024-2026. Approvazione del "Documento tecnico di accompagnamento", ripartito in titoli, tipologie e categorie per le entrate e in missioni, programmi, titoli e macroaggregati per le spese";

VISTA la deliberazione della Giunta regionale 28 dicembre 2023 n. 981, concernente: "Bilancio di previsione finanziario della Regione Lazio 2024-2026. Approvazione del "Bilancio finanziario gestionale", ripartito in capitoli di entrata e di spesa e assegnazione delle risorse finanziarie ai dirigenti titolari dei centri di responsabilità amministrativa";

VISTA la Deliberazione della Giunta Regionale del 4 marzo 2021, n. 115 con la quale è stata nominata Responsabile della Prevenzione della Corruzione e della Trasparenza della Giunta regionale del Lazio la Dott.ssa Maria Chiara Coletti, dirigente di ruolo della Giunta regionale del Lazio;

VISTA la Deliberazione della Giunta Regionale n. 34 del 18 gennaio 2024 con cui è stata approvata la procedura per la presentazione e la gestione delle segnalazioni di illeciti, stabilendo di adottare la piattaforma informatica fornita dalla Whistleblowing Solutions Impresa Sociale S.r.l. e demandando al RPCT la predisposizione degli atti consequenziali e necessari alla operatività della piattaforma;

VISTO l'accordo in merito al trattamento dei dati personali sottoscritto tra la Regione Lazio e Whistleblowing Solutions I.S. S.r.l.;

VISTE le Determinazioni n. F00001, n.F00002 e n.F00003 del 24.01.2024 con le quali sono stati individuati i soggetti incaricati del trattamento dei dati ai sensi dell'articolo 474, comma 5, del r.r. 6 settembre 2002, n. 1 e successive modificazioni e degli articoli 28, paragrafo 3, lett. b), 29 e 32, paragrafo 4, del Regolamento UE 2016/679 (RGPD);

CONSIDERATO che occorre procedere alla designazione del Responsabile del trattamento dei dati ai sensi dell'art. 28 del GDPR nonché all'approvazione dei modelli di Informativa privacy, Registro dei trattamenti e DPIA;

DETERMINA

- di designare Responsabile del trattamento dei dati in relazione alle operazioni di trattamento Dati Personali poste in essere nell'ambito della fornitura del servizio di whistleblowing digitale la Whistleblowing Solutions I.S. S.r.l., come da Accordo sottoscritto in data 23 gennaio 2024, che costituisce parte integrante e sostanziale del presente atto;
- di approvare i seguenti modelli:

a) Informativa privacy
b) Registro dei trattamenti;
c) DPIA.

Avverso il presente provvedimento è ammesso ricorso giurisdizionale innanzi al Tribunale Amministrativo del Lazio nel termine di 30 (trenta) giorni dalla sua pubblicazione.

IL RESPONSABILE DELLA PREVENZIONE
DELLA CORRUZIONE E DELLA TRASPARENZA
MARIA CHIARA COLETTI

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI
SEGNALAZIONE DI ILLECITI

Versione 2023-dicembre

Si descrivono, di seguito, le modalità e le finalità di trattamento dei dati personali degli utenti che accedono e usufruiscono della piattaforma di segnalazione di illeciti.

Sono rispettati i principi di correttezza, liceità, trasparenza e riservatezza e le disposizioni europee e nazionali in materia di protezione dei dati personali di cui al Regolamento (UE) 2016/679 (di seguito Regolamento o RGPD) e al Decreto legislativo 30 giugno 2003, n. 196 in versione vigente (c.d. Codice in materia di protezione dei dati personali) il cui obiettivo è quello di proteggere i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
Tale servizio, messo a disposizione dalla Regione Lazio, è accessibile da Amministrazione Trasparente, sotto-sezione Dati ulteriori

INFORMATIVA AI SENSI DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI (UE) 2016/679 ("RGPD").

La presente informativa è resa ai sensi dell'articolo 13 del RGPD

TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

Per le finalità istituzionali connesse alla gestione del sistema di whistleblowing il Titolare del trattamento è la Regione Lazio, con sede in Via Rosa Raimondi Garibaldi 7, 00145 Roma, contattabile via PEC all'indirizzo protocollo@regione.lazio.legalmail.it o telefonando al centralino allo 06.51681.

RESPONSABILE DELLA PROTEZIONE DATI PERSONALI

La Regione Lazio ha individuato un Responsabile della Protezione dei Dati, che è contattabile via PEC all'indirizzo DPO@regione.lazio.legalmail.it o attraverso la e-mail istituzionale: dpo@regione.lazio.it o presso URP-NUR 06-99500.

CATEGORIE DI DATI PERSONALI TRATTATI

La piattaforma di default richiede la compilazione dei seguenti dati: Nome, Cognome, Ruolo, Telefono, Email di ruolo dell'utente che effettua la registrazione e i dati relativi all'ente (nome, indirizzo, CF e PI)

ALTRI DATI TRATTATI: dati particolari; giudiziari

FINALITÀ E BASE GIURIDICA

Finalità	Base giuridica
I dati raccolti sono utilizzati esclusivamente ai fini della gestione della segnalazione di illecito	D.LGS.24/2023 (art. 12, co. 3, 4 e 7, art. 13 del d.lgs. n. 24/2023 in combinato disposto con l'art. 10 RGDP); RGDP 679/2016 (Art 6, par. 1 lett. c); art. 9, par. 2, lett. b), f) e g), art. 10)

PERIODO DI CONSERVAZIONE

Salva la necessità di conservazione ulteriore in caso di contenzioso legale ed esigenze difensive, i dati trattati sono conservati: i dati saranno conservati per il tempo necessario al trattamento della specifica segnalazione (12 mesi, prorogabili) e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

	**DESTINATARI** I dati trattati verranno comunicati alla società Whistleblowing Solutions nominata responsabile del trattamento ai sensi dell'art. 28 del Regolamento, nonché agli ulteriori responsabili e sub-responsabili eventualmente nominati. I dati potranno essere comunicati a terzi esclusivamente in adempimento di eventuali obblighi di legge e non verranno in alcun modo diffusi.
	**LUOGO E MODALITÀ DI TRATTAMENTO DEI DATI PERSONALI** I dati personali saranno trattati con strumenti cartacei e informatici e con altri mezzi all'interno dello Spazio Economico Europeo.
	**DIRITTI DEGLI INTERESSATI** La persona coinvolta o la persona menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione non possono esercitare i diritti che normalmente il Regolamento (UE) 2016/679 riconosce agli interessati (il diritto di accesso ai dati personali, il diritto a rettificarli, il diritto di ottenerne la cancellazione o cosiddetto diritto all'oblio, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati personali e quello di opposizione al trattamento)
	**RECLAMI** Al soggetto segnalato o alla persona menzionata nella segnalazione è preclusa anche la possibilità, laddove ritengano che il trattamento che li riguarda violi suddetti diritti, di rivolgersi al titolare del trattamento e, in assenza di risposta da parte di quest'ultimo, di proporre reclamo al Garante della protezione dei dati personali

FINE INFORMATIVA
LA REGIONE LAZIO LA RINGRAZIA DELLA CONSULTAZIONE

Dati trattamento	Legenda	Esempi	Trattamento Dati Segnalazione n._/202_
Denominazione trattamento	individuare e indicare il trattamento dei dati personali specifico.		segnalazione di Whistleblowing
Descrizione trattamento	Il trattamento deve essere descritto e deve essere esplicitamente indicato se è su larga scala.	fare riferimento ai seguenti fattori: - il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; - il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; - la durata, ovvero la persistenza, dell'attività di trattamento; - la portata geografica dell'attività di trattamento. Esempi di trattamento su larga scala: - trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività; - trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio). - Esempi di trattamento da non ritenersi su larga scala: - trattamenti di dati relativi a pazienti svolti da singoli professionisti sanitari; - trattamenti di dati personali relativi a condanne penali e reati svolti da singoli avvocati.	Attraverso la compilazione di un questionario guidato il segnalante (whistleblower) ha la possibilità di denunciare un illecito. Oggetto di segnalazione sono le informazioni sulle violazioni di normative nazionali e dell'Unione Europea. La segnalazione deve riguardare condotte illecite, cioè fatti illeciti e/o irregolarità (comportamenti, atti od omissioni) commessi ai danni dell'interesse pubblico o dell'integrità dell'amministrazione pubblica verificatisi all'interno dell'Amministrazione regionale di cui il segnalante sia venuto a conoscenza in ragione del proprio rapporto di lavoro, cioè in occasione e/o a causa ed in costanza dello svolgimento della propria attività professionale-lavorativa. Non si tratta di un trattamento su larga scala.
Finalità	Finalità perseguite dal trattamento		I dati raccolti sono utilizzati esclusivamente ai fini della gestione della segnalazione di illecito. L'interessato acconsente al trattamento dei propri dati personali per una finalità specifica ed esplicita.
Base giuridica e fonte normativa	La base giuridica deve essere individuata tra le condizioni di liceità previste nell'art. 6 del RGPD. Qualora il trattamento riguardi "categorie particolari di dati", l'individuazione della base giuridica deve essere effettuata riferendosi ai casi indicati all'art. 9, par. 2 del RGPD. Qualora il trattamento riguardi "dati relativi a condanne penali e reati" la base giuridica è costituita da specifica normativa dell'Unione o degli Stati membri che preveda idonee garanzie per i diritti e le libertà degli interessati e solo sotto il controllo dell'autorità pubblica (art. 10 del RGPD).		D.Lgs.24/2023: art. 12, co. 3, 4 e 7, art. 13 RGDP 679/2016: art. 6, par. 1 lett. c), art. 9, par. 2, lett. b), f) e g), art. 10 norma che prevede esplicitamente il trattamento: art. 13 del D.Lgs. n. 24/2023 in combinato disposto con l'art. 10 RGDP

Categoria di interessato	categorie di persone fisiche i cui dati sono oggetto del trattamento (es. dipendenti, fornitori, pazienti, ecc.). L'interessato è il destinatario finale dei diritti e delle tutele predisposte dal RGPD (artt. 13 e ss) azionabili nel caso in cui il trattamento dei dati personali sia stato realizzato in violazione delle disposizioni del Regolamento.		- dipendenti della Giunta regionale; - consulenti e collaboratori della Giunta regionale; - lavoratori autonomi che svolgono la propria attività lavorativa presso la Giunta regionale; - lavoratori o collaboratori che svolgono la propria attività lavorativa presso la Giunta regionale che forniscono beni o servizi o che realizzano opere in favore di terzi; - liberi professionisti che prestano la propria attività presso la Giunta regionale; - volontari e tirocinanti che prestano la propria attività presso la Giunta regionale; - persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso la Giunta regionale; - facilitatore; - la persona coinvolta e la persona menzionata nella segnalazione
Categoria del dato	tutte le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni su caratteristiche, abitudini, stile di vita, relazioni personali, stato di salute o situazione economica. In questa sezione va specificato il dato personale trattato. Per ogni dato trattato deve essere indicata la base giuridica che rende lecito il trattamento	Dati anagrafici (nome e cognome) o immagini che permettono l'identificazione diretta dell'interessato; - Numeri di identificazione (codice fiscale, indirizzo IP, numero di targa ecc.) che permettono l'identificazione indiretta dell'interessato. - Dati particolari (art. 9 RGPD) ossia i dati che possono rilevare l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale o i dati relativi alla salute, alla vita sessuale o i dati bioemetrici e genetici. - Dati relativi a condanne penali e reati (art. 10 RGPD) ossia i dati che possono rivelare l'esistenza di provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (es. provvedimenti penali di condanna definitivi, liberazione condizionale, divieto od obbligo di soggiorno, misure alternative alla detenzione) o la qualità di imputato o di indagato dell'interessato. - Dati di geolocalizzazione che possono fornire informazioni sui luoghi frequentati e sugli spostamenti.	Per la registrazione e attivazione del servizio sono richiesti unicamente i seguenti dati: Nome, Cognome, Ruolo, Telefono, Email di ruolo dell'utente che effettua la registrazione e i dati relativi all'ente (nome, indirizzo, CF e PI). EVENTUALI ALTRI DATI TRATTATI: dati particolari; giudiziari (art. 12, co. 3, 4 e 7, d.lgs. n. 24/2023)
Trasferimento all'estero dei dati **(Trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale) (solo se ricorre la fattispecie).**	Qualora non si proceda a trasferimento verso paesi terzi la relativa sezione del Registro dei Trattamenti può essere valorizzata con "no". Qualora ricorrano le condizioni e le garanzie del trasferimento ai sensi degli artt. 45, 46, 47 e 49 del RGDP in questa sezione dovranno essere identificati il paese terzo o l'Organizzazione Internazionale. Nel residuale caso in cui non sia possibile basare il trasferimento sulle disposizioni richiamate, vedi colonna esempi.	Nel residuale caso in cui non sia possibile basare il trasferimento sulle disposizioni richiamate il trasferimento è ammesso soltanto se: - non è ripetitivo; - riguarda un numero limitato di interessati; - è necessario per il perseguimento degli interessi legittimi cogenti del Titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e previa valutazione da parte del Titolare delle circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate alla protezione dei dati personali. In questo caso grava sul Titolare l'obbligo di informare l'autorità di controllo, di fornire le informazioni di cui agli artt. 13 e 14 RGPD e di informare l'interessato del trasferimento e degli interessi legittimi perseguiti	I Dati Personali sono trattati principalmente in Italia ed esclusivamente nei Paesi dell'Unione Europea. Non esiste alcun trasferimento di Dati Personali verso l'estero in paesi extra UE.

Termine di cancellazione dati (Periodo di conservazione)	termini ultimi previsti per la cancellazione delle diverse categorie di dati. Per stabilire i tempi di conservazione del dato si può fare riferimento a leggi, regolamenti, manuali di conservazione e scarto, normative di settore o policy di data retention ove presenti.	Esempio: in caso di rapporto contrattuale, i dati relativi saranno conservati per la durata di 10 anni dall'ultima registrazione, come previsto dall'art. 2220 del codice civile.	Policy di data retention di default delle segnalazioni di 12 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute. La proroga della scadenza può essere fatta dal soggetto ricevente più volte (per un massimo di 5 anni). Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio, a condizione che non esistano segnalazioni aperte sulla piattaforma.
Modalità del trattamento	Nome delle applicazioni software/sistemi utilizzate a supporto del trattamento e indicazione di eventuali archivi cartacei		I dati personali saranno trattati con strumenti cartacei e informatici (piattaforma di Whistleblowing) e con altri mezzi all'interno dello Spazio Economico Europeo. I dati inseriti dal segnalante, inoltre, non sono visibili nell'immediato nella piattaforma. Tutti i soggetti coinvolti nel trattamento dei dati hanno ricevuto opportune istruzioni.
Destinatari dei dati	Si tratta di categorie di destinatari a cui i dati personali sono o saranno comunicati. L'art. 4 punto 9 del RGPD definisce il destinatario del dato nella persona fisica o giuridica, nell'autorità pubblica, nel servizio o in un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Nella categoria di "terzo" rientrano la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo diversi dall'interessato, dal Titolare del trattamento, dal Responsabile del trattamento o dalle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile.	Esempio: Contitolari, Responsabili, Altre Pubbliche Amministrazioni, Enti previdenziali ecc.	RPCT; Istruttore; Altri destinatari eventuali a seconda del contenuto della segnalazione: - Altre strutture interne; - Organi esterni competenti: a titolo esemplificativo, Guardia di Finanza, Direzione Provinciale del Lavoro, Comando Vigili Urbani, Agenzia delle Entrate, Procura della Repubblica

Responsabile/i del trattamento	Il Responsabile del trattamento (art. 4 par. 1 n. 8 e art. 28 del RGPD) è individuato nella persona fisica o giuridica, nell'autorità pubblica, nel servizio o altro organismo, al quale è affidato il trattamento dei dati personali di competenza regionale dal Titolare del trattamento, che presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del RGPD e garantisca la tutela dei diritti dell'interessato. Il Titolare del trattamento disciplina i trattamenti affidati al Responsabile, i compiti e le istruzioni con specifico atto negoziale di incarico secondo lo schema "G" dell'allegato "NN" del Regolamento Regionale n. 1/2002.		I dati trattati verranno comunicati alla società Whistleblowing Solutions nominata responsabile del trattamento ai sensi dell'art. 28 del Regolamento, nonché agli ulteriori responsabili e sub-responsabili eventualmente nominati
Altro Responsabile	L'Altro Responsabile del trattamento (o sub-responsabile) è nominato dal Responsabile del trattamento previa autorizzazione del Titolare. L'autorizzazione può essere contenuta nel contratto di nomina del Responsabile del Trattamento sottoscritta dal Titolare. Svolge le proprie attività nel rispetto delle medesime istruzioni impartite dal Titolare al Responsabile di trattamento.		I dati trattati verranno comunicati alla società Seeweb e alla Società Transparency International Italia nominate sub-responsabili del trattamento ai sensi dell'art. 28 del Regolamento, nonché agli ulteriori responsabili e sub-responsabili eventualmente nominati
Amministratori di Sistema	L'Amministratore di sistema può essere un soggetto esterno individuato con atto di nomina da parte del Responsabile del Trattamento o interno individuato con atto di nomina del soggetto designato tra i soggetti della propria struttura, che per esperienza, capacità tecniche ed affidabilità forniscano idonea garanzia del pieno rispetto delle disposizioni di legge vigenti in materia, ivi compreso il profilo relativo alla sicurezza. L'atto di nomina contiene l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. L'amministratore di sistema sovrintende alle risorse del sistema informativo afferenti alla struttura di appartenenza. Amministratori di sistema esterni - art. 3 dello schema "G" dell'allegato "NN" Amministratori di sistema interni - Art. 474 nonies "Amministratori di sistema		Le attività di Amministratore di Sistema sono svolte dal personale della Società Whistleblowing Solutions alla quale la Giunta Regionale del Lazio ha affidato la gestione e la manutenzione del Sistema Informativo (come da atto di nomina ai sensi dell'art. 28 del RGPD)
Contitolari del trattamento	Eventuali soggetti contitolari		NO

Misure di sicurezza tecnica e organizzative	Tutte le misure tecniche ed organizzative applicate al trattamento per ridurre i rischi derivanti dal trattamento dei dati personali (art. 32 del RGPD). La determinazione delle misure da applicare e la valutazione finale relativa al livello di sicurezza adeguato ai rischi presentati dalle attività di trattamento è rimessa al Titolare. L'elenco delle misure contenuto nell'art. 32 RGPD costituisce una lista aperta e non esaustiva. Devono essere indicate in maniera sintetica, ma idonea a fornire un quadro generale delle misure adottate in relazione alle attività di trattamento svolte; pertanto, le misure devono essere adeguate e proporzionate al livello di rischio connesso al trattamento dei dati personali. È ammesso il rinvio e/o il richiamo ad altri documenti quali procedure organizzative interne, security policy, etc.	Esempi: Rientrano nelle misure di sicurezza tecniche quelle che garantiscono la protezione e la corretta conservazione dei dati (es. la cifratura dei dati e pseudonimizzazione). Rientrano nelle misure di sicurezza organizzative tutte le azioni poste in essere per assicurare l'applicazione del RGPD quali: adozione di procedure interne relative alla gestione del sistema di protezione dati (data breach, valutazione dei rischi, policy di data retention, codici di condotta, nomine degli ADS ecc.).	cifratura dei dati, pseudonimizzazione, backup periodici, tracciabilità (l'applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema. I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent). Quanto indicato è specificato nel dettaglio nella documentazione prodotta dal fornitore. accesso con nome e password, antivirus, aggiornamento dei sistemi operativi, inaccessibilità del pc, vigilanza, tornelli, stanze chiuse a chiave Il personale che svolge i trattamenti è stato appositamente autorizzato ed istruito (atto di nomina dei soggetti incaricati e corso di formazione svolto su piattaforma EduLazio organizzato dalla Regione)

REGIONE LAZIO

Strumento di calcolo per la valutazione dei rischi connessi alle attività di trattamento e valutazione d'impatto sulla protezione dei dati

Strumento di calcolo per la valutazione dei rischi connessi alle attività di trattamento e valutazione d'impatto sulla protezione dei dati

Redatto da	Tania Alivernini
Approvato da	Andrea Corbelli
in data	26/04/2023
Versione	**1.0**
Descrizione	Prima versione
Riservatezza	Documento riservato a Titolare, DPO e Direzione competente.

Scopo del Documento	Il presente documento costituisce uno strumento operativo per lo svolgimento documentato della valutazione dei rischi connessi al trattamento e della valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 del Reg. UE 679/2016.

REGIONE LAZIO

Indice

Indice
Di seguito l'indice dello strumento di analisi dei rischi e valutazione preliminare del trattamento utilizzato da Regione Lazio

REGIONE LAZIO

Istruzioni per l'utilizzo

Istruzioni Generali di compilazione

Al fine di effettuare la valutazione del rischio:

1. Compliare il modulo "**Anagrafica Trattamento**" con le informazioni identificative del trattamento oggetto di analisi.
2. Compilare il modulo "**B.Valutazione**", per calcolare il rischio del trattamento. Per la valorizzazione dei campi utilizzare:

- il foglio "L1.Probabilità" per definire la probabilità di accadimento della minaccia rispetto al trattamento di dati personali in esame al fine di compilare la colonna "Probabilità di accadimento inerente";
- il foglio "L2.Impatto", per definire il livello di impatto della minaccia sul trattamento al fine di compilare la colonna "Livello di impatto inerente"; la determinazione dell'impatto si riferisce principalmente ai parametri di Riservatezza - Integrità - Disponibilità (R.I.D) del dato dello standard ISO 27001:2022;
- il foglio "Controlli" dal quale scegliere (dalla colonna I), per ogni singola minaccia, le ulteriori misure da applicare e da inserire nella colonna "Misure di Sicurezza", nel caso sia necessario diminuire il rischio (azione di mitigazione del rischio). Il set di misure inserite nel foglio "Controlli" è associata alle minacce definite nelle colonne da M a AA secondo criteri generali che potrebbero variare in fattispecie specifiche. Pertanto, sia le misure previste, che non sono da considerarsi esaustive, sia l'associazione della misura di sicurezza/controllo (colonna I del foglio "Controllo") alle minacce (colonne M-AA) possono essere modificate ed adattate, all'occorrenza, allo specifico trattamento in esame. Se gli ulteriori controlli applicati nella colonna "Misure di Sicurezza" diminuiscono il rischio determinato dalla specifica minaccia sarà possibile diminuire la probabilità di accadimento della minaccia compilando la colonna "Probabilità Residua" diminuendo di un solo livello la probabilità già indicata nella colonna "Probabilità di accadimento inerente" (es. da Massima a Significativa, da Significativa a Limitata, da Limitata a Trascurabile). Effettuate le operazioni descritte, nella colonna "Rischio Residuo" verrà evidenziato il nuovo valore del rischio derivante dall'applicazione delle ulteriori misure di mitigazione.

3. Verificare nel foglio "**Risultato**" l'esito dell'analisi del rischio effettuata nel foglio "B. Valutazione" . Il modulo contiene anche gli spazi destinati al parere del DPO, anche ai fini di un'eventuale consultazione all'Autorità Garante della Privacy. Il valore del rischio è dato dal prodotto tra l'impatto (I) di una determinata minaccia e la probabilità (P) che la stessa accada (R=P*I) secondo le combinazioni definite nel modulo "L3. Classificazione del rischio".
4. Compilare il modulo "**A. VP trattamento**" rispondendo alle domande del Questionario finalizzate alla valutazione preliminare del trattamento ai fini della verifica dell'obbligatorietà della DPIA.
5. Procedere con la compilazione del modulo "**DPIA**" qualora il modulo "Risultato" o l'esito del questionario nel modulo "A. VP trattamento" rilevino l'opportunità o l'obbligatorietà dello sviluppo della DPIA. Per la compilazione delle sezioni "g.,h. e i." del modulo "DPIA" possono essere utilizzati i dati già inseriti nel modulo "B.Valutazione" .

Istruzioni specifiche per la compilazione del questionario contenuto nel modulo "A. V.P. trattamento"

Il questionario è utilizzato per effettuare una valutazione preliminare del trattamento e valutare se, per lo stesso, sia obbligatorio lo svolgimento della DPIA (Valutazione di impatto sulla protezione dei dati, ex ar.35 RGPD) .

La valutazione d'impatto sulla protezione dei dati è uno strumento fondamentale per la c.d. responsabilizzazione "Accountability".
Ai fini della valutazione preliminare sull'obbligatorietà dello sviluppo della DPIA, si tiene conto della natura del trattamento, del numero di interessati coinvolti, del contesto, delle finalità, delle categorie di dati personali trattati, delle attività di trattamento, dei diritti, rischi, misure di sicurezza e degli eventuali piano di rimedio (azioni di mitigazione del rischio).

La valutazione di impatto è riferita al trattamento descritto nel modulo "Anagrafica Trattamento".

L'art. 35 del Reg. UE 2016/679 prevede la possibilità che una singola valutazione di impatto possa esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

Il Questionario predisposto si basa:

• sui 9 criteri, definiti nel WP 248 rev.01 del 4 ottobre 2017 del Gruppo di Lavoro Articolo 29 per la protezione dati: nel caso in cui un trattamento (o l'insieme di trattamenti) soddisfi due criteri si rende obbligatoria la conduzione della DPIA;

• sui 12 criteri definiti nell'allegato 1 al provvedimento n. 467 dell'11 ottobre 2018 del Garante: nel caso in cui un trattamento (o l'insieme di trattamenti) soddisfi un criterio si rende obbligatoria la conduzione della DPIA.

E' possibile che la compilazione parziale del questionario rilevi già l'obbligatorietà della DPIA. In questo caso, dato il risultato, si può procedere alla compilazione del modulo DPIA senza valorizzare tutte le risposte del questionario.
Nei casi dubbi o nei casi in cui sia presente almeno 1 criterio selezionato, anche se il questionario non rileva l'obbligatorietà dello sviluppo della DPIA occorre valutare attentamente l'impatto del trattamento sui diritti e le libertà degli interessati e l'opportunità di effettuare comunque cautelativamente la DPIA utilizzando anche il risultato della valutazione del rischio presente nel modulo "Risultato".

A.1 Anagrafica Trattamento

Titolare dei dati personali	Giunta della Regione Lazio
Indirizzo/Sede legale	Via R. Raimondi Garibaldi, 7 00145 Roma
Direzione	/
Area	Area Prevenzione della corruzione e trasparenza
Email	anticorruzione@regione.lazio.it
Domicilio digitale (PEC o altro)	anticorruzione@regione.lazio.legalmail.it
DPO	Vasile Diaconescu
Email DPO	dpo@regione.lazio.it
PEC DPO	DPO@regione.lazio.legalmail.it

ID/Codice trattamento	D80100
Denominazione Trattamento	segnalazione di Whistleblowing tramite piattaforma web

Redatto da	Maria Chiara Coletti
in data	
Versione	1

A.2 Ruoli e Responsabilità

Data di inizio	
Scadenza programmata	
Titolare del trattamento	Giunta regionale
Responsabili del trattamento	Fornitori della piattaforma
Owner del trattamento	RPCT
Funzioni coinvolte	RPCT

A.3 Descrizione dell'ambito oggetto di valutazione

(compilare i campi sotto riportati, o allegare a questo file il trattamento come estrazione dal Privacy Manager)

Descrizione del trattamento	Attraverso la compilazione di un questionario guidato il segnalante (whistleblower) ha la possibilità di denunciare un illecito
Finalità del trattamento	I dati raccolti sono utilizzati esclusivamente ai fini della gestione della segnalazione di illecito
Categorie di interessati	dipendenti della Giunta regionale; consulenti e collaboratori della Giunta regionale; lavoratori autonomi che svolgono la propria attività lavorativa presso la Giunta regionale; lavoratori o collaboratori che svolgono la propria attività lavorativa presso la Giunta regionale che forniscono beni o servizi o che realizzano opere in favore di terzi; liberi professionisti che prestano la propria attività presso la Giunta regionale; volontari e tirocinanti che prestano la propria attività presso la Giunta regionale; persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso la Giunta regionale; facilitatore; la persona coinvolta e la persona menzionata nella segnalazione
Categorie di dati trattati (comuni, particolari, giudiziari)	comuni, particolari, giudiziari
Periodo di conservazione dei dati	Policy di data retention di default delle segnalazioni di 12 mesi, prorogabili sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute. La proroga della scadenza può essere fatta dal soggetto ricevente più volte (per un massimo di 5 anni). Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio, a condizione che non esistano segnalazioni aperte sulla piattaforma.
Soggetti autorizzati al trattamento	Responsabile della prevenzione della corruzione e della trasparenza
Tipo di Trattamento	sistema informatico
Comunicazioni di dati personali a terze parti	Altre strutture interne/Organi esterni competenti
Supporti elettronici e fisici impiegati	piattaforma web
Condizione di liceità	D.Lgs.24/2023 (art. 12, co. 3, 4 e 7, art. 13) RGDP 679/2016 (art. 6, par. 1 lett. c), art. 9, par. 2, lett. b), f) e g), art. 10) norma che prevede esplicitamente il trattamento: art. 13 del D.Lgs. n. 24/2023 in combinato disposto con l'art. 10 RGDP
Limitazione delle finalità	i dati sono raccolti solo al fine di gestire e dare seguito alle segnalazioni effettuate da parte dei soggetti tutelati dal d.lgs. 24/2023
Minimizzazione dei dati	i dati raccolti devono essere adeguati, pertinenti e limitati a quanto è necessario per la finalità del trattamento
Esattezza dei dati	L'aggiornamento dei dati è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata. Non appena vengono modificati i dati di contatto all'interno della piattaforma, questi diventano i dati di contatto ufficiali a cui sono inviate le comunicazioni relative a ogni tipo di aggiornamento.
Necessarietà	i dati utilizzati sono limitati a quelli strettamente necessari rispetto allo scopo per cui gli stessi sono raccolti
Proporzionalità	sono trattati i soli dati pertinenti e non eccedenti in relazione alle finalità perseguite

A.4 In sintesi i fattori di rischio che hanno determinato la necessità della conduzione della DPIA

Criterio	Informazioni rilevanti
WP248-criterio 4)	
WP248-criterio 7)	

REGIONE LAZIO

Foglio di calcolo per la Valutazione del rischio per il trattamento

Task 1 - Identificazione delle minacce ("Minaccia" e "Esempi")

Fare riferimento alle minacce indicate nella colonna "Minaccia" aiutandosi con gli esempi (non esaustivi) presenti nella colonna "Esempi".

Task 2 - Valutazione della probabilità di accadimento ("Probabilità accadimento inerente")

Per specificare il livello di probabilità di accadimento fare riferimento al foglio *L1. Probabilità*

Task 3 - Valutazione dell'impatto ("Livello Impatto Inerente")

Per specificare l'impatto fare riferimento al foglio *L2. Impatto* contenente brevi descrizioni ed alcuni esempi.

Task 4 – Valutazione del rischio inerente ("Rischio Inerente")

Il valore della valutazione del rischio viene rilevato automaticamente come prodotto tra probabilità ed impatto secondo la matrice del foglio *L3. Classificazione Rischio*

Task 5 – Identificazione delle contromisure di sicurezza ("Misure di sicurezza", "Owner" e "Termine")

Per le attività che presentano un rischio *Medio Alto* o *Alto*, è necessario identificare ulteriori misure di sicurezza al fine di mitigare i rischi secondo le indicazioni contenute nel foglio *Istruzioni* per l'utilizzo e l'applicazione delle misure presenti nel foglio *Controlli* .
Nella colonna "Misure di sicurezza" riportare le misure, nella colonna "Owner" l'owner del trattamento che ha adottato o adotterà le misure, nella colonna "Termine" indicare se le misure risultano già adottate o in alternativa il termine entro la quale si intende adottarle (nel caso di misure pianificate).

Task 6 – Valutazione del rischio residuo ("Probabilità residua" e "Rischio Residuo")

Alla luce delle misure di mitigazione inserite nella colonna "Misure di sicurezza" rivalutare il valore della probabilità di accadimento inserendo "manualmente" nella colonna "Probabilità residua" il valore della probabilità presente in "Probabilità di accadimento inerente" diminuito di un livello (es. da Massima a Significativa, da Significativa a Limitata, da Limitata a Trascurabile). L'impatto rimane invariato.
Il nuovo valore del rischio viene visualizzato in "Rischio Residuo".

Minaccia	Esempi	Probabilità accadimento inerente *(da valorizzare in base alla matrice presente in foglio L1)*	Livello Impatto Inerente *(da valorizzare in base alla matrice presente in foglio L1)*	Rischio Inerente	Misure di sicurezza	Owner	Termine	Probabilità residua *(da valorizzare come descritto in Task 6)*	Rischio residuo
Fattore Umano	Mancanza di formazione adeguata; Violazione dell'obbligo di riservatezza; Stress; Insoddisfazione professionale.	Trascurabile	Limitato	1. Basso	Gestione delle responsabilità	RPCT	già adottate	Trascurabile	1. Basso
Inadeguatezza Organizzativa	Mancanza di policy, procedure e istruzioni operative; Non disponibilità di strumenti idonei alla conservazione e/o distruzione dei documenti cartacei; Mancato controllo sull'operato dei fornitori esterni; Mancata o inadeguata segregazione di ruoli e responsabilità; Errata assegnazione di compiti e attività; Carenza del flusso di informazioni e mancata condivisione delle stesse; Accessi non autorizzati agli edifici, uffici o alle aree di sicurezza.	Trascurabile	Significativo	2. Medio Basso	Controllo degli accessi	Regione Lazio e Laziocrea spa	già adottate	Trascurabile	2. Medio Basso
Violazione normativa	Violazione delle clausole nei contratti con soggetti terzi; Violazione delle normative vigenti.	Trascurabile	Significativo	2. Medio Basso	Gestione delle responsabilità	Regione Lazio	già adottate	Trascurabile	2. Medio Basso
Disastro naturale, colposo / doloso	Incendio; Terremoto; Esplosione; Alluvione; Atti vandalici / terroristici.	Trascurabile	Trascurabile	1. Basso	Backup delle informazioni	Regione Lazio e Laziocrea spa	già adottate	Trascurabile	1. Basso
Attacchi informatici	Cracking delle credenziali di accesso; Tecniche di ingegneria sociale (furto di credenziali con mail di phishing, spear phishing); Hacking; Violazioni rilevate da parte delle soluzioni tecnologiche.	Limitata	Limitato	2. Medio Basso	Uso della crittografia	RPCT	già adottate	Trascurabile	1. Basso
Abuso di privilegi di accesso	Esecuzione di operazioni abusando dei privilegi sui sistemi informatici; Furto d'identità; Modifica non autorizzata delle abilitazioni di accesso; Violazione del sistema di autenticazione.	Limitata	Significativo	3. Medio Alto	Logging	Fornitore e Laziocrea	già adottate	Trascurabile	2. Medio Basso
Utilizzo o modifica non autorizzato dei dati	Modifica non autorizzata alle base dati o sugli archivi; Lettura e copia non autorizzata alle basi dati o sugli archivi; Divulgazione non autorizzata alle basi dati o sugli archivi	Trascurabile	Significativo	2. Medio Basso	Protezione dei log	Fornitore e Laziocrea	già adottate	Trascurabile	2. Medio Basso
Errori nei processi di elaborazione dei dati	Errata correlazione dei dati; Errata trasformazione dei dati; Errore di data entry.	Trascurabile	Limitato	1. Basso	Termini e condizioni d'impiego	RPCT	già adottate	Trascurabile	1. Basso
Inefficiente gestione del dato	Errata classificazione dei dati in termini di tipologia, posizione, livelli di accesso o protezione.	Trascurabile	Trascurabile	1. Basso	Termini e condizioni d'impiego	RPCT	già adottate	Trascurabile	1. Basso
Perdita integrità per guasto HW	Perdita integrità delle basi dati; Procedure di verifica dei dati archiviati non efficienti; Errori nelle procedure di ripristino dei dati.	Trascurabile	Limitato	1. Basso	Gestione delle configurazioni	Fornitore e Laziocrea	già adottate	Trascurabile	1. Basso
Interrogazioni improprie su base dati	Esecuzione di interrogazioni massive o non autorizzate; Accesso non autorizzato ai sistemi o alle librerie di backup.	Trascurabile	Trascurabile	1. Basso	Analisi dei log	Fornitore e Laziocrea	già adottate	Trascurabile	1. Basso
Perdita / furto di asset IT	Perdita / furto di dispositivi, di memorie di massa e documenti; Perdita / furto di dispositivi fissi e mobili; Perdita / furto di documentazione tecnica.	Trascurabile	Trascurabile	1. Basso	Sicurezza delle reti	Fornitore e Laziocrea	già adottate	Trascurabile	1. Basso
Utilizzo improprio di software o servizi	Divulgazioni di dati a terze parti; Utilizzo improprio della posta elettronica; Installazione di software non autorizzato; Esistenza di software e servizi non sottoposti alle misure organizzative e di sicurezza aziendali.	Trascurabile	Limitato	1. Basso	Sensibilizzazione, educazione e formazione alla sicurezza delle informazioni	Regione Lazio e Laziocrea spa	già adottate	Trascurabile	1. Basso
Perdita disponibilità per guasto HW	Guasti dei sistemi di storage; Perdita delle chiavi di crittografia dei dati; Errori nella manutenzione dell'HW; Guasti ai sistemi di backup che producono la perdita dei dati.	Trascurabile	Limitato	1. Basso	Gestione delle chiavi crittografiche	Responsabili del Trattamento	già adottate	Trascurabile	1. Basso
Cancellazione volontaria o accidentale dei dati	Errata cancellazione di dati su dispositivi; Cancellazione o cifratura malevola dei dati	Trascurabile	Limitato	1. Basso	Backup delle informazioni	Fornitore e Laziocrea	già adottate	Trascurabile	1. Basso

REGIONE LAZIO

Probabilità di accadimento della minaccia

Valore	Probabilità
Trascurabile	Improbabile che la minaccia si verifichi nell'arco temporale di 2 anni o oltre (casi isolati, non prevedibili)
Limitata	Probabilità ridotta che la minaccia si verifichi nell'arco temporale di 2 anni (nell'ordine di una volta all'anno)
Significativa	Significativa probabilità che la minaccia si verifichi nell'arco temporale di 2 anni (nell'ordine di più di una volta all'anno)
Massima	Elevata probabilità che la minaccia si verifichi nell'arco temporale di 2 anni (nell'ordine di almeno una volta al mese)

REGIONE LAZIO

Livello di impatto

Valore	Descrizione	Esempi di impatto
Trascurabile	Impatto trascurabile, che non incide significativamente sui diritti e le libertà degli interessati	- Perdita di tempo nel ripetere le formalità o attendere che siano soddisfatte - Ricezione di messaggi di posta elettronica non richiesti (ad esempio messaggi di spam) - Riutilizzo di dati pubblicati su siti Web a scopo di pubblicità mirata (informazioni ai social network, riutilizzo per la spedizione su carta) - Pubblicità mirata per prodotti di consumo comuni - Semplice fastidio causato da informazioni ricevute o richieste - Paura di perdere il controllo sui propri dati - Sensazione di violazione della privacy senza danno reale o oggettivo (ad esempio intrusione commerciale) - Perdita di tempo nella configurazione dei dati - Mancanza di rispetto per la libertà di navigazione online a causa della negazione dell'accesso a un sito commerciale (ad esempio proibito l'accesso a siti di vendita sostenze alcoliche a causa dell'età sbagliata)
Limitato	Impatto poco rilevante che, se non opportunamente gestito, può incidere sui diritti e le libertà degli interessati	- Pagamenti inattesi (ad esempio multe inflitte in modo errato), costi aggiuntivi (ad es. spese bancarie, spese legali), inadempienza dei pagamenti - Negazione dell'accesso a servizi amministrativi o servizi commerciali - Perdita opportunità di comfort (ad es. cancellazione di tempo libero, acquisti, ferie, chiusura di un conto online) - Account di servizi online bloccati (ad es. giochi, amministrazione) - Ricezione di articoli di posta indesiderata mirati che potrebbero danneggiare la reputazione degli interessati - Aumento dei costi (ad es. aumento dei prezzi assicurativi) - Dati non aggiornati (ad esempio, posizione precedentemente detenuta) - Elaborazione di dati errati che creano, ad esempio, malfunzionamenti delle utenze (banca, clienti, organizzazioni sociali, ecc.) - Pubblicità online mirata su un aspetto privato che l'individuo desidera mantenere riservato (ad esempio pubblicità in gravidanza, trattamento farmacologico) - Profilazione imprecisa o inappropriata - Rifiuto di continuare a utilizzare i sistemi di informazione (whistleblowing, social network) - Disturbi psicologici di entità minore ma oggettiva (diffamazione, reputazione) - Problemi nelle relazioni personali o professionali (ad esempio immagine, reputazione offuscata, perdita di riconoscimento) - Sensazione di violazione della privacy senza danni irreversibili - Intimidazione sui social network
Significativo	Impatto rilevante che, se non opportunamente gestito, può dar luogo a indebite lesioni o rilevanti limitazioni all'esercizio dei diritti e delle libertà degli interessati	- Appropriazione indebita di denaro non risarcita - Difficoltà finanziarie non temporanee (ad es. obbligo di prendere un prestito) - Perdita di opportunità mirate, uniche e non ricorrenti (ad esempio mutuo per la casa, rifiuto di studi, stage o lavoro, divieto di esame) - Divieto di detenere conti bancari - Danno alla proprietà - Perdita finanziaria a seguito di una frode (ad esempio dopo un tentativo di phishing) - Perdita di dati dei clienti - Disturbi psicologici gravi (ad es. depressione, sviluppo di una fobia) - Sensazione di violazione della privacy con danni irreversibili - Sensazione di vulnerabilità dopo una citazione in tribunale - Senso di violazione dei diritti fondamentali (ad esempio discriminazione, libertà di espressione) - Vittima di ricatti - Cyberbullismo e molestie
Massimo	Impatto molto rilevante che, se non opportunamente e tempestivamente gestito, può causare danni particolarmente gravosi o addirittura irreversibili ai diritti e alle libertà degli interessati coinvolti	- Rischi finanziari - Debiti sostanziali - Incapacità di lavorare - Incapacità di trasferirsi - Perdita di abitazioni - Perdita di lavoro - Perdita di prove nel contesto del contenzioso - Perdita di accesso a infrastrutture vitali (acqua, elettricità) - Disturbi psicologici a lungo termine o permanenti - Condanne penali - Rapimenti - Perdita dei legami familiari - Inabilità a citare in giudizio - Modifica dello stato amministrativo e / o perdita dell'autonomia legale (tutela)

Controlli ISO 27001:2022										Minacce														
ID Ambito	Categoria Misura	ID Misura di sicurezza	Misura di sicurezza	Tipologia di controllo	Proprietà dell'informazione	Capacità operative	Domini di sicurezza	Descrizione del Controllo	controllo applicato	Fattore Umano	Inadeguatezza Organizzativa	Violazione normativa	Disastro naturale, colposo / doloso	Attacchi informatici	Abuso di privilegi di accesso	Utilizzo o modifica non autorizzato dei dati	Errori nei processi di elaborazione dei dati	Inefficiente gestione dei dati	Perdita integrità per guasto HW	Interrogazioni improprie su base dati	Perdita / furto di asset IT	Utilizzo improprio di software o servizi	Perdita disponibilità per guasto HW	Cancellazione volontaria o accidentale dei dati
5	Controlli organizzativi	5.1	Politiche per la sicurezza delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Governance	Governance and Ecosystem Resilience	L'organizzazione definisce le politiche del sistema di gestione che sono approvate dalla direzione, pubblicate sulla intranet aziendale, comunicate al personale e alle terze parti rilevanti, riesaminate a intervalli regolari e in caso di cambiamenti significativi.		Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì	Sì
5	Controlli organizzativi	5.1	Politiche per la sicurezza delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Governance	Governance and Ecosystem Resilience	Le politiche del sistema di gestione prendono in considerazione requisiti che derivano dalle linee strategiche dell'Ente, dai regolamenti, da legislazione vigente e accordi contrattuali, dai rischi e dalle minacce di sicurezza in continua evoluzione.		Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì	Sì
5	Controlli organizzativi	5.1	Politiche per la sicurezza delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Governance	Governance and Ecosystem Resilience	L'organizzazione si impegna a soddisfare i requisiti e il miglioramento continuo del sistema di gestione.		Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì	Sì
5	Controlli organizzativi	5.1	Politiche per la sicurezza delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Governance	Governance and Ecosystem Resilience	L'organizzazione definisce un processo per il trattamento delle eccezioni.		Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì	Sì
5	Controlli organizzativi	5.2	Ruoli e responsabilità per la sicurezza informatica	Preventivo	Riservatezza Integrità Disponibilità	Governance	Governance and Ecosystem Protection Resilience	L'organizzazione definisce i ruoli e le responsabilità del sistema di gestione in accordo con le necessità dell'Ente.		Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì
5	Controlli organizzativi	5.3	Segregation of duties	Preventivo	Riservatezza Integrità Disponibilità	Governance Identity and access management	Governance and Ecosystem	L'organizzazione segrega i ruoli e le aree di responsabilità in conflitto.		Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì
5	Controlli organizzativi	5.4	Gestione delle responsabilità	Preventivo	Riservatezza Integrità Disponibilità	Governance	Governance and Ecosystem	Il personale è informato circa il proprio ruolo e relative responsabilità anche attraverso linee guida che definiscono le aspettative di sicurezza delle informazione e la protezione dei dati personali relativamente al loro ruolo all'interno dell'organizzazione.		Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì
5	Controlli organizzativi	5.4	Gestione delle responsabilità	Preventivo	Riservatezza Integrità Disponibilità	Governance	Governance and Ecosystem	Il personale è adeguatamente formato circa la sicurezza delle informazioni e la protezione dei dati personali relativamente al proprio ruolo e responsabilità.		Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì
5	Controlli organizzativi	5.4	Gestione delle responsabilità	Preventivo	Riservatezza Integrità Disponibilità	Governance	Governance and Ecosystem	All'interno dei contratti di assunzione L'organizzazione definisce, per coloro i quali saranno impegnati in ruoli aventi impatto il sistema di gestione, delle clausole relative alla sicurezza delle informazioni e protezione dei dati personali. In particolare, sono definite le clausole di riservatezza		Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì
5	Controlli organizzativi	5.4	Gestione delle responsabilità	Preventivo	Riservatezza Integrità Disponibilità	Governance	Governance and Ecosystem	Sono messi a disposizione canali riservati per riportare violazioni alla politica di sicurezza delle informazione, protezione dei dati personali e cloud.		Sì	Sì	No	No	Sì	Sì	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì
5	Controlli organizzativi	5.5	Contatti con le Autorità	Preventivo Correttivo	Riservatezza Integrità Disponibilità	Governance	Defence Resilience	L'organizzazione stabilisce e mantiene contatti con le autorità rilevanti rispetto al Sistema di Gestione nominando il Data Protection Officer (DPO) quale punto di contatto per la protezione dei dati personali.		No	Sì	Sì	No	Sì	No	No	No	No	No	No	No	Sì	No	No
5	Controlli organizzativi	5.6	Contatti con gruppi d'interesse specialistici	Preventivo Correttivo	Riservatezza Integrità Disponibilità	Governance	Defence	L'organizzazione stabilisce e mantiene contatti con gruppi di interesse speciali o altri forum di sicurezza specializzati e associazioni professionali.		No	Sì	Sì	No	Sì	No	No	No	No	No	No	No	Sì	No	No
5	Controlli organizzativi	5.7	Threat intelligence	Preventivo Investigativo Correttivo	Riservatezza Integrità Disponibilità	Threat and vulnerability management	Defence Resilience	L'organizzazione raccoglie ed analizza le informazioni relative alle minacce alla sicurezza delle informazioni per produrre informazioni sulle minacce stesse al fine di prevenire, rilevare o rispondere alle minacce.		No	Sì	No	No	Sì	No	No	Sì	Sì	Sì	No	Sì	Sì	No	Sì
5	Controlli organizzativi	5.8	Sicurezza delle informazioni nella gestione dei progetti	Preventivo	Riservatezza Integrità Disponibilità	Governance	Governance and Ecosystem Protection	L'organizzazione integra la sicurezza delle informazioni nella gestione dei progetti al fine di assicurare che i rischi per la sicurezza delle informazioni siano affrontati come parte della gestione del progetto		No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
5	Controlli organizzativi	5.9	Inventario delle informazioni e di altri beni associati	Preventivo	Riservatezza Integrità Disponibilità	Asset Management	Governance and Ecosystem Protection	L'organizzazione sviluppa e mantiene un inventario degli asset e delle informazioni e risorse associate, inclusi i proprietari e lo mantiene aggiornato, accurato, coerente e allineato con altri inventari.		No	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì	Sì	Sì	Sì	No
5	Controlli organizzativi	5.9	Inventario delle informazioni e di altri beni associati	Preventivo	Riservatezza Integrità Disponibilità	Asset Management	Governance and Ecosystem Protection	L'organizzazione identifica le sue informazioni e gli asset associati e determina la loro importanza in termini di sicurezza delle informazioni secondo la classificazione delle informazioni associata. La documentazione viene mantenuta in inventari dedicati, a seconda dei casi.		No	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì	Sì	Sì	Sì	No
5	Controlli organizzativi	5.9	Inventario delle informazioni e di altri beni associati	Preventivo	Riservatezza Integrità Disponibilità	Asset Management	Governance and Ecosystem Protection	L'organizzazione assegna tempestivamente l'ownership dell'asset a un individuo o a un gruppo per le informazioni identificate e altri asset associati, identificando anche il livello di classificazione. Tali soggetti sono responsabili della corretta gestione dell'asset durante l'intero ciclo di vita dell'asset.		Sì	Sì	No	No	No	Sì	No	No	No	No	Sì	Sì	Sì	No	No
5	Controlli organizzativi	5.9	Inventario delle informazioni e di altri beni associati	Preventivo	Riservatezza Integrità Disponibilità	Asset Management	Governance and Ecosystem Protection	L'organizzazione riassegna l'ownership dell'asset quando in caso di dimissioni o modifica del ruolo lavorativo.		Sì	Sì	No	No	No	Sì	No	No	No	No	Sì	Sì	Sì	No	No
5	Controlli organizzativi	5.10	Uso accettabile delle informazioni e di altre risorse associate	Preventivo	Riservatezza Integrità Disponibilità	Asset Management Information protection	Governance and Ecosystem Protection	L'organizzazione identifica, documenta e implementa le regole per l'uso accettabile e le procedure per il trattamento delle informazioni e altre risorse associate.		Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì	Sì
5	Controlli organizzativi	5.10	Uso accettabile delle informazioni e di altre risorse associate	Preventivo	Riservatezza Integrità Disponibilità	Asset Management Information protection	Governance and Ecosystem Protection	L'organizzazione provvede ad assicurare che il personale e gli utenti esterni che usano o hanno accesso alle informazioni ed altre risorse associate siano messe al corrente dei requisiti di sicurezza delle informazioni per la protezione e la gestione delle informazioni e degli asset associati.		Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì	Sì
5	Controlli organizzativi	5.11	Restituzione degli asset	Preventivo	Riservatezza Integrità Disponibilità	Asset Management	Protection	L'organizzazione provvede ad assicurare che il personale e le altri parti interessate, a seconda dei casi, restituiscano tutte le dotazioni in loro possesso, al momento del cambiamento o della cessazione del loro impiego, contratto o accordo		Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì
5	Controlli organizzativi	5.12	Classificazione delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Information protection	Protection Defence	L'organizzazione classifica le informazioni secondo le esigenze di sicurezza delle informazioni dell'Ente basate sulla riservatezza, integrità, disponibilità e sui requisiti delle parti interessate.		No	Sì	No	No	No	No	No	Sì	Sì	No	Sì	Sì	Sì	No	No
5	Controlli organizzativi	5.13	Etichettatura delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Information protection	Protection Defence	L'organizzazione sviluppa e implementa una serie appropriata di procedure per l'etichettatura delle informazioni in conformità con lo schema di classificazione delle informazioni adottato dall'Ente.		No	Sì	No	No	No	No	No	Sì	Sì	No	Sì	Sì	Sì	No	No
5	Controlli organizzativi	5.14	Trasferimento delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Asset Management Information protection	Protection	L'organizzazione pone in essere regole, procedure o accordi di trasferimento delle informazioni per tutti i tipi di trasferimento all'interno dell'Ente e tra l'Ente e altre parti.		Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì
5	Controlli organizzativi	5.14	Trasferimento delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Asset Management Information protection	Protection	L'organizzazione stabilisce e mantiene gli accordi di trasferimento, incluso l'autenticazione del destinatario, quando le informazioni vengono trasferite tra l'Ente e le terze parti, al fine di proteggere le informazioni in tutte le forme in transito.		Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì
5	Controlli organizzativi	5.14	Trasferimento delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Asset Management Information protection	Protection	L'organizzazione per tutte le regole, procedure o accordi di trasferimento delle informazioni prevede controlli progettati per proteggere le informazioni da intercettazioni, accesso non autorizzato, modifica, distruzione, denial of service, compresi i livelli di controllo dell'accesso commisurato alle informazioni coinvolte.		Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì
5	Controlli organizzativi	5.14	Trasferimento delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Asset Management Information protection	Protection	L'organizzazione applica opportuni controlli per assicurare la tracciabilità e il non ripudio, compreso il mantenimento di una catena di custodia per le informazioni in transito e l'identificazioni di appropriati contatti relativi al trasferimento delle informazioni come i proprietari delle informazioni, risk owners e i responsabili della sicurezza.		Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì
5	Controlli organizzativi	5.14	Trasferimento delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Asset Management Information protection	Protection	L'organizzazione tiene in considerazione qualsiasi requisito legale, statutario, normativo e contrattuale relativo al trasferimento di informazioni, come ad esempio i requisiti per le firme elettroniche.		Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì
5	Controlli organizzativi	5.14	Trasferimento delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Asset Management Information protection	Protection	L'organizzazione, quando utilizza mezzi di comunicazione elettronica per il trasferimento delle informazioni, protegge le informazioni elettroniche contro i malware.		Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì

Atto n. F00004 del 24/01/2024

5	Controlli organizzativi	5.14	Trasferimento delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Asset Management Information protection	Protection	L'organizzazione, quando trasferisce supporti di archiviazione fisica, provvede a tenere registri per l'identificazione del contenuto dei supporti di archiviazione, la protezione applicata, nonché registrazione dell'elenco dei destinatari autorizzati, i tempi di trasferimento e di ricevimento a destinazione.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.14	Trasferimento delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Asset Management Information protection	Protection	L'organizzazione, con riferimento al trasferimento verbale delle informazioni, ricorda al personale e alle altri parti interessate i corretti comportamenti da tenere al fine di preservare la divulgazione di informazioni riservate.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.15	Controllo degli accessi	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione stabilisce ed implementa regole per controllare l'accesso fisico e logico alle informazioni e altri asset associati, in base ai requisiti di sicurezza delle informazioni.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.15	Controllo degli accessi	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione determina quali entità hanno il diritto di richiedere l'accesso alle informazioni e altri asset associati a tali informazioni, mantenendo una coerenza tra i diritti di accesso e la classificazione delle informazioni ed i requisiti di sicurezza del perimetro fisico.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.15	Controllo degli accessi	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione provvede ad attuare un processo formale di autorizzazione delle richieste di accesso.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.15	Controllo degli accessi	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione provvede a garantire l'accesso solo alle informazioni e asset associati per i quali sono stati autorizzati all'utilizzo.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.15	Controllo degli accessi	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione applica i principi di "need-to-know", "need-to-use" e "least privilege".		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.15	Controllo degli accessi	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione effettua una revisione periodica dei diritti di accesso.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.16	Gestione delle identità	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione gestisce l'intero ciclo di vita delle utenze, assegnando una specifica utenza ad una singola persona la quale sarà responsabile delle azioni compiute da quella specifica utenza.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.16	Gestione delle identità	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione permette l'utilizzo delle utenze condivise solo per ragioni commerciali o operative e autorizza tale eventualità solo tramite un processo di approvazione formale.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.16	Gestione delle identità	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione prevede che le utenze assegnate ad entità non umane siano soggette a un'approvazione adeguatamente differenziata e ad una supervisione continua ed indipendente.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.16	Gestione delle identità	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione provvede a disattivare e rimuovere tempestivamente le utenze che non sono più necessarie (ad esempio se la persona associata a quell'utenza ha lasciato l'Ente o ha cambiato ruolo)		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.16	Gestione delle identità	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione veta la duplicazione delle utenze, ovvero proibisce che si creino utenze multiple per la stessa entità all'interno dello stesso contesto.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.16	Gestione delle identità	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione provvede a mantenere un registro di tutti gli eventi significativi riguardanti l'uso e la gestione delle utenze e delle informazioni di autenticazione.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.16	Gestione delle identità	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione, quando impiega utenze fornite o emesse da terzi, garantisce che i fornitori assicurano un livello di sicurezza adeguato e che qualsiasi rischio associato sia conosciuto e sufficientemente trattato.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.17	Informazioni di autenticazione	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione effettua controlli periodici sull'assegnazione e la gestione delle informazioni di autenticazione, compresa la consulenza al personale sulle gestione appropriata delle informazioni di autenticazione.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.17	Informazioni di autenticazione	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione provvede a fornire password e/o numeri di identificazione personale (PIN) temporanee che non siano indovinabili ed unici per ogni persona, richiedendo agli utenti di cambiarle al primo utilizzo.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.17	Informazioni di autenticazione	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione provvede a trasmettere in modo sicuro le informazioni di autenticazione, anche quelle temporanee, richiedendo agli utenti conferma di avvenuta ricezione.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.17	Informazioni di autenticazione	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione provvede a cambiare immediatamente le informazioni di autenticazione predefinite dai fornitori, subito dopo l'installazione di sistemi o software		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.17	Informazioni di autenticazione	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione registra e conserva gli eventi significativi riguardanti l'assegnazione e la gestione delle informazioni.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.17	Informazioni di autenticazione	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione informa tutto il personale e le parti interessate che le informazioni segrete di autenticazione come le password devono esser tenute riservate e non devono esser condivise con nessuno.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.17	Informazioni di autenticazione	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione assicura che le informazioni di autenticazione colpite o compromesse vengono cambiate immediatamente dopo la notifica o qualsiasi altra indicazione di compromissione.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.17	Informazioni di autenticazione	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione utilizza un sistema di gestione delle password che permette agli utenti di selezionare e cambiare le proprie password.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.17	Informazioni di autenticazione	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione forza gli utenti a cambiare le loro password al primo accesso, imponendo il cambio di password se necessario, ad esempio dopo un incidente di sicurezza, la cessazione o el cambio di lavoro.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.17	Informazioni di autenticazione	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione, tramite il sistema di gestione delle password, previene il riutilizzo di password precedenti e l'utilizzo di password di uso comune e la visualizzazione delle password sullo schermo quando vengono inserite.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.18	Diritti d'accesso	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione provvede a fornire, rivedere, modificare e rimuovere i diritti di accesso alle informazione e ad altri asset associati in conformità con le politiche aziendali.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.18	Diritti d'accesso	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione nel processo di assegnazione e revoca dei diritti di accesso fisico e logico verso utente autorizzate, tiene in considerazione i requisiti e le regole aziendali sul controllo dell'accesso.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.18	Diritti d'accesso	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione assicura che i diritti di accesso vengono rimossi quando qualcuno non ha più la necessità di accedere alle informazioni e ad altri asset associati, in particolare assicurando che i diritti di accesso degli utenti che hanno lasciato l'organizzazione siano rimossi in modo tempestivo.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.18	Diritti d'accesso	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione nel processo di assegnazione e revoca dei diritti di accesso fisico e logico tiene in considerazione la possibilità di dare diritti di accesso temporanei per un periodo di tempo limitato e revocarli alla scadenza, in particolare per il personale temporaneo.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.18	Diritti d'accesso	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione verifica che il livello di accesso concesso sia conforme alle politiche specifiche sul controllo dell'accesso ed coerente con altri requisiti di sicurezza delle informazioni come ad esempio la segregazione dei compiti.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.18	Diritti d'accesso	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione assicura che i diritti di accesso siano attivati solo dopo che le procedure di autorizzazione sono state completate con successo		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.18	Diritti d'accesso	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione mantiene un registro centrale dei diritti di accesso concessi ad un utente per accedere alle informazioni ed altri asset associati.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.18	Diritti d'accesso	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione effettua revisioni regolari dei diritti di accesso fisici e logici, tenendo in considerazione qualsiasi cambiamento all'interno dell'Ente (ad esempio cambio di lavoro, promozione) o cessazione del rapporto di lavoro e qualsiasi valutazione di fattori di rischio quali, ad esempio, il valore delle attività e le sue informazioni attualmente accessibili		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.19	Sicurezza delle informazioni nelle relazioni con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione definisce ed implementa processi e procedure per la gestione dei rischi di sicurezza delle informazioni associati all'uso di prodotti o servizi erogati da fornitori, anche in riferimento a fornitori di servizi Cloud.		No	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.19	Sicurezza delle informazioni nelle relazioni con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione provvede ad identificare e documentare i tipi di fornitori (ad es. servizi ICT, logistica, servizi di pubblica utilità, servizi finanziari, componenti di infrastrutture ICT) che possono influire sulla riservatezza, integrità e disponibilità delle informazioni.		No	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.19	Sicurezza delle informazioni nelle relazioni con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione provvede a stabilire regole su come valutare e selezionare i fornitori in base alla tenibilità delle informazioni, prodotti e servizi e provvede a selezionare i prodotti o servizi del fornitore che hanno adeguati controlli di sicurezza delle informazioni e che assicurano l'integrità delle informazioni e del trattamento delle informazioni		No	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.20	Sicurezza delle informazioni nelle relazioni con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione definisce le informazioni dell'organizzazione, i servizi ICT e l'infrastruttura fisica a cui i fornitori possono accedere, controllare ed utilizzare.		No	SI	SI	No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.20	Sicurezza delle informazioni nelle relazioni con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione definisce i tipi di componenti dell'infrastruttura ICT e i servizi forniti dai fornitori che possono influire sulla riservatezza, integrità e disponibilità delle informazioni.		No	SI	SI	No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.19	Sicurezza delle informazioni nelle relazioni con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione valuta e gestisce i rischi di sicurezza delle informazioni associate all'uso da parte dei fornitori delle informazioni e di altre risorse associate, compresi i rischi derivanti da potenziali malintenzionati appartenenti al personale del fornitore, e malfunzionamenti e vulnerabilità dei prodotti o dei servizi offerti dai fornitori		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

5	Controlli organizzativi	5.19	Sicurezza delle informazioni nelle relazioni con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione monitora la conformità ai requisiti di sicurezza delle informazioni per ogni tipo di fornitore e tipo di accesso, mitigando la non conformità di un fornitore sia questa sia stata rilevata attraverso il monitoraggio o con altri mezzi		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.19	Sicurezza delle informazioni nelle relazioni con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione gestisce gli incidenti e gli imprevisti associati al prodotto e ai servizi dei fornitori, comprese responsabilità sia dell'organizzazione che dei fornitori.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.19	Sicurezza delle informazioni nelle relazioni con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione effettua corsi di formazione per il personale che interagisce con il personale dei fornitore per quanto riguarda le regole di ingaggio appropriate, le politiche, i processi e le procedure specifiche per argomento e comportamento in base al tipo di fornitore e al livello di accesso del fornitore ai sistemi e alle informazioni dell'organizzazione		SI	SI	SI	No	No	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.19	Sicurezza delle informazioni nelle relazioni con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione definisce i requisiti per garantire una cessazione sicura del rapporto con il fornitore, tra cui il de-provisioning dei diritti di accesso, il trattamento delle informazioni, il determinare la proprietà intellettuale sviluppata durante l'impiego, la portabilità delle informazioni in caso di cambio di fornitore, la restituzione dei beni, lo smaltimento sicuro delle informazioni.		No	SI	SI	No	No	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.20	Sicurezza delle informazioni negli accordi con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione stabilisce e concorda con ogni tipo di fornitore i requisiti di sicurezza delle informazioni, in base al tipo di relazione con il fornitore, affinché ci sia una chiara comprensione tra l'Ente ed il fornitore per quanto riguarda gli obblighi di entrambi le parti necessari per soddisfare i requisiti di sicurezza delle informazioni.		No	SI	SI	No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.20	Sicurezza delle informazioni negli accordi con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione prevede regole di uso accettabile delle informazioni e degli asset associati, compreso l'uso non accettabile.		No	SI	SI	No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.20	Sicurezza delle informazioni negli accordi con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione definisce procedure e condizioni per l'autorizzazione e la rimozione dell'autorizzazione per l'uso delle informazioni e altri asset associati da parte del personale del fornitore		No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.20	Sicurezza delle informazioni negli accordi con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione definisce requisiti di sicurezza delle informazioni riguardanti l'infrastruttura ICT del fornitore.		No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.20	Sicurezza delle informazioni negli accordi con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione definisce indennizzi e rimedi per il mancato rispetto dei requisiti da parte del fornitore.		No	SI	SI	No	No	No	No	No	No	No	No	No	No	No	No
5	Controlli organizzativi	5.20	Sicurezza delle informazioni negli accordi con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione definisce disposizioni rilevanti per il subappalto, compresi i controlli che devono essere implementati, come l'accordo sull'uso dei subfornitori (ad esempio averli sotto gli stessi obblighi del fornitore, richiedendo di avere un elenco di subfornitori)		No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.20	Sicurezza delle informazioni negli accordi con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione richiede, nei limiti previsti dalla legge, qualsiasi requisito di screening del personale del fornitore, comprese le procedure di notifica se lo screening non è stato completato o se i risultati danno motivo di dubbio o preoccupazione.		SI	SI	No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.20	Sicurezza delle informazioni negli accordi con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione prevede l'obbligo per il fornitore di consegnare periodicamente una relazione sull'efficacia dei controlli e l'accordo sulla correzione tempestiva delle questioni rilevanti sollevate dal rapporto e la risoluzione dei difetti e dei conflitti.		No	SI	SI	No	No	No	No	No	No	No	No	No	No	No	No
5	Controlli organizzativi	5.20	Sicurezza delle informazioni negli accordi con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione prevede che sia assicurata la disponibilità di una struttura alternativa (sito di disaster recovery) non soggetta alle stesse minacce della struttura primaria e considerazioni per i controlli di ripresa (controlli alternativi) nel caso in cui i controlli primari falliscano.		No	SI	SI	SI	SI	No	No	No	SI	SI	No	No	No	SI	No
5	Controlli organizzativi	5.20	Sicurezza delle informazioni negli accordi con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione è dotata di un processo di gestione dei cambiamenti che assicura la notifica preventiva e la possibilità di non accettare i cambiamenti.		No	SI	No	No	No	No	No	No	No	No	No	No	SI	No	No
5	Controlli organizzativi	5.20	Sicurezza delle informazioni negli accordi con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione prevede clausole di rescissione alla conclusione dell'accordo, compresa la gestione delle registrazioni, la restituzione dei beni, lo smaltimento sicuro delle informazioni e di altri asset associati e qualsiasi obblighi di riservatezza in corso.		No	SI	SI	No	No	SI	SI	No	SI	No	No	SI	SI	No	SI
5	Controlli organizzativi	5.20	Sicurezza delle informazioni negli accordi con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione si assicura che sia fornito un metodo per la distruzione in modo sicuro delle informazioni e di altri asset associati conservati dal fornitore non appena non sono più necessarie.		No	SI	SI	No	No	SI	SI	No	SI	No	No	SI	SI	No	SI
5	Controlli organizzativi	5.20	Sicurezza delle informazioni negli accordi con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione si assicura che sia garantito che, alla fine del contratto, avvenga il passaggio del materiale ad un altro fornitore o all'Ente stesso.		No	SI	SI	No	No	SI	SI	No	SI	No	No	SI	SI	No	SI
5	Controlli organizzativi	5.20	Sicurezza delle informazioni negli accordi con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione mantiene un registro degli accordi con le terze parti (es. contratti, memurandum of understanding, accordi di condivisione di informazioni) per tenere traccia di dove sono le informazioni.		No	SI	SI	No	No	SI	SI	No	No	No	No	No	No	SI	SI
5	Controlli organizzativi	5.20	Sicurezza delle informazioni negli accordi con i fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione rivede, convalida ed aggiorna regolarmente i suoi accordi con le terze parti per assicurarsi che siano ancora necessari e adatti allo scopo con le relative clausole di sicurezza delle informazioni.		No	SI	SI	No	No	SI	SI	No	No	No	No	No	No	SI	SI
5	Controlli organizzativi	5.21	Gestire la sicurezza delle informazioni nella catena di fornitura ICT	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione definisce ed implementa processi e procedure per gestire i rischi di sicurezza delle informazioni associati alla catena di fornitura di prodotti e servizi ICT.		No	SI	SI	No	SI	SI	SI	No	No	No	No	No	SI	No	SI
5	Controlli organizzativi	5.21	Gestire la sicurezza delle informazioni nella catena di fornitura ICT	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione definisce i requisiti di sicurezza delle informazioni da applicare all'acquisizione di prodotti o servizi ICT, richiedendo ai fornitori di servizi ICT di utilizzare tali requisiti in tutta la catena di fornitura se subappaltano parti del servizio ICT fornito all'organizzazione.		No	SI	No	No	No	No	SI	SI	SI	SI	No	SI	SI	SI	SI
5	Controlli organizzativi	5.21	Gestire la sicurezza delle informazioni nella catena di fornitura ICT	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione richiede ai fornitori di prodotti ICT di fornire informazioni che descrivano i componenti software utilizzati nei prodotti e le funzioni di sicurezza implementate		No	SI	No	No	No	No	SI	SI	SI	SI	No	SI	SI	SI	SI
5	Controlli organizzativi	5.21	Gestire la sicurezza delle informazioni nella catena di fornitura ICT	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione implementa un processo di monitoraggio e metodi accettabili per convalidare che i prodotti e servizi ICT consegnati siano conformi ai requisiti di sicurezza dichiarati		No	SI	No	No	No	No	SI	SI	SI	SI	No	SI	SI	SI	SI
5	Controlli organizzativi	5.21	Gestire la sicurezza delle informazioni nella catena di fornitura ICT	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione implementa un processo per identificare e documentare i componenti di prodotti o servizi che sono critici per il mantenimento delle funzionalità e che richiedono maggiore attenzione, controllo e follow-up, specialmente se il fornitore esternalizza aspetti dei componenti di prodotti o servizi ad altri fornitori		No	SI	SI	No	SI	No	No	No	No	SI	No	SI	SI	SI	No
5	Controlli organizzativi	5.21	Gestire la sicurezza delle informazioni nella catena di fornitura ICT	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione ottiene la garanzia che i componenti critici e la loro origine possono essere rintracciati lungo tutta la catena di fornitura		No	SI	SI	No	SI	No	No	No	No	SI	No	SI	SI	SI	No
5	Controlli organizzativi	5.21	Gestire la sicurezza delle informazioni nella catena di fornitura ICT	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione implementa processi per assicurare che i componenti dei fornitori siano autentici e smaltati rispetto alle loro specifiche e che raggiungano i livelli di sicurezza richiesti.		No	SI	SI	No	SI	No	No	No	No	SI	No	SI	SI	SI	No
5	Controlli organizzativi	5.22	Monitoraggio, revisione e gestione del cambiamento dei servizi dei fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection Defence Information security assurance	L'organizzazione monitora, rivede, valuta e gestisce regolarmente i cambiamenti nelle pratiche di sicurezza delle informazioni del fornitore e nella fornitura del servizio.		No	SI	SI	No	SI	No	SI	No	SI	SI	No	SI	SI	SI	SI
5	Controlli organizzativi	5.22	Monitoraggio, revisione e gestione del cambiamento dei servizi dei fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection Defence Information security assurance	L'organizzazione attua il monitoraggio, la revisione e la gestione dei cambiamenti dei servizi del fornitore garantendo che i termini e le condizioni di sicurezza delle informazioni degli accordi siano rispettati, che gli incidenti e i problemi di sicurezza delle informazioni siano gestiti correttamente e che i cambiamenti nei servizi del fornitore o nello stato dell'attività non influiscano sulla fornitura del servizio.		No	SI	SI	No	SI	No	SI	No	SI	SI	No	SI	SI	SI	SI
5	Controlli organizzativi	5.22	Monitoraggio, revisione e gestione del cambiamento dei servizi dei fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection Defence Information security assurance	L'organizzazione attua un processo per gestire la relazione tra l'Ente e il fornitore al fine di monitorare i livelli di prestazione dei servizi, le modifiche apportate dai fornitori (miglioramenti agli attuali servizi offerti, sviluppo di eventuali nuove applicazioni o sistemi, modifiche o aggiornamenti delle politiche e procedure del fornitore) e monitorare i cambiamenti nei servizi del fornitore (modifiche e miglioramenti alle reti, uso di nuove tecnologie, nuovi strumenti ed ambienti di sviluppo, cambi di subfornitori, subappalto ad un altro fornitore).		No	SI	SI	No	SI	No	SI	No	SI	SI	No	SI	SI	SI	SI
5	Controlli organizzativi	5.22	Monitoraggio, revisione e gestione del cambiamento dei servizi dei fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection Defence Information security assurance	L'organizzazione effettua un riesame dei rapporti di servizi prodotti dal fornitore e organizza regolarmente riunioni periodiche sullo stato di avanzamento.		No	SI	SI	No	SI	No	SI	No	SI	SI	No	SI	SI	SI	SI
5	Controlli organizzativi	5.22	Monitoraggio, revisione e gestione del cambiamento dei servizi dei fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection Defence Information security assurance	L'organizzazione conduce audit dei fornitori e dei subfornitori, insieme alla revisione delle relazioni dei revisori indipendenti, dando seguito agli eventuali rilievi identificati.		No	SI	SI	No	SI	No	SI	No	SI	SI	No	SI	SI	SI	SI
5	Controlli organizzativi	5.22	Monitoraggio, revisione e gestione del cambiamento dei servizi dei fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection Defence Information security assurance	L'organizzazione richiede al fornitore informazioni circa gli incidenti relativi alla sicurezza delle informazioni e rivede queste informazioni come richiesto dagli accordi e da qualsiasi linea guida.		No	SI	SI	No	SI	No	SI	No	SI	SI	No	SI	SI	SI	SI
5	Controlli organizzativi	5.22	Monitoraggio, revisione e gestione del cambiamento dei servizi dei fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection Defence Information security assurance	L'organizzazione esamina gli aspetti della sicurezza delle informazioni delle relazioni del fornitore con i propri fornitori.		No	SI	SI	No	SI	No	SI	No	SI	SI	No	SI	SI	SI	SI

5	Controlli organizzativi	5.22	Monitoraggio, revisione e gestione del cambiamento dei servizi dei fornitori	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection Defence Information security assurance	L'organizzazione si assicura che il fornitore mantenga una sufficiente capacità di servizio insieme ai piani attuabili per assicurare che i livelli di continuità del servizio concordati siano mantenuti a seguito di crisi o disastro.		No	SI	SI	SI	SI	No	SI	No	SI	SI	No	SI	SI	SI	SI
5	Controlli organizzativi	5.23	Sicurezza delle informazioni per l'uso dei servizi cloud	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione stabilisce i processi per l'acquisizione, l'uso, la gestione e la cessazione dei servizi Cloud in conformità con i requisiti di sicurezza delle informazioni dell'organizzazione.		No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.23	Sicurezza delle informazioni per l'uso dei servizi cloud	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione definisce e comunica a tutte le parti interessate una politica specifica sull'uso dei servizi cloud, all'interno della quale vengono definiti tutti i requisiti di sicurezza delle informazioni rilevanti associati a: - l'uso dei servizi cloud, - i criteri di selezione del servizio cloud e l'ambito di utilizzo del servizio cloud, - i ruoli e le responsabilità relative all'uso e alla gestione dei servizi in cloud, - quali controlli di sicurezza delle informazioni sono gestiti dal fornitore di servizi cloud e quali sono gestiti		No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.23	Sicurezza delle informazioni per l'uso dei servizi cloud	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione prevede che gli accordi sui servizi cloud siano predefiniti e non aperti a negoziazione e che tali accordi affrontino i requisiti di riservatezza, integrità, disponibilità e gestione delle informazioni dell'organizzazione, con appropriati obiettivi di livello e qualitativi del servizio cloud.		No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.23	Sicurezza delle informazioni per l'uso dei servizi cloud	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione effettua valutazioni del rischio pertinenti per identificare i rischi associati all'uso del servizio in cloud e qualsiasi rischio residuo connesso all'uso del servizio cloud viene chiaramente identificato e accettato dalla direzione		No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.23	Sicurezza delle informazioni per l'uso dei servizi cloud	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione prevede all'interno degli accordi tra il fornitore di servizi Cloud e l'Ente che: - vengano fornite soluzioni basate su standard accettati dal settore, - i controlli di accesso al servizio cloud soddisfino i requisiti dell'organizzazione, - vengano implementate soluzioni di monitoraggio e protezione da malware, - l'elaborazione e l'archiviazione di informazioni sensibili dell'organizzazione avvenga in luoghi appropriati, - venga fornito supporto dedicato in caso di un incidente di sicurezza delle informazioni nell'ambiente del servizio cloud, - siano soddisfatti i requisiti di sicurezza delle informazioni nel caso in cui i servizi cloud siano ulteriormente		No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.23	Sicurezza delle informazioni per l'uso dei servizi cloud	Preventivo	Riservatezza Integrità Disponibilità	Supplier relationship security	Governance and Ecosystem Protection	L'organizzazione, agendo come cliente del servizio cloud, tiene in considerazione se l'accordo dovrebbe richiedere ai fornitori di servizi cloud di fornire una notifica anticipata prima di qualsiasi cambiamento che abbia un impatto sostanziale e che riguardi il modo in cui il servizio viene fornito all'organizzazione, tra cui modifiche all'infrastruttura tecnica, l'ubicazione o archiviazione di informazioni in una nuova giurisdizione e l'uso di fornitori di servizi cloud alla pari o di altri subappaltatori.		No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.24	Pianificazione e preparazione della gestione degli incidenti di sicurezza delle informazioni	Correttivo	Riservatezza Integrità Disponibilità	Governance information security event management	Defence	L'organizzazione pianifica e si prepara a gestire gli incidenti di sicurezza delle informazioni definendo, stabilendo e comunicando i processi di gestione degli incidenti di sicurezza delle informazioni, i ruoli e le responsabilità.		No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.24	Pianificazione e preparazione della gestione degli incidenti di sicurezza delle informazioni	Correttivo	Riservatezza Integrità Disponibilità	Governance information security event management	Defence	L'organizzazione definisce i ruoli e le responsabilità per eseguire le procedure di gestione degli incidenti, comunicandoli alle parti interessate interne ed esterne		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.24	Pianificazione e preparazione della gestione degli incidenti di sicurezza delle informazioni	Correttivo	Riservatezza Integrità Disponibilità	Governance information security event management	Defence	L'organizzazione stabilisce un metodo comune per la segnalazione di eventi relativi alla sicurezza delle informazioni, compresi i punti di contatto e stabilisce un processo di gestione degli incidenti per avere la capacità di gestione degli incidenti di sicurezza delle informazioni, compresa l'amministrazione, la documentazione, il rilevamento, la prioritizzazione, l'analisi, la comunicazione e il coordinamento delle parti interessate.		SI	SI	SI	No	SI	No	No	No	No	No	No	No	No	No	No
5	Controlli organizzativi	5.24	Pianificazione e preparazione della gestione degli incidenti di sicurezza delle informazioni	Correttivo	Riservatezza Integrità Disponibilità	Governance information security event management	Defence	L'organizzazione stabilisce un processo di risposta agli incidenti per fornire all'Ente la capacità di valutare, rispondere e imparare dagli incidenti di sicurezza delle informazioni		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.24	Pianificazione e preparazione della gestione degli incidenti di sicurezza delle informazioni	Correttivo	Riservatezza Integrità Disponibilità	Governance information security event management	Defence	L'organizzazione permette solo al personale competente di gestire le questioni relative agli incidenti di sicurezza delle informazioni all'interno dell'organizzazione, inoltre, stabilisce un processo per identificare la formazione richiesta, la certificazione e lo sviluppo professionale continuo per il personale addetto alla risposta agli incidenti.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.24	Pianificazione e preparazione della gestione degli incidenti di sicurezza delle informazioni	Correttivo	Riservatezza Integrità Disponibilità	Governance information security event management	Defence	L'organizzazione, tramite la direzione, assicura che un piano di gestione degli incidenti di sicurezza sia creato considerando diversi scenari e che siano sviluppate e implementate procedure per: - la valutazione degli eventi di sicurezza delle informazioni secondo i criteri di ciò che costituisce un incidente di sicurezza delle informazioni, - monitoraggio, rilevamento, classificazione, analisi e segnalazione degli eventi e degli incidenti relativi alla sicurezza delle informazioni, - gestire gli incidenti di sicurezza delle informazioni fino alla conclusione degli stessi, compresa la risposta e l'escalation secondo il tipo e la categoria dell'incidente, eventuale attivazione della crisi e attivazione di piani di continuità, recupero controllato di un incidente e comunicazione alle parti interessate interne ed esterne, - il coordinamento con le parti interessate interne ed esterne (come le autorità, i gruppi e forum di interesse, fornitori e clienti), - registrazione delle attività di gestione degli incidenti e gestione delle prove, - identificazione delle lezioni apprese ed eventuali miglioramenti alle procedure di gestione degli incidenti o controlli di sicurezza delle informazioni che sono necessari.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.24	Pianificazione e preparazione della gestione degli incidenti di sicurezza delle informazioni	Correttivo	Riservatezza Integrità Disponibilità	Governance information security event management	Defence	L'organizzazione, per le procedure di segnalazione, prevede che siano incluse azioni da intraprendere in caso di un evento di sicurezza delle informazioni (ad es. annotare tutti i dettagli pertinenti immediatamente), l'uso di moduli di incidente per supportare il personale nell'esecuzione di azioni necessarie quando si segnalano incidenti di sicurezza delle informazioni e qualsiasi requisito esterno sulla segnalazione di incidenti entro il tempo definito.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.25	Valutazione e decisione su eventi di sicurezza delle informazioni	Investigativo	Riservatezza Integrità Disponibilità	Information security event management	Defence	L'organizzazione, tramite il personale responsabile del coordinamento e della risposta agli incidenti di sicurezza delle informazioni, esegue una valutazione e prende una decisione sugli eventi relativi alla sicurezza delle informazioni e registra in dettaglio i risultati della valutazione e della decisione allo scopo di riferimenti futuri e di verifica.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.26	Risposta agli incidenti di sicurezza delle informazioni	Correttivo	Riservatezza Integrità Disponibilità	Information security event management	Defence	L'organizzazione affronta gli incidenti di sicurezza delle informazioni in conformità con le procedure adottate, comunicandole a tutte le parti interessate.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.26	Risposta agli incidenti di sicurezza delle informazioni	Correttivo	Riservatezza Integrità Disponibilità	Information security event management	Defence	L'organizzazione, nella sua risposta agli incidenti di sicurezza delle informazioni, prevede a: - contenere, se le conseguenze dell'incidente possono diffondersi, i sistemi colpiti dall'incidente, - raccogliere le evidenze il più presto possibile dopo l'intervento, - gestire la crisi ed attivare i piani di continuità operativa, - assicurare che tutte le attività di risposta coinvolte siano adeguatamente registrate per un'analisi successiva, - comunicare l'esistenza dell'incidente di sicurezza delle informazioni o qualsiasi dettaglio rilevante a tutte le parti interessate, interne ed esterne, secondo il principio del need-to-know. - coordinarsi con le parti interne ed esterne come autorità, gruppi di interesse esterni e forum, fornitori e clienti per migliorare l'efficacia della risposta e contribuire a minimizzare le conseguenze per altre organizzazioni, - una volta che l'incidente è stato affrontato con successo, chiuderlo formalmente e registrarlo, - condurre l'analisi forense della sicurezza delle informazioni, - eseguire l'analisi post-incidente per identificare la causa principale, - identificare e gestire le vulnerabilità e le debolezze del sistema delle informazioni, comprese quelle relative ai controlli che hanno causato, contribuito a o non sono riusciti a prevenire.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

5	Controlli organizzativi	5.27	Imparare dagli incidenti di sicurezza delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Information security event management	Defence	L'organizzazione utilizza la conoscenza acquisita dagli incidenti di sicurezza delle informazioni per rafforzare e migliorare i controlli di sicurezza delle informazioni ed il piano di gestione degli incidenti, identificare gli incidenti ricorrenti o gravi e le loro cause, migliorare la consapevolezza e la formazione del personale.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.28	Raccolta delle evidenze	Correttivo	Riservatezza Integrità Disponibilità	Information security event management	Defence	L'organizzazione stabilisce ed implementa procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione delle prove relative agli eventi di sicurezza delle informazioni.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.28	Raccolta delle evidenze	Correttivo	Riservatezza Integrità Disponibilità	Information security event management	Defence	L'organizzazione tramite le procedure per l'identificazione, la raccolta, acquisizione e conservazione delle prove relative agli eventi di sicurezza delle informazioni riesce a dimostrare che: - le registrazioni sono complete e non sono state manomesse in alcun modo; - le copie delle evidenze elettroniche sono probabilmente identiche agli originali; - qualsiasi sistema informatico da cui sono state raccolte le evidenze funzionava correttamente al momento in cui le evidenze sono state registrate.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.29	Sicurezza delle informazioni durante le interruzioni	Preventivo Correttivo	Riservatezza Integrità Disponibilità	Continuity	Protection Resilience	L'organizzazione pianifica come mantenere la sicurezza delle informazioni a un livello appropriato durante l'interruzione.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.29	Sicurezza delle informazioni durante le interruzioni	Preventivo Correttivo	Riservatezza Integrità Disponibilità	Continuity	Protection Resilience	L'organizzazione implementa e mantiene controlli sulla sicurezza delle informazioni, sistemi e strumenti di supporto all'interno dei piani di continuità aziendale e dell'ICT, processi per mantenere i controlli di sicurezza delle informazioni durante la fase di interruzione, controlli compensativi per i controlli di sicurezza delle informazioni che non possono essere mantenuti durante l'interruzione.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.30	Prontezza dell'ICT per la continuità dell'attività	Correttivo	Disponibilità	Continuity	Resilience	L'organizzazione pianifica, implementa, mantiene e testa la prontezza dell'ICT sulla base degli obiettivi di continuità aziendale e sui requisiti di continuità dell'ICT.		No	SI	SI	No	SI	No	No	No	SI	SI	No	No	SI	SI	No
5	Controlli organizzativi	5.30	Prontezza dell'ICT per la continuità dell'attività	Correttivo	Disponibilità	Continuity	Resilience	L'organizzazione assicura che è in atto una struttura organizzativa adeguata per prevenire, mitigare e rispondere a un'interruzione supportata da personale con necessaria responsabilità, autorità e competenza.		SI	SI	SI	No	SI	No	No	No	SI	SI	No	No	SI	SI	No
5	Controlli organizzativi	5.30	Prontezza dell'ICT per la continuità dell'attività	Correttivo	Disponibilità	Continuity	Resilience	L'organizzazione, tramite i suoi piani di continuità ICT, le procedure di risposta e recupero, descrive in dettaglio come l'organizzazione pianifica un'interruzione del servizio ICT ed effettua regolarmente valutazioni tramite esercizi e test e servizio approvati dalla direzione.		No	SI	SI	No	SI	No	No	No	SI	SI	No	No	SI	SI	No
5	Controlli organizzativi	5.30	Prontezza dell'ICT per la continuità dell'attività	Correttivo	Disponibilità	Continuity	Resilience	L'organizzazione prevede che nei suoi piani di continuità ICT siano incluse specifiche di performance e capacità per soddisfare gli obiettivi di continuità dell'attività.		No	SI	SI	No	SI	No	No	No	SI	SI	No	No	SI	SI	No
5	Controlli organizzativi	5.31	Requisiti legali, statutari, normativi e contrattuali	Preventivo	Riservatezza Integrità Disponibilità	Legal and compliance	Governance and Ecosystem Protection	L'organizzazione identifica, documenta e tiene aggiornati i requisiti legali, statutari, normativi e contrattuali relativi alla sicurezza delle informazioni.		No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.31	Requisiti legali, statutari, normativi e contrattuali	Preventivo	Riservatezza Integrità Disponibilità	Legal and compliance	Governance and Ecosystem Protection	L'organizzazione prende in considerazione i requisiti esterni, compresi i requisiti legali, statutari, normativi e contrattuali quando: - sviluppa politiche e procedure di sicurezza delle informazioni, - progetta, implementa o modifica dei controlli di sicurezza delle informazioni, - classifica le informazioni e altri asset associati come parte del processo di definizione dei requisiti di sicurezza delle informazioni per esigenze interne o per accordi con i fornitori, - esegue valutazioni del rischio per la sicurezza delle informazioni e determina il rischio per la sicurezza delle informazioni, - determina i processi con i relativi ruoli e responsabilità inerenti alla sicurezza delle informazioni, - determina i requisiti contrattuali dei fornitori rilevanti per l'organizzazione e l'ambito di fornitura di prodotti e servizi.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.31	Requisiti legali, statutari, normativi e contrattuali	Preventivo	Riservatezza Integrità Disponibilità	Legal and compliance	Governance and Ecosystem Protection	L'organizzazione identifica e rivede regolarmente tutta la legislazione e i regolamenti rilevanti per la sicurezza delle informazioni dell'organizzazione al fine di essere consapevole dei requisiti per il proprio tipo di attività e prende in considerazione la conformità in tutti i paesi pertinenti quando conduce affari in altri paesi o utilizza prodotti e servizi di altri paesi in cui le leggi e i regolamenti possono influenzare l'organizzazione o trasferisce informazioni attraverso i confini giurisdizionali dove le leggi e i regolamenti possono influenzarle.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.31	Requisiti legali, statutari, normativi e contrattuali	Preventivo	Riservatezza Integrità Disponibilità	Legal and compliance	Governance and Ecosystem Protection	L'organizzazione prende in considerazione restrizioni all'importazione o all'esportazione di hardware e software progettati per avere funzioni crittografiche, possibili restrizioni all'uso della crittografia, metodi obbligatori o discrezionali di accesso da parte delle autorità alle informazioni criptate, validità di firme digitali, sigilli e certificati.		No	SI	SI	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
5	Controlli organizzativi	5.32	Diritti di proprietà intellettuale	Preventivo	Riservatezza Integrità Disponibilità	Legal and compliance	Governance and Ecosystem Protection	L'organizzazione implementa procedure appropriate per proteggere i diritti di proprietà intellettuale, come ad esempio l'acquisto di software solo attraverso fonti note e rispettabili, il mantenimento di registri di beni con requisiti per proteggere i diritti di proprietà intellettuale, evitare che non sia superato il numero massimo di utenti consentito all'interno della licenza.		No	SI	SI	No	No	SI	SI	No	No	No	No	No	SI	No	SI
5	Controlli organizzativi	5.33	Protezione delle registrazioni	Preventivo	Riservatezza Integrità Disponibilità	Legal and compliance Asset Management Information protection	Defence	L'organizzazione protegge i registri da perdita, distruzione, falsificazione, accesso non autorizzato e rilascio non autorizzato tramite l'emissione di linee guida sulla conservazione, la gestione della catena di custodia e lo smaltimento dei documenti, che include la prevenzione della manipolazione dei documenti, la redazione di un programma di categorizzazione delle registrazioni e un programma di conservazione che definisce i documenti e il periodo di tempo per il quale dovrebbero essere conservati.		SI	SI	SI	No	No	SI	SI	SI	SI	No	SI	No	SI	No	SI
5	Controlli organizzativi	5.34	Privacy e protezione delle PII	Preventivo	Riservatezza Integrità Disponibilità	Information protection Legal and compliance	Protection	L'organizzazione identifica e soddisfa i requisiti relativi alla conservazione della privacy e protezione delle PII secondo le leggi e i regolamenti applicabili e requisiti contrattuali.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.34	Privacy e protezione delle PII	Preventivo	Riservatezza Integrità Disponibilità	Information protection Legal and compliance	Protection	L'organizzazione stabilisce, implementa e comunica a tutto il personale e le parti interessate politiche e procedure specifiche sulla privacy e la protezione delle PII.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.35	Revisione indipendente della sicurezza delle informazioni	Preventivo Correttivo	Riservatezza Integrità Disponibilità	Information security assurance	Governance and Ecosystem	L'organizzazione rivede, ad intervalli pianificati o quando si verificano cambiamenti significativi, l'approccio alla gestione della sicurezza delle informazioni e la sua implementazione, incluse le persone, processi e tecnologie.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.35	Revisione indipendente della sicurezza delle informazioni	Preventivo Correttivo	Riservatezza Integrità Disponibilità	Information security assurance	Governance and Ecosystem	L'organizzazione, tramite la sua direzione, pianifica e avvia revisioni indipendenti periodiche che includano le valutazioni circa le opportunità di miglioramento e la necessità di modifiche all'approccio alla sicurezza delle informazioni, compresa la politica di sicurezza delle informazioni, le politiche specifiche per argomento e altri controlli. Tali revisioni vengono effettuate da individui indipendenti dall'area in esame e i risultati delle revisioni vengono riportati alla direzione e al top management.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.35	Revisione indipendente della sicurezza delle informazioni	Preventivo Correttivo	Riservatezza Integrità Disponibilità	Information security assurance	Governance and Ecosystem	L'organizzazione effettua revisioni indipendenti quando le leggi e i regolamenti che riguardano l'organizzazione cambiano, quando si verificano incidenti significativi, quando l'organizzazione inizia ad usare un nuovo prodotto o servizio e quando cambia significativamente i controlli e le procedure di sicurezza delle informazioni.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.36	Conformità con le politiche, le regole e gli standard per la sicurezza delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Legal and compliance Information security assurance	Governance and Ecosystem	L'organizzazione rivede regolarmente la conformità con la politica di sicurezza delle informazioni con le politiche, le regole e gli standard specifici dell'argomento.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.36	Conformità con le politiche, le regole e gli standard per la sicurezza delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Legal and compliance Information security assurance	Governance and Ecosystem	L'organizzazione, nel caso in cui qualsiasi non conformità viene trovata come risultato della revisione, identifica le cause della non conformità, valuta la necessità di azioni correttive per raggiungere la conformità, implementa azioni correttive appropriate, rivede le azioni correttive intraprese per verificarne l'efficacia e identifica e eventuali carenze o deficienze		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
5	Controlli organizzativi	5.37	Procedure operative documentate	Preventivo Correttivo	Riservatezza Integrità Disponibilità	Asset management Physical security System and network security Application security Secure	Governance and Ecosystem Protection Defence	L'organizzazione documenta e rende disponibile al personale che ne ha bisogno le procedure operative per le strutture di elaborazione delle informazioni.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
6	Controlli sulle persone	6.1	Screening	Preventivo	Riservatezza Integrità Disponibilità	Human resource security	Governance and Ecosystem	L'organizzazione esegue controlli sul background di tutti i candidati a diventare parte del personale prima di entrare a far parte dell'organizzazione su base continuativa, prendendo in considerazione le leggi, i regolamenti ed etica proporzionati ai requisiti aziendali, alla classificazione delle informazioni e ai rischi percepiti.		SI	SI	SI	No	SI	Na	SI	No	SI	No	No	No	SI	No	SI

6	Controlli sulle persone	6.1	Screening	Preventivo	Riservatezza Integrità Disponibilità	Human resource security	Governance and Ecosystem	L'organizzazione effettua lo screening prendendo in considerazione tutta la legislazione pertinente in materia di privacy, protezione delle PII e relativa all'occupazione, includendo: - disponibilità di referenze soddisfacenti; - una verifica del curriculum vitae del candidato; - conferma delle qualifiche accademiche e professionali dichiarate; - verifica indipendente dell'identità; - verifica più dettagliata, come la revisione del casellario giudiziario.		SI	SI	SI	No	SI	No	SI	No	SI	No	No	No	SI	No	SI
6	Controlli sulle persone	6.2	Termini e condizioni d'impiego	Preventivo	Riservatezza Integrità Disponibilità	Human resource security	Governance and Ecosystem	L'organizzazione, tramite gli accordi contrattuali, dichiara le responsabilità del personale e dell'organizzazione per la sicurezza delle informazioni.		SI	SI	SI	No	SI	No	SI	No	SI	No	No	No	SI	No	SI
6	Controlli sulle persone	6.2	Termini e condizioni d'impiego	Preventivo	Riservatezza Integrità Disponibilità	Human resource security	Governance and Ecosystem	L'organizzazione prevede accordi di riservatezza o di non divulgazione con il personale che ha accesso a informazioni riservate, richiedendone la firma prima dell'autorizzazione ad accedere alle informazioni ed altri asset associati.		SI	SI	SI	No	SI	No	SI	No	SI	No	No	No	SI	No	SI
6	Controlli sulle persone	6.2	Termini e condizioni d'impiego	Preventivo	Riservatezza Integrità Disponibilità	Human resource security	Governance and Ecosystem	L'organizzazione prevede responsabilità per la classificazione ed il trattamento delle informazioni ricevute dalle parti interessate e azioni da intraprendere se il personale non rispetta i requisiti dell'organizzazione.		SI	SI	SI	No	SI	No	SI	No	SI	No	No	No	SI	No	SI
6	Controlli sulle persone	6.2	Termini e condizioni d'impiego	Preventivo	Riservatezza Integrità Disponibilità	Human resource security	Governance and Ecosystem	L'organizzazione si assicura che il personale accetti i termini e condizioni riguardanti la sicurezza delle informazioni. Tali termini e condizioni sono appropriati alla natura e all'estensione dell'accesso che avranno alle risorse associate ai sistemi e ai servizi di informazione.		SI	SI	SI	No	SI	No	SI	No	SI	No	No	No	SI	No	SI
6	Controlli sulle persone	6.3	Sensibilizzazione, educazione e formazione alla sicurezza delle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Human resource security	Governance and Ecosystem	L'organizzazione provvede a fornire al personale e le parti interessate appropriate sensibilizzazione e consapevolezza circa la sicurezza, istruzione e formazione e aggiornamenti sulla politica di sicurezza delle informazioni, insieme alle politiche e procedure specifiche dell'argomento.		SI	SI	SI	No	SI	No	SI	SI	SI	No	SI	No	SI	No	SI
6	Controlli sulle persone	6.4	Processo disciplinare	Preventivo	Riservatezza Integrità Disponibilità	Human resource security	Governance and Ecosystem	L'organizzazione formalizza e comunica l'esistenza di un processo disciplinare e lo attua contro il personale e altri parti interessate che hanno commesso una violazione della politica di sicurezza delle informazioni.		SI	SI	SI	No	SI	No	SI	No	SI	No	No	No	SI	No	SI
6	Controlli sulle persone	6.4	Processo disciplinare	Preventivo	Riservatezza Integrità Disponibilità	Human resource security	Governance and Ecosystem	L'organizzazione effettua un processo disciplinare che prevede una risposta graduale che prende in considerazione fattori quali: - la natura (chi, cosa quando, come) e la gravità della violazione e le sue conseguenze, - se l'infrazione è stata intenzionale (dolosa) o non intenzionale (accidentale), - se si tratta di una prima o ripetuta infrazione, - se il trasgressore è stato adeguatamente formato o meno Il processo disciplinare viene utilizzato anche come deterrente per impedire al personale ed altre parti interessate di violare la politica di sicurezza delle informazioni, le politiche e le procedure specifiche		SI	SI	SI	No	SI	No	SI	No	SI	No	No	No	SI	No	SI
6	Controlli sulle persone	6.5	Responsabilità dopo la cessazione o cambiamento di lavoro	Preventivo	Riservatezza Integrità Disponibilità	Human resource security Asset Management	Governance and Ecosystem	L'organizzazione definisce, applica e comunica al personale pertinente e alle parti interessate le responsabilità e i doveri di sicurezza delle informazioni che rimangono validi dopo la cessazione o il cambio di lavoro.		SI	SI	SI	No	SI	No	SI	No	SI	No	No	No	SI	No	SI
6	Controlli sulle persone	6.6	Accordi di riservatezza o di non divulgazione	Preventivo	Riservatezza Integrità Disponibilità	Human resource security Information protection Supplier relationships	Governance and Ecosystem	L'organizzazione identifica, documenta, rivede regolarmente e sottopone alla firma del personale e delle altri parti interessate accordi di riservatezza o di non divulgazione che riflettono le esigenze dell'organizzazione per la protezione delle informazioni.		SI	SI	SI	No	SI	SI	SI	No	SI	No	No	No	SI	No	SI
6	Controlli sulle persone	6.6	Accordi di riservatezza o di non divulgazione	Preventivo	Riservatezza Integrità Disponibilità	Human resource security Information protection Supplier relationships	Governance and Ecosystem	L'organizzazione, per identificare i requisiti di riservatezza o di non divulgazione, prende in considerazione i seguenti elementi: - una definizione delle informazioni da proteggere, - la durata prevista di un accordo, compresi i casi in cui può essere necessario mantenere riservatezza a tempo indeterminato o fino a quando l'informazione diventa disponibile al pubblico, - azioni richieste quando un accordo viene terminato, - le responsabilità e le azioni dei firmatari per evitare la divulgazione non autorizzata delle informazioni; la proprietà delle informazioni, i segreti commerciali e la proprietà intellettuale, - l'uso consentito delle informazioni riservate e i diritti del firmatario di utilizzare le informazioni, - il processo di notifica e segnalazione della divulgazione non autorizzata o della fuga di informazioni riservate, - i termini per le informazioni da restituire o distruggere al termine dell'accordo, - le azioni previste da intraprendere in caso di mancata rispetto dell'accordo.		SI	SI	SI	No	SI	SI	SI	No	SI	No	No	No	SI	No	SI
6	Controlli sulle persone	6.7	Lavoro a distanza	Preventivo	Riservatezza Integrità Disponibilità	Asset Management Information protection Physical security System and network security	Protection	L'organizzazione implementa misure di sicurezza quando il personale lavora in remoto per proteggere le informazioni accessibili, elaborate o memorizzate al di fuori dei locali dell'organizzazione.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	No	SI	No	SI
6	Controlli sulle persone	6.8	Segnalazione di eventi di sicurezza delle informazioni	Detective	Riservatezza Integrità Disponibilità	Information security event management	Defence	L'organizzazione fornisce un meccanismo per il personale per segnalare eventi di sicurezza delle informazioni osservati o sospetti attraverso canali appropriati e in modo tempestivo.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
7	Controlli fisici	7.1	Perimetri di sicurezza fisica	Preventivo	Riservatezza Integrità Disponibilità	Physical security	Protection	L'organizzazione definisce e utilizza perimetri di sicurezza per proteggere le aree che contengono informazioni e altre risorse associate.		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI
7	Controlli fisici	7.2	Accesso fisico	Preventivo	Riservatezza Integrità Disponibilità	Physical security Identity and Access Management	Protection	L'organizzazione protegge le aree sicure tramite appropriati controlli di ingresso e punti di accesso (ad esempio aree di consegna e di carico) limitando l'accesso ai siti e agli edifici solo al personale autorizzato e richiedendo a tutto il personale e alle parti interessate di indossare una qualche forma di identificazione visibile e di avvisare immediatamente il personale di sicurezza se incontrano visitatori senza scorta e chiunque senza un identificativo visibile.		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI
7	Controlli fisici	7.2	Accesso fisico	Preventivo	Riservatezza Integrità Disponibilità	Physical security Identity and Access Management	Protection	L'organizzazione stabilisce e attua un processo e meccanismi tecnici per la gestione dell'accesso alle aree in cui le informazioni vengono elaborate o conservate.		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI
7	Controlli fisici	7.2	Accesso fisico	Preventivo	Riservatezza Integrità Disponibilità	Physical security Identity and Access Management	Protection	L'organizzazione provvede ad autenticare l'identità dei visitatori con mezzi appropriati, registrandone data e ora di entrata ed uscita e concedendo l'accesso ai visitatori solo per scopi specifici e autorizzati e con istruzioni sui requisiti di sicurezza dell'area e sulle procedure di emergenza, sorvegliandoli a meno che non venga concessa un'eccezione esplicita		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI
7	Controlli fisici	7.2	Accesso fisico	Preventivo	Riservatezza Integrità Disponibilità	Physical security Identity and Access Management	Protection	L'organizzazione limita l'accesso alle aree di consegna e di carico dall'esterno dell'edificio a personale identificato e personale autorizzato		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI
7	Controlli fisici	7.2	Accesso fisico	Preventivo	Riservatezza Integrità Disponibilità	Physical security Identity and Access Management	Protection	L'organizzazione progetta le aree di consegna e di carico in modo che le consegne possano essere caricate e scaricate senza che il personale addetto alle consegne acceda senza autorizzazione alle altre parti dell'edificio e mette in sicurezza le porte esterne delle aree di consegna e di carico quando le porte delle aree riservate sono aperte. Inoltre, registra le consegne in arrivo secondo le procedure di gestione delle risorse all'ingresso nel sito		SI	SI	No	SI	SI	SI	SI	No	Na	SI	No	SI	SI	SI
7	Controlli fisici	7.3	Messa in sicurezza di uffici, stanze e strutture	Preventivo	Riservatezza Integrità Disponibilità	Physical security Asset Management	Protection	L'organizzazione progetta ed implementa la sicurezza fisica di uffici, stanze e strutture.		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI
7	Controlli fisici	7.4	Monitoraggio della sicurezza fisica	Preventivo Investigativo	Riservatezza Integrità Disponibilità	Physical security Asset Management	Protection Defence	L'organizzazione monitora continuamente i locali per l'accesso fisico non autorizzato tramite sistemi di sorveglianza che includono guardie, allarmi anti-intrusione, sistemi di monitoraggio video.		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI
7	Controlli fisici	7.5	Proteggere dalle minacce fisiche e ambientali	Preventivo	Riservatezza Integrità Disponibilità	Physical security	Protection	L'organizzazione progetta e implementa misure per la protezione contro le minacce fisiche e ambientali, come i disastri naturi e altre minacce fisiche intenzionali o non intenzioni alle infrastrutture		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI
7	Controlli fisici	7.6	Lavorare in aree sicure	Preventivo	Riservatezza Integrità Disponibilità	Physical security	Protection	L'organizzazione progetta ed implementa misure di sicurezza per lavorare in aree sicure.		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI
7	Controlli fisici	7.7	Clear desk and clear screen	Preventivo	Riservatezza	Physical security	Protection	L'organizzazione definisce e fa rispettare regole per una scrivania pulita e per uno schermo pulito, come ad esempio l'utilizzo di un meccanismo di blocco dello schermo e della tastiera quando il computer non è utilizzato dall'utente, l'archiviazione sicura di documenti e supporti di memorizzazioni rimovibili contenenti informazioni sensibili o cancellare le informazioni sensibili da lavagne o altri tipi di display quando non sono più necessari		SI	SI	No	SI	SI	SI	SI	No	Na	SI	No	SI	SI	SI

7	Controlli fisici	7.8	Posizionamento e protezione delle apparecchiature	Preventivo	Riservatezza Integrità Disponibilità	Physical security Asset Management	Protection	L'organizzazione provvede a collocare le attrezzature in modo sicuro e protetto, in modo da ridurre al minimo l'accesso non autorizzato o non necessario. Inoltre, adotta controlli per ridurre al minimo il rischio di potenziali minacce fisiche e ambientali e monitora le condizioni ambientali (come temperatura e umidità) che possano influire negativamente sul funzionamento degli impianti di elaborazione delle informazioni.		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI	SI
7	Controlli fisici	7.9	Sicurezza dei beni al di fuori della sede	Preventivo	Riservatezza Integrità Disponibilità	Physical security Asset Management	Protection	L'organizzazione protegge qualsiasi dispositivo utilizzato al di fuori dei locali dell'organizzazione che memorizza o elabora informazioni, compresi i dispositivi di proprietà dell'Ente che i dispositivi di proprietà privata e utilizzati per conto dell'organizzazione, richiedendo agli utenti e alle parti interessate di non lasciarli incustoditi in luoghi pubblici e di osservare le istruzioni dei produttori per proteggere le apparecchiature in ogni momento.		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI	SI
7	Controlli fisici	7.10	Supporti di memorizzazione	Preventivo	Riservatezza Integrità Disponibilità	Physical security Asset Management	Protection	L'organizzazione gestisce i supporti di archiviazione attraverso il loro ciclo di vita di acquisizione, uso, trasporto e smaltimento in conformità con lo schema di classificazione dell'organizzazione e i requisiti di gestione.		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI	SI
7	Controlli fisici	7.10	Supporti di memorizzazione	Preventivo	Riservatezza Integrità Disponibilità	Physical security Asset Management	Protection	L'organizzazione provvede a stabilire una politica specifica per argomento ed a comunicarla a tutte le parti interessate. Inoltre, tutti i supporti di memorizzazione sono conservati in un ambiente sicuro e protetto secondo la classificazione delle informazioni e protetti da minacce ambientali. Nel caso in cui la riservatezza e l'integrità delle informazioni sono considerati importanti, vengono utilizzate tecniche crittografiche per proteggere le informazioni contenute nei supporti di memorizzazione removibili.		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI	SI
7	Controlli fisici	7.10	Riutilizzo o smaltimento sicuro	Preventivo	Riservatezza Integrità Disponibilità	Physical security Asset Management	Protection	L'organizzazione stabilisce procedure per il riutilizzo o lo smaltimento sicuro dei supporti di memorizzazione per minimizzare il rischio di fuga di informazioni riservate a persone non autorizzate.		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI	SI
7	Controlli fisici	7.11	Servizi di supporto	Preventivo Investigativo	Integrità Disponibilità	Physical security	Protection	L'organizzazione protegge le strutture per l'elaborazione delle informazioni da interruzioni di corrente e altre interruzioni causate da guasti ai servizi di supporto, assicurandosi che le apparecchiature che supportano le utenze siano configurate, azionate e mantenute in conformità alle specifiche del produttore.		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI	SI
7	Controlli fisici	7.12	Sicurezza dei cablaggi	Preventivo	Riservatezza Disponibilità	Physical security	Protection	L'organizzazione protegge i cavi che trasportano energia, dati o servizi informativi di supporto da intercettazioni, interferenze o danni.		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI	SI
7	Controlli fisici	7.13	Manutenzione delle attrezzature	Preventivo	Riservatezza Integrità Disponibilità	Physical security Asset Management	Protection Resilience	L'organizzazione mantiene le attrezzature al fine di garantire la disponibilità, l'integrità e la riservatezza delle informazioni.		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI	SI
7	Controlli fisici	7.14	Smaltimento o riutilizzo delle attrezzature	Preventivo	Riservatezza	Physical security Asset Management	Protection	L'organizzazione verifica gli elementi dell'attrezzatura che contengono supporti di memorizzazione per garantire che tutti i dati sensibili e il software con licenza sono stati rimossi o sovrascritti in modo sicuro prima dello smaltimento o del riutilizzo.		SI	SI	No	SI	SI	SI	SI	No	No	SI	No	SI	SI	SI	SI
8	Controlli tecnologici	8.1	Dispositivi endpoint dell'utente	Preventivo	Riservatezza Integrità Disponibilità	Asset Management Information protection	Protection	L'organizzazione protegge le informazioni memorizzate, elaborate o accessibili tramite dispositivi endpoint dell'utente tramite una politica specifica sull'argomento che viene comunicata a tutto il personale interessato e considera: - il tipo di informazione e il livello di classificazione che i dispositivi endpoint dell'utente possano gestire, elaborare, archiviare o supportare. - registrazione dei dispositivi endpoint dell'utente, - requisiti per la protezione fisica, - restrizione dell'installazione del software, - requisiti per il software dei dispositivi endpoint dell'utente, - regole per la connessione a servizi di informazione, reti pubbliche o qualsiasi altra rete, - controlli di accesso, - crittografia dei dispositivi di memorizzazione, - protezione contro il malware, disabilitazione, cancellazione o blocco a distanza, - backup, - utilizzo di servizi web e applicazioni web, - utilizzo di dispositivi removibili.		SI	SI	No	No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
8	Controlli tecnologici	8.1	Dispositivi endpoint dell'utente - Responsabilità dell'utente	Preventivo	Riservatezza Integrità Disponibilità	Asset Management Information protection	Protection	L'organizzazione mette al corrente tutti gli utenti circa i requisiti di sicurezza e le procedure per la protezione degli endpoint dell'utente, così come delle loro responsabilità nell'implementazione di tali misure di sicurezza.		SI	SI	No	No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
8	Controlli tecnologici	8.1	Dispositivi endpoint dell'utente - Uso di dispositivi personali	Preventivo	Riservatezza Integrità Disponibilità	Asset Management Information protection	Protection	L'organizzazione, nei casi in cui consente l'utilizzo di dispositivi personali, richiede la separazione dell'uso personale e aziendale dei dispositivi, compreso l'uso di software per supportare tale separazione e fornisce l'accesso alle informazioni aziendali solo dopo che gli utenti hanno confermato la visione delle loro responsabilità circa il corretto utilizzo.		SI	SI	No	No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
8	Controlli tecnologici	8.1	Dispositivi endpoint dell'utente - Connessioni wireless	Preventivo	Riservatezza Integrità Disponibilità	Asset Management Information protection	Protection	L'organizzazione stabilisce procedure per la configurazione delle connessioni wireless sui dispositivi, l'uso di connessioni wireless o cablate con larghezza di banda appropriata in conformità con le relative politiche specifiche dell'argomento.		No	SI	SI	No	SI	SI	SI	No	No	No	No	SI	SI	No	SI
8	Controlli tecnologici	8.2	Diritti di accesso privilegiato	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione gestisce e limita l'assegnazione e l'uso di diritti di accesso privilegiati tramite un processo di autorizzazione che identifica gli utenti che necessitano di diritti di accesso privilegiati per ogni sistema o processo ed assegna i diritti di accesso privilegiato secondo necessità.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.3	Restrizione dell'accesso alle informazioni	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione limita l'accesso alle informazioni ed altri asset associati in conformità con le politiche stabilite per ogni argomento, impedendo l'accesso a informazioni sensibili da parte di identità sconosciute o in modo anonimo, controllando a quali dati può accedere un particolare utente e quali utenti hanno accesso alla lettura, scrittura, cancellazione delle informazioni.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.4	Accesso al codice sorgente	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management Application security Secure configuration	Protection	L'organizzazione gestisce in modo appropriato l'accesso in lettura e scrittura al codice sorgente, agli strumenti di sviluppo e alle librerie software.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.5	Autenticazione sicura	Preventivo	Riservatezza Integrità Disponibilità	Identity and access management	Protection	L'organizzazione implementa le tecnologie e le procedure di autenticazione sicura in base alle restrizioni di accesso alle informazioni e alla politica sul controllo degli accessi, considerando misure come, ad esempio, mostrare un avviso generale che avverta che il sistema o l'applicazione o il servizio sono accessibili solo da utenti autorizzati o convalidare le informazioni di accesso solo dopo aver completato tutti i passaggi o proteggere contro tentivi di accesso brute force.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.6	Gestione della capacità	Preventivo Investigativo	Integrità Disponibilità	Continuity	Governance and Ecosystem Protection	L'organizzazione monitora e regola l'uso delle risorse in linea con le esigenze di capacità attuale e prevista, tenendo conto delle criticità dei sistemi e dei processi interessati ed effettuando stress test di sistemi e servizi per confermare che una capacità del sistema sia disponibile per soddisfare i requisiti di picco delle prestazioni.		No	SI	No	SI	SI	No	SI	SI	SI	SI	No	No	SI	SI	SI
8	Controlli tecnologici	8.7	Protezione contro i malware	Preventivo Investigativo Correttivo	Riservatezza Integrità Disponibilità	System and network security Information protection	Protection Difence	L'organizzazione effettua e basa la protezione contro i malware su software di rilevamento e riparazione, sulla consapevolezza della sicurezza delle informazioni da parte del personale e un appropriato accesso al sistema e sul controllo di gestione dei cambiamenti.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.8	Gestione delle vulnerabilità tecniche	Preventivo	Riservatezza Integrità Disponibilità	Threat and vulnerability management	Governance and Ecosystem Protection Difence	L'organizzazione ottiene informazioni circa le vulnerabilità tecniche dei sistemi informativi in uso, valuta l'esposizione dell'Ente a tali vulnerabilità e adotta misure per mitigarle.		SI	SI	No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
8	Controlli tecnologici	8.9	Identificazione delle vulnerabilità tecniche	Preventivo	Riservatezza Integrità Disponibilità	Threat and vulnerability management	Governance and Ecosystem Protection Difence	L'organizzazione ha un inventario accurato degli asset all'interno del quale sono indicati il fornitore del software, il nome del software e i numeri di versione, lo stato attuale di implementazione, la persona o le persone che lo hanno installato e la persona o persone responsabili del software all'interno dell'Ente.		SI	SI	No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
8	Controlli tecnologici	8.8	Identificazione delle vulnerabilità tecniche	Preventivo	Riservatezza Integrità Disponibilità	Threat and vulnerability management	Governance and Ecosystem Protection Difence	L'organizzazione definisce e stabilisce i ruoli e le responsabilità associate alla gestione delle vulnerabilità tecniche, compreso il monitoraggio e la valutazione del rischio e richiede ai fornitori di sistemi informativi di garantire la segnalazione, la gestione e la divulgazione delle vulnerabilità, compresi i requisiti nei contratti applicabili. Inoltre, utilizza strumenti di scansione delle vulnerabilità adatti alle tecnologie in uso e conduce penetration test pianificati, documentati e ripetibili e traccia l'uso di librerie di terze parti e il codice sorgente per le vulnerabilità.		SI	SI	No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
8	Controlli tecnologici	8.8	Valutazione delle vulnerabilità tecniche	Preventivo	Riservatezza Integrità Disponibilità	Threat and vulnerability management	Governance and Ecosystem Protection Difence	L'organizzazione analizza e verifica i rapporti per determinare quale attività di risposta e rimedio sia necessario e, una volta identificata una potenziale vulnerabilità tecnica, identifica i rischi associati e le azioni da intraprendere (ad esempio l'aggiornamento dei sistemi vulnerabili o l'applicazione di altri controlli).		SI	SI	No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

A	Controlli tecnologici	8.8	Adottare misure appropriate per affrontare le vulnerabilità tecniche	Preventivo	Riservatezza Integrità Disponibilità	Threat and vulnerability management	Governance and Ecosystem Protection Defence	L'organizzazione implementa un processo di aggiornamento del software per assicurare che le più aggiornate patch approvate e gli aggiornamenti delle applicazioni siano installati per tutti i software autorizzati e, nel caso in cui siano necessarie modifiche, il software originale dovrebbe essere conservat e le modifiche applicate ad una copia designata. Tutte le modifiche vengono completamente testate e documentate, in modo che possano essere riapplicate a futuri aggiornamenti del software.		SI	SI	No	SI	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
B	Controlli tecnologici	8.9	Gestione della configurazioni	Preventivo	Riservatezza Integrità Disponibilità	Secure configuration	Protection	L'organizzazione stabilisce,documenta, implementa, monitora e rivede le configurazioni, comprese quelle di sicurezza, di hardware, software, servizi e reti.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
E	Controlli tecnologici	8.9	Gestione delle configurazioni	Preventivo	Riservatezza Integrità Disponibilità	Secure configuration	Protection	L'organizzazione definisce modelli standard per la configurazione sicura di hardware, software, servizi e reti considerando livelli di protezione necessari per determinare un livello sufficiente di sicurezza e considerando la fattibilità e l'applicabilità delle configurazioni di sicurezza nel contesto dell'Ente. Tali modelli vengono rivisti periodicamente e aggiornati quando nuove minacce o vulnerabilità vengono identificate o quando vengono introdotte nuove versioni di software o hardware.		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
A	Controlli tecnologici	8.9	Gestione delle configurazioni	Preventivo	Riservatezza Integrità Disponibilità	Secure configuration	Protection	L'organizzazione mantiene un registro di tutti i cambiamenti di configurazione, archiviandolo in modo sicuro. Tali registri contengono informazioni aggiornate sul proprietario dell'asset, sulla data dell'ultimo cambio di configurazione, la versione del modello di configurazione e la relazione con le configurazioni di altri asset		SI	SI	No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
E	Controlli tecnologici	8.9	Monitoraggio delle configurazioni	Preventivo	Riservatezza Integrità Disponibilità	Secure configuration	Protection	L'organizzazione monitora le configurazioni con un set completo di strumenti di gestione del sistema su base regolare al fine di verificare le impostazioni di configurazione, valutare la forza delle password e valutare le attività svolte.		SI	SI	No	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
A	Controlli tecnologici	8.10	Cancellazione delle informazioni	Preventivo	Riservatezza	Information protection Legal and compliance	Protection	L'organizzazione provvede a cancellare le informazioni memorizzate nei sistemi informativi, nei dispositivi o in qualsiasi altro supporto di memorizzazione quando non sono più necessarie, selezionando un metodo di cancellazione in conformità con i requisiti aziendali e tenendo conto delle pertinenti norme di sicurezza.		No	SI	SI	No	SI	No	SI	SI	No	No	SI	SI	SI	No	SI
E	Controlli tecnologici	8.10	Cancellazione delle informazioni	Preventivo	Riservatezza	Information protection Legal and compliance	Protection	L'organizzazione, quando utilizza fornitori di servizi di cancellazione delle informazioni, si assicura di ottenere da loro la prova della cancellazione delle informazioni. Quando invece utilizza fornitori di servizi di conservazione delle informazioni per suo conto, L'organizzazione include requisiti sulla cancellazione delle informazioni negli accordi con i terzi		No	SI	SI	No	SI	No	SI	SI	No	No	SI	SI	SI	No	SI
E	Controlli tecnologici	8.11	Data Masking	Preventivo	Riservatezza	Information protection	Protection	L'organizzazione utilizza tecniche di pseudonimizzazione o anonimizzazione dei dati quando vuole proteggere dati sensibili (come ad esempio le PII).		SI	SI	SI	No	SI	No	SI	SI	SI	No	SI	No	SI	No	SI
E	Controlli tecnologici	8.12	Prevenzione dalla perdita di dati	Preventivo Investigativo	Riservatezza	Information protection	Protection Defence	L'organizzazione identifica e classifica le informazioni per proteggerle dalla fuga di dati e monitora i canali di fuga dei dati, agendo per prevenire la fuga di informazioni (ad esempio, mettendo in quarantena le e-mail contenenti informazioni sensibili		No	SI	SI	No	SI	No	SI	SI	SI	No	No	No	SI	No	SI
A	Controlli tecnologici	8.13	Backup delle informazioni	Correttivo	Integrità Disponibilità	Continuity	Protection	L'organizzazione mantiene e testa regolarmente le copie di backup delle informazioni, software e sistemi in conformità con la politica di Backup.		SI	SI	SI	SI	SI	No	SI	SI	SI	SI	No	SI	SI	SI	SI
E	Controlli tecnologici	8.13	Backups delle informazioni	Correttivo	Integrità Disponibilità	Continuity	Protection	L'organizzazione sviluppa piani di backup considerando di produrre registrazioni accurate e complete delle copie di backup e procedure di ripristino, di riflettere i requisiti aziendali e di sicurezza delle informazioni, immagazzinare i backup in un luogo remoto sicuro e protetto e a una distanza sufficiente per sfuggire a qualsiasi danno nel sito principale, effettuare test regolari sui supporti di backup per garantire che si possa fare affidamento su di essi in un caso di emergenza, testare le capacità di ripristino dei dati di backup su un sistema di prova e non sovrascrivendo l'originale e facendo attenzione a garantire che la perdita involontaria di dati sia rilevata prima che il backup sia effettuato.		SI	SI	SI	SI	SI	No	SI	SI	SI	SI	No	SI	SI	SI	SI
A	Controlli tecnologici	8.14	Ridondanza delle strutture di elaborazione delle informazioni	Preventivo	Disponibilità	Continuity Asset management	Protection Resilience	L'organizzazione progetta ed implementa l'architettura dei sistemi con un'appropriata ridondanza per soddisfare i requisiti identificati dall'Ente e viene messa in atto un meccanismo per avvisare l'organizzazione di qualsiasi guasto nelle strutture di elaborazione delle informazioni, per consentire l'esecuzione della procedura pianificata e per mantenere la disponibilità continua mentre le strutture di elaborazione delle informazioni vengono riparate o sostituite.		No	SI	No	No	No	No	No	SI	No	SI	No	No	No	SI	SI
E	Controlli tecnologici	8.15	Logging	Investigativo	Riservatezza Integrità Disponibilità	Information security event management	Protection Defence	L'organizzazione produce, conserva, protegge ed analizza i log che registrano attività, eccezioni, guasti ed altri eventi rilevanti. I log includono: - ID utente, - attività del sistema, - date, orari e dettagli degli eventi rilevanti, - identità del dispositivo, - indirizzi e protocolli di rete.		No	SI	No	No	No	No	No	SI	No	SI	No	No	No	SI	SI
A	Controlli tecnologici	8.15	Logging	Investigativo	Riservatezza Integrità Disponibilità	Information security event management	Protection Defence	L'organizzazione considera i seguenti eventi per la registrazione: - tentativi di accesso al sistema riusciti e respinti, - tentativi di accesso ai dati e ad altre risorse, riusciti e respinti, - modifiche alla configurazione del sistema, - uso di privileg, - uso di programmi di utilità e applicazioni, - file consultati e tipo di accesso, compresa la cancellazione di importanti file di dati, - allarmi generati dal sistema di controllo degli accessi, - attivazione e disattivazione dei sistemi di sicurezza, come i sistemi antivirus e di rilevamento delle intrusioni, - creazione, modifica o cancellazione di identità, - transazioni eseguite dagli utenti nelle applicazioni		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	No
E	Controlli tecnologici	8.15	Protezione dei log	Investigativo	Riservatezza Integrità Disponibilità	Information security event management	Protection Defence	L'organizzazione non concede il permesso di cancellare o disattivare i registri delle proprie attività, neanche agli utenti con diritti di accesso privilegiato.		SI	SI	SI	No	SI	SI	SI	SI	SI	SI	No	SI	SI	SI	No	No
A	Controlli tecnologici	8.15	Analisi dei log	Investigativo	Riservatezza Integrità Disponibilità	Information security event management	Protection Defence	L'organizzazione prsovede ad effettuare l'analisi dei log, copre l'analisi e l'interpretazione degli eventi di sicurezza delle informazioni, per aiutare a identificare attività insolite o comportamenti anomali che possono rappresentare indicatori di compromissione.		SI	SI	SI	No	SI	SI	SI	SI	SI	SI	No	SI	SI	SI	No	No
E	Controlli tecnologici	8.16	Attività di monitoraggio	Investigativo Correttivo	Riservatezza Integrità Disponibilità	Information security event management	Defence	L'organizzazione effettua il monitoraggio di reti, sistemi e applicazioni per identificare comportamenti anomali e azioni appropriate da intraprendere per valutare potenziali incidenti di sicurezza delle informazioni. Vengono tenute in considerazione: - traffico di rete, di sistema e applicativo in uscita e in entrata, - accesso ai sistemi, server, apparecchiature di rete, sistema di monitoraggio, applicazioni critiche, etc. - file di configurazione di sistema e di rete di livello critico o amministrativo, - registri da strumenti di sicurezza, - registri di eventi relativi all'attività di sistema e di rete, - controllare che il codice in esecuzione sia autorizzato a girare nel sistema e che non sia stato manomesso. - l'uso delle risorse e le loro prestazioni		SI	SI	SI	SI	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
A	Controlli tecnologici	8.17	Sincronizzazione degli orologi	Investigativo	Integrità	Information security event management	Protection Defence	L'organizzazione sincronizza gli orologi dei sistemi di elaborazioni utilizzati con fonti di tempo appropriate.		No	SI	No	No	SI	SI	No	No	SI	No	No	No	SI	No	No
E	Controlli tecnologici	8.18	Utilizzo di programmi di utilità privilegiati	Preventivo	Riservatezza Integrità Disponibilità	System and network security Secure configuration	Protection	L'organizzazione limita e controlla l'utilizzo di programmi di utilità che possono essere in grado di scavalcare i controlli del sistema		SI	SI	SI	SI	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
A	Controlli tecnologici	8.19	Installazione di software su sistemi operativi	Preventivo	Riservatezza Integrità Disponibilità	Secure configuration Application security	Protection	L'organizzazione implementa procedure e misure per gestire in modo sicuro l'installazione di software su sistemi operativi, come ad esempio l'esecuzione degli aggiornamenti del software operativo solo previa autorizzazione della direzione o permettere l'installazione e l'aggiornamento del software solo dopo aver effettuato con successo test approfonditi.		No	SI	No	SI	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
A	Controlli tecnologici	8.20	Sicurezza delle reti	Preventivo Investigativo	Riservatezza Integrità Disponibilità	System and network security	Protection	L'organizzazione protegge, gestisce e controlla le reti e i dispositivi di rete per proteggere le informazioni nei sistemi e applicazioni. Implementa controlli finalizzati a stabilire le responsabilità e le procedure per la gestione delle apparecchiature e dei dispositivi di rete, mantenere aggiornata la documentazione, compresi i diagrammi di rete e i file di configurazione dei dispositivi, stabilire controlli per salvaguardare la riservatezza e l'integrità dei dati che passano su reti pubbliche, reti di terzi o su reti senza fili.		No	SI	No	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI

8	Controlli tecnologici	8.21	Sicurezza dei servizi di rete	Preventivo	Riservatezza Integrità Disponibilità	System and network security	Protection	L'organizzazione identifica, implementa e monitora i meccanismi di sicurezza, i livelli di servizio e i requisiti di servizio dei servizi di rete, assicurandosi che i fornitori di servizi di rete implementino queste misure. Inoltre, monitora regolarmente la capacità del fornitore di servizi di rete di gestire i servizi concordati in modo sicuro.		No	SI	No	SI	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.22	Segregazione delle reti	Preventivo	Riservatezza Integrità Disponibilità	System and network security	Protection	L'organizzazione segrega i gruppi di servizi d'informazione, utenti e sistemi di informazione nelle reti dell'organizzazione, dividendo le grandi reti in domini di rete separati e separandoli dalla rete pubblica.		No	SI	No	SI	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.23	Filtraggio del web	Preventivo	Riservatezza Integrità Disponibilità	System and network security	Protection	L'organizzazione gestisce l'accesso a siti web esterni per ridurre l'esposizione a contenuti dannosi, come ad esempio bloccando l'indirizzo IP o il dominio del sito web in questione		No	SI	No	SI	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.24	Uso della crittografia	Preventivo	Riservatezza Integrità Disponibilità	Secure configuration	Protection	L'organizzazione assicura un uso corretto ed efficace della crittografia per proteggere la riservatezza, l'autenticità o l'integrità delle informazioni secondo i requisiti di business e di sicurezza delle informazioni e prendendo in considerazione i requisiti legali, statutari, normativi e contrattuali relativi alla crittografia.		SI	SI	No	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.24	Gestione delle chiavi crittografiche	Preventivo	Riservatezza Integrità Disponibilità	Secure configuration	Protection	L'organizzazione assicura una gestione appropriata delle chiavi crittografiche tramite processi sicuri per generare, memorizzare, archiviare, recuperare, distribuire, ritirare e distruggere le chiavi crittografiche.		SI	SI	No	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.25	Ciclo di vita di sviluppo sicuro	Preventivo	Riservatezza Integrità Disponibilità	Application security System and network security	Protection	L'organizzazione stabilisce ed applica norme per lo sviluppo sicuro di software e sistemi.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.26	Requisiti di sicurezza delle applicazioni	Preventivo	Riservatezza Integrità Disponibilità	Application security System and network security	Protection Defence	L'organizzazione identifica, specifica ed approva i requisiti di sicurezza delle informazioni quando si sviluppano o si acquistano applicazioni. Tali requisiti includono, a seconda dei casi: - il livello di fiducia nell'identità dell'entità, - identificazione del tipo di informazioni e del livello di classificazione che l'applicazione deve trattare, - necessità di segregazione e livello di accesso ai dati, - resilienza contro attacchi malevoli, - requisiti legali, statutari e normativi, - esigenze di privacy		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
8	Controlli tecnologici	8.26	Requisiti di sicurezza delle applicazioni - Servizi transazionali	Preventivo	Riservatezza Integrità Disponibilità	Application security System and network security	Protection Defence	L'organizzazione identifica ulteriori requisiti di sicurezza delle informazioni per le applicazioni che offrono servizi transazionali, come ad esempio: - processi di autorizzazione associati a chi può approvare i contenuti, emettere o firmare documenti chiave, - la riservatezza e l'integrità di qualsiasi transazione, - requisiti su quanto tempo mantenere riservata una transazione;		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.26	Requisiti di sicurezza delle applicazioni - Applicazioni per ordini e pagamenti elettronici	Preventivo	Riservatezza Integrità Disponibilità	Application security System and network security	Protection Defence	L'organizzazione identifica ulteriori requisiti di sicurezza delle informazioni per le applicazioni che offrono servizi di ordini e pagamenti elettronici, come ad esempio: - evitare la perdita o la duplicazione delle informazioni sulle transazioni; - memorizzare i dettagli della transazione al di fuori di qualsiasi ambiente pubblicamente accessibile.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.27	Architettura di sistema sicuri e principi di ingegneria	Preventivo	Riservatezza Integrità Disponibilità	Application security Systems and network security	Protection	L'organizzazione stabilisce, documenta, mantiene ed applica i principi per la progettazione di sistemi sicure a tutte le attività di sviluppo dei sistemi informativi.		No	SI	SI	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.28	Codifica sicura	Preventivo	Riservatezza Integrità Disponibilità	Application security System and network security	Protection	L'organizzazione applica i principi di codifica sicura allo sviluppo del software, sia per i nuovi sviluppi che negli scenari di riutilizzo. Inoltre, i processi di codifica sicura vengono estesi per coprire i componenti software di terze parti e per software open-source.		No	SI	SI	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.28	Codifica sicura	Preventivo	Riservatezza Integrità Disponibilità	Application security System and network security	Protection	L'organizzazione monitora le minacce del mondo relare e le informazioni agiornati sulle vulnerabilità del software per guidare i principi di codifica sicura dell'organizzazione attraverso un continuo miglioramento e apprendimento.		SI	SI	SI	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.29	Test di sicurezza nello sviluppo e nell'accettazione	Preventivo	Riservatezza Integrità Disponibilità	Application security Information security assurance System and network security	Protection	L'organizzazione definisce ed implementa processi di test di sicurezza nel ciclo di vita dello sviluppo, che sono parte integrante dei test per sistemi o componenti. Tali test dovrebbero includere funzioni di sicurezza e uso di crittografia, codifica sicura, configurazioni sicure.		No	SI	No	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.29	Test di sicurezza nello sviluppo e nell'accettazione	Preventivo	Riservatezza Integrità Disponibilità	Application security Information security assurance System and network security	Protection	I piani di test vengono determinati utilizzando una serie di criteri e l'estensione dei test è proporzionata all'importanza, alla natura del sistema e all'impatto potenziale del cambiamento introdotto.		No	SI	No	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.30	Sviluppo in outsourcing	Preventivo Investigativo	Riservatezza Integrità Disponibilità	Application security Supplier relationships security System and network security	Governance and Ecosystem Protection	L'organizzazione dirige, monitora e rivede le attività relative allo sviluppo del sistema in outsourcing, comunicando e concordando i requisiti e le aspettative, e monitorando e riesaminando continuamente se la del lavoro esternalizzato soddisfa queste aspettative.		No	SI	No	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.31	Separazione degli ambienti di sviluppo, test e produzione	Preventivo	Riservatezza Integrità Disponibilità	Application security System and network security	Protection	L'organizzazione provvede a separare e proteggere gli ambienti di sviluppo, test e produzione per prevenire problemi di produzione		No	SI	No	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.32	Change Management	Preventivo	Riservatezza Integrità Disponibilità	Application security System and network security	Protection	L'organizzazione prevede procedure di gestione dei cambiamenti quando avvengono cambiamenti alle strutture di elaborazione delle informazioni per garantire la riservatezza, l'integrità e la disponibilità delle informazioni nelle strutture di elaborazione delle informazioni e nei sistemi informativi per l'intero ciclo di vita dello sviluppo del sistema, dalle prime fasi di progettazione fino a tutti i successivi sforzi.		No	SI	No	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.33	Informazioni sui test	Preventivo	Riservatezza Integrità	Information protection	Protection	L'organizzazione seleziona, protegge e gestisce le informazioni dei test in modo appropriato, al fine di garantire l'affidabilità dei risultati dei test e la riservatezza delle informazioni operative pertinenti.		No	SI	No	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI
8	Controlli tecnologici	8.34	Protezione dei sistemi informativi durante i test di audit	Preventivo	Riservatezza Integrità	System and network security Information protection	Governance and Ecosystem Protection	L'organizzazione pianifica e concorda i test di audit e altre attività di garanzia che coinvolgono la valutazione dei sistemi operativi		No	SI	No	No	SI	SI	SI	SI	SI	No	SI	SI	SI	No	SI

REGIONE LAZIO

Risultato della Valutazione d'impatto del rischio per il trattamento - VDR e Valutazione del DPO

Nel caso in cui il rischio del trattamento è alto, sarà necessario avviare la consultazione preventiva dell'Autorità di Controllo, come disciplinato dal Processo per la realizzazione della valutazione d'impatto sulla protezione dei dati.

Rischio del trattamento
2. Medio Basso
per il trattamento non è necessario sviluppare la DPIA e può essere avviato senza consultazione preventiva dell'autorità di controllo

Parere del DPO	
Possibilità di iniziare/continuare l'attività di trattamento	
Motivazione	
Note	

REGIONE LAZIO

Classificazione del Rischio

Rischio		Impatto			
		Trascurabile	Limitato	Significativo	Massimo
Probabilità	Trascurabile	1. Basso	1. Basso	2. Medio Basso	2. Medio Basso
	Limitata	1. Basso	2. Medio Basso	3. Medio Alto	3. Medio Alto
	Significativa	2. Medio Basso	2. Medio Basso	3. Medio Alto	4. Alto
	Massima	2. Medio Basso	2. Medio Basso	4. Alto	4. Alto

REGIONE LAZIO

Questionario per la Valutazione Preliminare del trattamento ai fini dell'obbligatorietà dello sviluppo della DPIA (ex art.35 RGDP)

Questionario di valutazione preliminare del trattamento ai fini della verifica sull'obbligatorietà della DPIA

Vedere le specifiche istruzioni nel foglio *Istruzioni* .

Il Questionario si basa sui 9 criteri definiti nel WP 248 rev.01 del 4 ottobre 2017 del Gruppo di Lavoro Articolo 29 per la protezione dati (due o più criteri valorizzati con "SI" rendono obbligatoria DPIA) e sui i 12 criteri definiti nell'allegato 1 al provvedimento n. 467 dell'11 ottobre 2018 del Garante (uno o più criteri valorizzati con "SI" rende obbligatoria la DPIA). Nei casi dubbi o nei casi in cui sia presente almeno 1 criterio selezionato, anche se il questionario non rileva l'obbligatorietà dello sviluppo della DPIA occorre valutare attentamente l'impatto del trattamento sui diritti e le libertà degli interessati e l'opportunità di effettuare comunque cautelativamente la DPIA utilizzando anche il risultato della valutazione del rischio presente nel modulo "Risultato".

ID (questo)	Obbligatorietà	Domanda	Risposta	Valore Risposta	DPIA necessaria
1	provv.467-tratt. 01	Il trattamento di dati personali, implica valutazioni o scoring su larga scala? Riguarda un trattamento che comporta la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad *"aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato* "?	No		
2	provv.467-tratt. 02	Il trattamento di dati personali contempla trattamenti automatizzati finalizzati ad assumere decisioni che producono *"effetti giuridici"* oppure che incidono *"in modo analogo significativamente"* sull'interessato? (sono comprese le decisioni che impediscono di esercitare un diritto o avvalersi un bene o un servizio o continuare ad esser parte un contratto in essere, e ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).	No		
3	provv.467-tratt. 03	Il trattamento di dati personali viene effettuato mediante utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati? (compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche I trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.)	No		
4	provv.467-tratt. 04	Il trattamento dei dati personali prevede trattamenti su larga scala aventi carattere estremamente personale (v. WP 248, rev. 01)? In tale obbligatorietà si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazionecomporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).	No		
5	provv.467-tratt. 05	Il trattamento di dati personali viene effettuato nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi videosorveglianza e geolocalizzazione) dai quali derivi la possibilità effettuare un controllo a distanza dell'attività dei dipendenti della Giunta della Regione Lazio? (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri n. 3, 7 e 8)	No		No
6	provv.467-tratt. 06	Il trattamento in esame prevede trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)?	No		
7	provv.467-tratt. 07	Il trattamento di dati personali viene effettuato attraverso l'uso di tecnologie innovative? Anche con particolari misure di carattere organizzativo (es: IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogni qualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .	No		
8	provv.467-tratt. 08	Il trattamento di dati personali comporta scambio di dati tra diversi titolari su larga scala con modalità telematiche?	No		
9	provv.467-tratt. 09	Il trattamento di dati personali viene svolto mediante interconnessione, combinazione o raffronto informazioni? Sono compresi i trattamenti che prevedono l'incrocio dei dati consumo beni digitali con dati di pagamento (es. mobile payment).	No		
10	provv.467-tratt. 10	Il trattamento dei dati contempla trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure dati relativi a condanne penali e a reati cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse?	No		
11	provv.467-tratt. 11	Il trattamento dei dati include trattamenti sistematici di dati biometrici? Tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività trattamento.	No		
12	provv.467-tratt. 12	Il trattamento dei dati contempla trattamenti sistematici di dati genetici? Tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività trattamento.	No		
ID (questo)	Obbligatorietà	Domanda	Risposta	Valore Risposta	DPIA necessaria
13	WP248-criterio 1)	Nel trattamento di dati personali viene effettuata una valutazione o assegnazione di un punteggio? Per valutazione o assegnazione di un punteggio si include la profilazione e previsione,ed in particolare anche nel caso in cui si prendono in considerazione "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (considerando 71 e 91).	No		
14	WP248-criterio 2)	Il trattamento di dati personali viene effettuato mediante processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente? Il trattamento mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche" (articolo 35, paragrafo 3, lettera a)]? *Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti delle persone. Il trattamento che non ha effetto o ha soltanto un effetto limitato sulle persone non risponde a questo criterio specifico. Ulteriori spiegazioni in merito a queste nozioni saranno fornite nelle linee guida sulla profilazione che saranno pubblicate prossimamente dal WP29*	No		
15	WP248-criterio 3)	Il trattamento di dati personali contempla monitoraggio sistematico e questo viene utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" [anche rif. articolo 35, paragrafo 3, lettera c)]? Si ricorda che questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico)	No		
16	WP248-criterio 4)	Il trattamento di dati personali contempla dati sensibili o dati aventi carattere altamente personale? Questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10. *Un esempio: quello di un ospedale generale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli dei trasgressori. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali documenti personali, messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone e che che consentono di tenere traccia del proprio stile di vita*	Sì		
17	WP248-criterio 5)	Il trattamento di dati personali viene effettuato su larga scala? Il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala: a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; c. la durata, ovvero la persistenza, dell'attività di trattamento; d. la portata geografica dell'attività di trattamento	No		Sì
18	WP248-criterio 6)	Il trattamento di dati personali implica creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato?	No		
19	WP248-criterio 7)	Il trattamento contempla dati personali relativi a interessati vulnerabili? In rif. al considerando 75 RGPD, il trattamento di questo tipo di dati è un criterio ai fini della DPIA in quanto è più accentuato lo squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (I quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;	Sì		
20	WP248-criterio 8)	Il trattamento di dati personali contempla l'uso innovativo o l'applicazione di nuove soluzioni tecnologiche od organizzative, come la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc...? Rispondere a tale questione ricordando che il regolamento generale sulla protezione dei dati chiarisce (articolo 35, paragrafo 1 e considerando 89 e 91) che l'uso di una nuova tecnologia, definita "in conformità con il grado di conoscenze tecnologiche raggiunto" (considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi. *Un esempio potrebbero essere alcune applicazioni di "Internet delle cose" potrebbero avere un impatto significativo sulla vita quotidiana e sulla vita privata delle persone e, di conseguenza, richiedono la realizzazione di una valutazione d'impatto sulla protezione dei dati.*	No		
21	WP248-criterio 9)	Il trattamento di dati personali in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" ? Nel rispondere a tale quesito, si ricorda che, ai sensi dell'art.22 e considerando 91 RGPD, ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto. *Un esempio di ciò è rappresentato dal caso in cui una banca esamina i suoi clienti (screening dei clienti) rispetto a una banca dati di riferimento per il credito al fine di decidere se offrire loro un prestito o meno*	No		

Modulo di valutazione d'impatto del rischio per il trattamento - DPIA (ex art.35 RGPD)		
ID	Sezioni della DPIA	Descrizioni/Risposte
a.	Informazioni sul trattamento	
a.1	Nome del DPO/RPD	Vasile Diaconescu
a.2	Posizione del DPO/RPD	
a.3	Parere del DPO/RPD	
a.4	Richiesta del parere degli interessati	
a.5	Motivazione della mancata richiesta del parere degli interessati	
b.	Contesto - Panoramica del trattamento	
b.1	Quali sono le responsabilità connesse al trattamento?	Il whistleblower si assume la responsabilità rispetto a quanto denunciato. L'RPCT è l'unico soggetto che, all'interno dell'Amministrazione, può ricevere le segnalazioni di whistleblowing, con le connesse garanzie di protezione del segnalante e vi provvede nel rispetto dei principi di imparzialità e riservatezza dei dati. Il fornitore: garantisce che la fornitura avverrà nel rispetto delle disposizioni di Legge in materia di protezione dei dati personali (D.Lgs.196/2003 e s.m.i.), con modalità idonee a garantirne la sicurezza e la riservatezza.
b.2	Ci sono standard applicabili al trattamento?	La piattaforma risponde nativamente alle Linee Guida emanate dall'ANAC attualmente in vigore e compliant a legge 179/2017, D.Lgs. 24/2023 e al GDPR. La piattaforma è conforme e rispetta gli standard: • ISO27001 "Erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaks" • ISO27017 controlli di sicurezza sulle informazioni basati sulla per i servizi Cloud • ISO27018 per la protezione dei dati personali nei servizi Public Cloud • Qualifica AGID • Certificazione CSA Star
b.3	Il trattamento dei dati contempla trattamenti sistematici di dati genetici?	NO
c.	Contesto - Dati, processo e risorse di supporto	
c.1	Quali sono i dati trattati?	dati comuni, particolari, giudiziari
c.2	Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?	Attraverso la compilazione di un questionario guidato, il segnalante (whistleblower) ha la possibilità di denunciare un illecito all'interno della propria struttura per il quale è stato testimone. La segnalazione di illecito è registrata attraverso l'utilizzo di una piattaforma. I dati raccolti sono necessari per la corretta valutazione della segnalazione a seguito di una prima fase di preistruttoria. Qualora, a seguito dell'attività svolta, il RPCT ravvisi elementi di manifesta infondatezza della segnalazione, ne dispone l'archiviazione con adeguata motivazione. Qualora, all'esito della verifica, la segnalazione risulti fondata, il Responsabile della prevenzione della corruzione e della trasparenza, in relazione alla natura della violazione, provvederà: a) a presentare denuncia all'autorità giudiziaria competente; b) a comunicare l'esito dell'accertamento al Responsabile della struttura di appartenenza dell'autore della violazione accertata, affinché provveda all'adozione dei provvedimenti di competenza, incluso, sussistendone i presupposti, l'esercizio dell'azione disciplinare; c) a comunicare l'esito dell'accertamento alla Direzione competente in materia di personale e alle strutture competenti ad adottare gli eventuali ulteriori provvedimenti e/o azioni che nel caso concreto si rendano necessari a tutela dell'Amministrazione. d) In caso di pluralità di segnalazioni da parte dello stesso dipendente, il RPCT potrà istruire la prima e archiviare le successive, aventi il medesimo oggetto, informandone il segnalante. I dati saranno conservati per il tempo necessario al trattamento della specifica segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.
d.	Principi fondamentali - Proporzionalità e necessità	
d.1	Gli scopi del trattamento sono specifici, espliciti e legittimi?	SI
d.2	Quali sono le basi legali che rendono lecito il trattamento?	La base giuridica di riferimento è la seguente: adempiere un obbligo legale al quale è soggetto il titolare del trattamento (artt. 6, par. 1, lett. c) ed e) GDPR, art 9, par. 2, lett. b), f) e g) GDPR e art. 10 del GDPR in relazione alle disposizioni di cui al D.lgs 24 /2023 (art. 13)
d.3	I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità	SI
d.4	I dati sono esatti e aggiornati?	Si
d.5	Qual è il periodo di conservazione dei dati?	i dati saranno conservati per il tempo necessario al trattamento della specifica segnalazione (12 mesi, prorogabili al doppio più volte) e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione
e.	Misure a tutela dei diritti degli interessati	
e.1	Come sono informati del trattamento gli interessati?	La piattaforma restituisce dei pop up informativi che non possono essere bypassati e che devono essere validati per poter procedere con la registrazione di una segnalazione. La compilazione del questionario inizia con una schermata che riporta l'informativa privacy completa.
e.2	Ove applicabile: come si ottiene il consenso degli interessati?	All'inizio della segnalazione è possibile inserire un link interno contenente l'informativa privacy completa del Titolare. Il consenso viene raccolto con la spunta di un flag obbligatorio per procedere con l'inserimento della segnalazione di illecito.
e.3	Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?	La persona coinvolta o la persona menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione non possono esercitare i diritti che normalmente il Regolamento (UE) 2016/679 riconosce agli interessati (il diritto di accesso ai dati personali, il diritto a rettificarli, il diritto di ottenerne la cancellazione o cosiddetto diritto all'oblio, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati personali e quello di opposizione al trattamento)
e.4	Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?	La persona coinvolta o la persona menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione non possono esercitare i diritti che normalmente il Regolamento (UE) 2016/679 riconosce agli interessati (il diritto di accesso ai dati personali, il diritto a rettificarli, il diritto di ottenerne la cancellazione o cosiddetto diritto all'oblio, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati personali e quello di opposizione al trattamento)

e.5	Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?	La persona coinvolta o la persona menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione non possono esercitare i diritti che normalmente il Regolamento (UE) 2016/679 riconosce agli interessati (il diritto di accesso ai dati personali, il diritto a rettificarli, il diritto di ottenerne la cancellazione o cosiddetto diritto all'oblio, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati personali e quello di opposizione al trattamento)
e.6	Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?	Il responsabile del trattamento sottoscrive la designazione e sottoscrive la documentazione fornita dal titolare. Gli obblighi sono riportati all'interno della stessa documentazione firmata da entrambe le parti.
e.7	In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?	Si
f.	RISCHI - Misure esistenti o pianificate	
f.1	Controllo degli accessi logici	L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password. Il sistema implementa protocollo di autenticazione a due fattori con protocollo.
f.2	Tracciabilità	L'applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema. I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent. I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati.
f.3	Archiviazione	Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura. I dati saranno conservati per il tempo necessario al trattamento della specifica segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.
f.4	Minimizzazione dei dati	Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati quali applicativo GlobaLeaks, log di sistema e firewall sono configurati per non registrare alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP, User Agents e altri Metadata. L'applicativo GlobaLeaks vede abilitata la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.
f.5	Vulnerabilità	L'applicativo GlobaLeaks e la relativa metodologia di fornitura SaaS sono periodicamente soggetti ad audit di sicurezza indipendenti di ampio respiro su base almeno annuale e tutti i report vengono pubblicati per finalità di peer review. A questi si aggiunge la peer review indipendente realizzata dalla crescente comunità di stakeholder composta da un crescente numero di società quotate, fornitori e utilizzatori istituzionali che su base regolare commissionano audit indipendenti che vengono forniti al progetto privatamente.
f.6	Lotta contro il malware	Tutti i computer del personale di Whistleblowing e dei sub-responsabili nominati eseguono firewall e antivirus come da policy aziendale ed il personale riceve continua e aggiornata formazione al passo con lo stato dell'arte in materia di lotta contro il malware. Parimenti le utenze del servizio di whistleblowing vengono sensibilizzate sulla tematica tramite formazione diretta o documentazione online.
f.7	Gestione postazioni	Le misure già adottate per la gestione delle postazioni sono: accesso con nome e password, antivirus, aggiornamento dei sistemi operativi, inaccessibilità del pc, vigilanza, tornelli, stanze chiuse a chiave
f.8	Backup	I sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery.
f.9	Sicurezza dei canali informatici	Tutte le connessioni sono protette tramite protocollo TLS 1.2+ Le connessioni amministrative privilegiate sono mediate tramite accesso VPN e connessioni
f.10	Controllo degli accessi fisici	il fornitore non ha accesso al data center fisicamente.
f.11	Sicurezza dell'hardware	I datacenter del fornitore IaaS dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7x24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7x24.
f.12	Prevenzione delle fonti di rischio	Crittografia (l'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington; nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento), Controllo degli accessi logici, Anonimizzazione, Tracciabilità (l'applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema. I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent)
f.13	Integrare la protezione dei dati personali nei progetti	la protezione dei dati personali degli utenti è integrata e presente lungo tutto il ciclo di progettazione del servizio. Il software è stato progettato e sviluppato secondo i principi della privacy by design e by default.
f.14	Gestire gli incidenti di sicurezza e le violazioni dei dati personali	Whistleblowing Solutions ha definito una procedura per la gestione delle violazioni dei dati personali.
f.15	Gestione delle politiche di tutela della privacy	Dati riservati per tutto il processo di gestione della segnalazione, raccolta del consenso al trattamento e alla divulgazione verso terzi obbligatorio
g.	RISCHI - Accesso illegittimo ai dati	
g.1	Quali potrebbero essere i principali impatti sugli interessati se il rischio	Divulgazioni di informazioni riservate relativi ai contenuti presenti all'interno della denuncia di illeciti corruttivi, Accesso a dati riservati di terze parti, danno d'immagine
g.2	Quali sono le principali minacce che potrebbero concretizzare il rischio?	attacchi informatici, Utilizzo o modifica non autorizzato dei dati, Abuso di privilegi di accesso, Errori nei processi di elaborazione dei dati, Utilizzo improprio di software o servizi, Perdita disponibilità per guasto HW
g.3	Quali sono le fonti di rischio?	utenti interni ed esterni; Perdita / furto di documentazione tecnica; guasti; violazioni della normativa
g.4	Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	Crittografia dei dati, Controllo degli accessi logici, Anonimizzazione, Tracciabilità, formazione del personale
g.5	Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure	limitato
g.6	Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e	Trascurabile
h.	RISCHI - Modifiche indesiderate ai dati	
h.1	Quali sarebbero i principali impatti sugli interessati se il rischio si	Divulgazioni di informazioni riservate relativi ai contenuti presenti all'interno della denuncia di illeciti corruttivi, danno d'immagine
h.2	Quali sono le principali minacce che potrebbero consentire la	attacchi informatici, Utilizzo o modifica non autorizzato dei dati, Abuso di privilegi di accesso, Errori nei processi di elaborazione dei dati, Utilizzo improprio di software o servizi
h.3	Quali sono le fonti di rischio?	utenti interni ed esterni; Perdita / furto di documentazione tecnica; guasti; violazioni della normativa
h.4	Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?	Crittografia dei dati, Anonimizzazione, Controllo degli accessi logici, Tracciabilità, Vulnerabilità, Sicurezza dei siti web, Backup, formazione del personale

h.5	Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure	limitato
h.6	Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure	Trascurabile
i.	RISCHI - Perdita di dati	
i.1	Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?	Divulgazioni di informazioni riservate relativi ai contenuti presenti all'interno della denucia di illeciti corruttivi, danno d'immagine
i.2	Quali sono le principali minacce che potrebbero consentire la	attacchi informatici, Utilizzo o modifica non autorizzato dei dati, Abuso di privilegi di accesso, Errori nei processi di elaborazione dei dati, Utilizzo improprio di software o servizi, Perdita disponibilità per guasto HW
i.3	Quali sono le fonti di rischio?	utenti interni ed esterni; Perdita / furto di documentazione tecnica; guasti; violazioni della normativa
i.4	Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?	Crittografia, Anonimizzazione, Controllo degli accessi logici, Tracciabilità, formazione del personale
i.5	Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure	limitato
i.6	Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure	Trascurabile