PRESIDENZA DEL CONSIGLIO DEI MINISTRI DIPARTIMENTO DELLA FUNZIONE PUBBLICA

DECRETO 3 novembre 2023

Individuazione, caratteristiche e modalita' di funzionamento del portale www.InPA.gov.it (23A06837)

(GU n.294 del 18-12-2023)

IL MINISTRO
PER LA PUBBLICA AMMINISTRAZIONE

Visto il decreto-legge 31 maggio 2021, n. 77, convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108, recante «Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure»;

Visto il decreto-legge 9 giugno 2021, n. 80, convertito, con modificazioni, dalla legge 6 agosto 2021, n. 113, recante «Misure urgenti per il rafforzamento della capacita' amministrativa delle pubbliche amministrazioni funzionali all'attuazione del piano nazionale di ripresa e resilienza (PNRR) e per l'efficienza della giustizia» e, in particolare, l'art. 1, che disciplina le modalita' di selezione dei professionisti ed esperti per il conferimento di incarichi di collaborazione da parte delle amministrazioni impegnate nell'attuazione dei progetti del Pino nazionale di ripresa e resilienza (PNRR);

Visto il decreto-legge 30 aprile 2022, n. 36, convertito con modificazioni dalla legge 29 giugno 2022, n. 79 e, in particolare l'art. 2, comma 2, il quale ha disposto che il Portale unico del reclutamento di cui all'art. 35-ter del decreto legislativo n. 165 del 2001 e' operativo dal 1° luglio 2022 e, a decorrere dalla medesima data, puo' essere utilizzato dalle amministrazioni pubbliche centrali di cui all'art. 1, comma 2, del medesimo decreto legislativo n. 165 del 2001 e dalle autorita' amministrative indipendenti e che a decorrere dal 1° novembre 2022 le medesime amministrazioni utilizzano il Portale per tutte le procedure di assunzione a tempo determinato e indeterminato;

Visto il decreto legislativo 30 marzo 2001, n. 165, recante «Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche» e successive modificazioni e, in particolare, il comma 2 dell'art. 35-ter recante «Portale unico del reclutamento» nella parte in cui dispone che con decreto del Ministro per la pubblica amministrazione, previa acquisizione del parere del Garante per la protezione dei dati personali e dell'intesa in sede di Conferenza unificata di cui all'art. 8 del decreto legislativo 28 agosto 1997, n. 281, sono individuate le caratteristiche e le modalita' di funzionamento del Portale, le informazioni necessarie per la registrazione al medesimo da parte degli utenti, le modalita' di accesso e di utilizzo dello stesso da parte delle amministrazioni di cui ai commi 1 e 4 e quelle per la pubblicazione dei bandi di

concorso, degli avvisi di mobilita' e degli avvisi di selezione di professionisti ed esperti, ivi comprese le comunicazioni ai candidati e la pubblicazione delle graduatorie, i tempi di conservazione dei dati raccolti o comunque trattati e le misure per assicurare l'integrita' e la riservatezza dei dati personali, nonche' le modalita' per l'adeguamento e l'evoluzione delle caratteristiche tecniche del Portale;

Visto il decreto-legge 24 febbraio 2023, n. 13, convertito con modificazioni dalla legge 21 aprile 2023, n. 41 e, in particolare, l'art. 12, comma 2 il quale ha disposto che «Fino alla data di entrata in vigore del decreto del Ministro per la pubblica amministrazione previsto dall'art. 35-ter, comma 2, del decreto legislativo 30 marzo 2001, n. 165, come modificato dal comma 1, continua ad applicarsi la disciplina contenuta nei protocolli adottati d'intesa tra il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri e ciascuna amministrazione ai sensi dell'art. 35-ter, comma 3, del decreto legislativo n. 165 del 2001 nel testo vigente prima della data di entrata in vigore del presente decreto»;

Visto il decreto-legge 22 aprile 2023, n. 44 convertito con modificazioni dalla legge 21 giugno 2023, n. 74 recante «Disposizioni urgenti per il rafforzamento della capacita' amministrativa delle amministrazioni pubbliche» e in particolare l'art. 3-ter recante «Misure per favorire il reclutamento di giovani nella pubblica amministrazione»;

Visto il decreto del Presidente della Repubblica 9 maggio 1994, n. 487, recante «Regolamento recante norme sull'accesso agli impieghi nelle pubbliche amministrazioni e le modalita' di svolgimento dei concorsi, dei concorsi unici e delle altre forme di assunzione nei pubblici impieghi»;

Visto il decreto del Presidente della Repubblica 16 giugno 2023, n. 82 recante «Regolamento recante modifiche al decreto del Presidente della Repubblica 9 maggio 1994, n. 487, concernente norme sull'accesso agli impieghi nelle pubbliche amministrazioni e le modalita' di svolgimento dei concorsi, dei concorsi unici e delle altre forme di assunzione nei pubblici impieghi»;

Visto il decreto del Ministro della pubblica amministrazione del 14 ottobre 2021 recante «Modalita' per l'istituzione degli elenchi dei professionisti e del personale in possesso di un'alta specializzazione per il PNRR» adottato in attuazione dell'art. 1 del decreto-legge 9 giugno 2021, n. 80, convertito, con modificazioni, dalla legge 6 agosto 2021, n. 113 di cui al punto precedente;

Visto il decreto del Ministro della pubblica amministrazione del 15 settembre del 2022 e, in particolare, l'art. 1, comma 3, in base al quale «In fase di prima applicazione, e comunque non oltre sei mesi dall'entrata in vigore del presente decreto, comunque non oltre il 31 maggio 2023, le regioni e gli enti locali possono continuare ad utilizzare anche i propri portali eventualmente gia' in uso»;

Visto l'art. 27 della legge 29 marzo 1983, n. 93, che ha istituito il Dipartimento della funzione pubblica nell'ambito della Presidenza del Consiglio dei ministri;

Vista la legge 23 agosto 1988, n. 400, recante «Disciplina dell'attivita' di Governo e ordinamento della Presidenza del Consiglio dei ministri»;

Visto il decreto legislativo 30 luglio 1999, n. 300, recante «Riforma dell'organizzazione del Governo, a norma dell'art. 11 della legge 15 marzo 1997, n. 59» e successive modificazioni;

Visto il decreto legislativo 30 luglio 1999, n. 303, e successive modificazioni e integrazioni, recante «Ordinamento della Presidenza del Consiglio dei ministri a norma dell'art. 11 della legge 15 marzo 1999, n. 59», e, in particolare, l'art. 7, comma 3, che riserva alle determinazioni del segretario generale ovvero del Ministro o del Sottosegretario delegato, nell'ambito delle rispettive competenze, l'organizzazione interna delle strutture nelle quali si articola la Presidenza del Consiglio dei ministri;

Visto il decreto del Presidente del Consiglio dei ministri del 1°

ottobre 2012, recante «Ordinamento delle strutture generali della Presidenza del Consiglio dei ministri» e, in particolare, l'art. 14 relativo al Dipartimento della funzione pubblica;

Visto il decreto del Presidente della Repubblica 21 ottobre 2022, con il quale il sen. Paolo Zangrillo e' stato nominato Ministro senza portafoglio;

Visto il decreto del Presidente del Consiglio dei ministri del 23 ottobre 2022, con il quale al predetto Ministro e' stato conferito l'incarico per la pubblica amministrazione;

Visto il decreto del Presidente del Consiglio dei ministri del 12 novembre 2022, con il quale al Ministro senza portafoglio per la pubblica amministrazione, sen. Paolo Zangrillo, sono state delegate le funzioni relative a «lavoro pubblico, organizzazione delle pubbliche amministrazioni e sistemi di gestione orientati ai risultati, nonche' in materia di innovazione organizzativa e gestionale delle amministrazioni pubbliche e semplificazione amministrativa»;

Considerato 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, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

Considerato il decreto legislativo 30 giugno 2003, n. 196, recante il «Codice in materia di protezione dei dati personali», integrato con le modifiche introdotte dal decreto legislativo 10 agosto 2018, n. 101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE» (regolamento generale sulla protezione dei dati);

Acquisita l'intesa in sede di Conferenza unificata di cui all'art. 8 del decreto legislativo 28 agosto 1997, n. 281 in data 6 settembre 2023;

Acquisito il parere dell'Autorita' garante per la protezione dei dati personali in data 3 novembre 2023;

Decreta:

Art. 1

Finalita' e ambito di applicazione

1. Il presente decreto e' adottato in attuazione dell'art. 35-ter, comma 2, del decreto legislativo 30 marzo 2001, n. 165, previa acquisizione del parere del Garante per la protezione dei dati personali e dell'intesa in sede di Conferenza unificata di cui all'art. 8 del decreto legislativo 28 agosto 1997, n. 281, e si applica alle amministrazioni pubbliche centrali di cui all'art. 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 e alle autorita' amministrative indipendenti, nonche' alle regioni e agli enti locali.

2. Le disposizioni del presente decreto si applicano alle regioni a statuto speciale e alle Province autonome di Trento e di Bolzano e relativi enti locali compatibilmente con i rispettivi statuti speciali e con le relative norme di attuazione.

3. Per la Provincia autonoma di Bolzano sono fatte salve, in ogni caso, le disposizioni di cui all'art. 1 del decreto del Presidente della Repubblica 26 luglio 1976, n. 752.

4. Al fine di garantire il pieno rispetto dei principi di autonomia costituzionalmente garantiti alle regioni a statuto speciale e alle Province autonome di Trento e Bolzano e relativi enti locali, il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri stipula, con le regioni a statuto speciale, con le Province autonome di Trento e Bolzano e con i relativi enti locali,

specifici protocolli per l'applicazione del presente decreto, prevedendo misure speciali per il pieno rispetto delle specificita' statutarie e del principio del bilinguismo.

5. Per le amministrazioni di cui all'art. 3 del decreto legislativo 30 marzo 2001, n. 165, le disposizioni di cui al presente decreto si applicano in quanto compatibili restando salve le disposizioni previste dai rispettivi ordinamenti.

6. Le amministrazioni di cui ai commi precedenti utilizzano il Portale unico del reclutamento per la pubblicazione e la gestione dei bandi di concorso, degli avvisi di mobilita' e degli avvisi di selezione di professionisti ed esperti di cui all'art. 1, comma 5, lettera a), del decreto-legge 6 giugno 2021, n. 80, convertito con modificazioni, dalla legge 6 agosto 2021, n. 113 e per le ulteriori finalita' individuate dalla disciplina vigente.

7. Per la disciplina relativa all'utilizzo del Portale con riguardo agli avvisi di selezione di professionisti ed esperti di cui all'art. 1, comma 5, lettera a), del decreto-legge 6 giugno 2021, n. 80, convertito con modificazioni, dalla legge 6 agosto 2021, n. 113, si applica il decreto del Ministro per la pubblica amministrazione del 14 ottobre 2021 recante «Modalita' per l'istituzione degli elenchi dei professionisti e del personale in possesso di un'alta specializzazione per il PNRR».

Art. 2

Caratteristiche e modalita' di funzionamento

1. L'assunzione a tempo determinato e indeterminato nelle amministrazioni pubbliche avviene mediante concorsi pubblici, orientati alla massima partecipazione e alla individuazione delle competenze qualificate, che si svolgono secondo le modalita' definite nel decreto del Presidente della Repubblica 9 maggio 1994, n. 487, come modificato dal decreto del Presidente della Repubblica 16 giugno 2023, n. 82 nel rispetto delle disposizioni e dei criteri di cui agli articoli 35, 35-ter e 35-quater del decreto legislativo 30 marzo 2001, n. 165.

2. Le funzioni disponibili sul Portale unico del reclutamento per le amministrazioni coprono l'intera gestione del processo di reclutamento, nelle sue fasi di:

a. individuazione, per mezzo di dati aggregati, elaborati dall'analisi della sezione curriculum vitae del Portale unico del reclutamento, della tipologia e della numerosita' delle professionalita' presenti in uno specifico ambito territoriale, finalizzata a supportare le politiche di reclutamento delle pubbliche amministrazioni;

b. pubblicazione di bandi di concorso pubblico per il reclutamento del personale a tempo determinato e indeterminato, di avvisi per la mobilita' dei dipendenti pubblici e di selezione di professionisti ed esperti ai sensi dell'art. 1 del decreto-legge 9 giugno 2021, n. 80, fermo quanto previsto dall'art. 10, comma 4, del decreto-legge 30 aprile 2022, n. 36, convertito, con modificazioni, dalla legge 29 giugno 2022, n. 79, secondo cui, al fine di rafforzare la propria capacita' amministrativa, per il conferimento di incarichi professionali le amministrazioni, con riferimento a procedure da avviare e gia' avviate, possono ricorrere al Portale;

c. monitoraggio e supporto alle candidature relative ai bandi e agli avvisi;

d. comunicazioni dirette agli utenti connesse alla candidatura, tramite posta elettronica, prima della scadenza dello specifico bando o avviso di selezione per informare l'utente dell'imminente scadenza, invitando contestualmente l'interessato a completare la propria candidatura;

e. acquisizione delle candidature e dei profili professionali congruenti alle esigenze dell'amministrazione;

f. comunicazione ai candidati concernente il concorso, compreso il calendario delle relative prove e del loro esito;

g. pubblicazione degli avvisi per la raccolta delle candidature a

componente di commissione esaminatrice, secondo quanto previsto dall'art. 9, comma 2 del decreto del presidente della repubblica 9 maggio 1994, n. 487;

h. pubblicazione dell'avviso selettivo per individuare i componenti degli organismi indipendenti di valutazione;

i. pubblicazione delle graduatorie finali di merito e degli esiti delle procedure di conferimento degli incarichi a professionisti o esperti;

j. richiesta di scelta della sede di destinazione da parte dei candidati successivamente alla pubblicazione della graduatoria di merito;

k. richiesta di supporto tecnico durante l'intera gestione del processo di reclutamento.

3. Il Portale unico del reclutamento offre le seguenti funzionalita' per gli utenti:

a. creazione e modifica del curriculum vitae, utile per agevolare l'interessato nella ricerca, selezione e compilazione delle domande di candidatura ad una posizione;

b. ricerca georeferenziata delle posizioni disponibili, in base ai filtri selezionati dall'utente;

c. compilazione della domanda di candidatura alla posizione di interesse e salvataggio della stessa all'interno del proprio profilo personale;

d. proposizione nonche' gestione delle candidature connesse alle posizioni;

e. comunicazioni dirette agli utenti connesse alla domanda di candidatura;

f. proposizione di candidatura a componente di commissione esaminatrice, secondo quanto previsto dall'art. 9, comma 2, del decreto del presidente della repubblica 9 maggio 1994, n. 487;

g. proposizione di candidatura all'avviso selettivo per individuare i componenti degli Organismi indipendenti di valutazione;

h. ricezione di comunicazioni concernenti il concorso, compreso il calendario delle relative prove e del relativo esito;

i. consultazione delle graduatorie finali di merito e degli esiti delle procedure di conferimento degli incarichi a professionisti o esperti;

j. scelta della sede di destinazione da parte del vincitore successivamente alla pubblicazione della graduatoria di merito;

k. richiesta di supporto tecnico.

4. Il Dipartimento della funzione pubblica svolge le seguenti funzioni sul Portale:

a. gestione del servizio di registrazione e di compilazione del curriculum vitae nell'apposita sezione del Portale di cui all'art. 3 del presente decreto;

b. monitoraggio della domanda e dell'offerta di lavoro pubblico presente sul Portale al fine di migliorare i processi e la qualita' del reclutamento nella pubblica amministrazione;

c. adeguamento delle caratteristiche tecniche di cui all'art. 9 del presente decreto;

d. supporto tecnico agli interessati e alle amministrazioni.

Art. 3

Informazioni per la registrazione da parte degli utenti

1. Per la registrazione al Portale del reclutamento sono richiesti:

a. la maggiore eta';

b. l'indicazione di un indirizzo di posta elettronica certificata o di un domicilio digitale a cui ricevere ogni comunicazione relativa alla procedura cui intende partecipare, ivi inclusa quella relativa all'eventuale assunzione in servizio;

c. un recapito telefonico;

d. la dichiarazione di avvenuta lettura dell'informativa sul trattamento dei dati personali, adottata, ai sensi degli articoli 13 e 14 del regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, pubblicata sul sito

http://www.inpa.gov.it/

2. La registrazione al Portale del reclutamento e' gratuita e puo' essere realizzata mediante i sistemi di identificazione di cui all'art. 64, commi 2-quater (SPID, CIE) e 2-nonies (CNS), del decreto legislativo 7 marzo 2005, n. 82, nonche' tramite identita' digitali eIDAS ai sensi del Regolamento UE n. 910/2014 sull'identita' digitale.

3. All'interno del Portale l'interessato compila il proprio curriculum vitae in un'apposita sezione dedicata, indicando:

a. il cognome e il nome;

b. il codice fiscale;

c. il luogo di nascita;

d. la data di nascita;

e. il sesso;

f. di essere cittadino italiano o di altro Stato membro dell'Unione europea, ai sensi dell'art. 38 del decreto legislativo 30 marzo 2001, n. 165, ovvero di essere titolare dello status di rifugiato ovvero dello status di protezione sussidiaria, o di essere cittadino di Paesi terzi in possesso del permesso di soggiorno UE per soggiornanti di lungo periodo e dei requisiti di cui all'art. 2, comma 2;

g. l'indirizzo di residenza o di domicilio, se diverso dalla residenza, il proprio indirizzo PEC o un domicilio digitale a lui intestato al quale intende ricevere le comunicazioni relative al concorso, unitamente a un recapito telefonico;

h. il comune nelle cui liste elettorali e' iscritto, oppure i motivi della non iscrizione o della cancellazione dalle liste medesime;

i. il titolo di studio posseduto o l'abilitazione professionale, con indicazione dell'universita' o dell'istituzione che lo ha rilasciato e la data del conseguimento. Se il titolo di studio e' stato conseguito all'estero il candidato indica gli estremi del provvedimento con il quale il titolo stesso e' stato riconosciuto equipollente al corrispondente titolo italiano o dichiara che provvedera' a richiedere l'equiparazione;

j. la specializzazione posseduta o la professionalita' esercitata;

k. le documentate esperienze professionali e gli altri titoli posseduti al momento della compilazione e dell'aggiornamento del proprio curriculum vitae.

4. I dati di cui al presente articolo, comma 3:

lettera a), b), c), d), e) e g) possono ricavarsi tramite SPID, fermo restando che i dati di cui alla lettera g) possono essere modificati dall'utente accedendo alla sezione anagrafica;

lettera a), b), c), d) ed e) possono ricavarsi tramite CIE o CNS;

lettera a) possono ricavarsi tramite eiDAS.

I suddetti dati sono ricavati tramite accesso per mezzo degli strumenti di cui al comma 2, nel rispetto del principio di minimizzazione di cui all'art. 5, par. 1 lettera c) del regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

Art. 4

Compilazione e presentazione delle candidature

1. L'interessato che si registra al Portale attraverso le modalita' di cui all'art. 3 accede all'apposita sezione della candidatura selezionando uno specifico bando o avviso d'interesse attraverso le funzioni di ricerca.

2. Per la compilazione della candidatura tramite il Portale del reclutamento sono richiesti i requisiti previsti dal bando o dall'avviso di interesse, nel rispetto di quanto previsto dalla normativa vigente in materia.

3. Ai fini della compilazione della candidatura, il candidato puo' replicare, mediante specifica funzionalita' presente nel Portale, le informazioni d'interesse necessarie gia' presenti nel curriculum

vitae compilato in fase di registrazione ed eventualmente aggiornato negli accessi successivi.

4. La domanda di partecipazione viene salvata automaticamente nella pagina personale dell'utente e conservata ai fini dell'eventuale proposizione della candidatura che potra' avvenire entro il termine previsto dallo specifico bando o avviso.

5. L'interessato riceve comunicazioni, connesse alla candidatura compilata e non trasmessa, tramite posta elettronica prima della scadenza dello specifico bando o avviso volte ad informare l'utente dell'imminente scadenza del termine per la proposizione della candidatura.

6. La trasmissione della canditura si perfeziona tramite verifica da parte dell'interessato dei dati inseriti e successivo invio. Contestualmente, l'interessato puo' aggiornare, mediante specifica funzionalita', il proprio curriculum vitae con le informazioni d'interesse inserite in fase di candidatura.

7. Il candidato dichiara, altresi', che le dichiarazioni sono rese ai sensi degli articoli 46 e 47 del Testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445. La veridicita' delle dichiarazioni rese dagli interessati ai sensi degli articoli 46 e 47 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e' verificata dalle amministrazioni che indicono le selezioni e utilizzano il Portale in quanto amministrazioni procedenti ai sensi dell'art. 71 del medesimo Testo unico di cui al decreto del Presidente della Repubblica n. 445/2000.

8. I dati personali trattati in tale sede possono riguardare anche le categorie particolari di cui agli articoli 9 e 10 del regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

Art. 5

Modalita' di accesso da parte delle PA

1. Per le finalita' di cui all'art. 2, le amministrazioni nominano uno o piu' «Responsabile unico» del procedimento appositamente dotato di uno dei sistemi di identificazione di cui all'art. 64, commi 2-quater e 2-nonies, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e di firma digitale che operera' secondo quanto previsto dal successivo comma 2. Ogni amministrazione puo', altresi', individuare uno o piu' «Operatore» autorizzato ad operare sul Portale del reclutamento, dotato di uno dei sistemi di identificazione di cui all'art. 64, commi 2-quater e 2-nonies, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82. Nell'ambito delle procedure di autenticazione informatica, mediante uno dei predetti sistemi di autenticazione, vengono acquisiti esclusivamente il codice fiscale, il cognome e il nome del personale autorizzato, nominato «Responsabile unico» o «Operatore».

2. Le amministrazioni accedono al Portale mediante il processo di accreditamento che prevede le seguenti fasi:

l'identificazione da parte dell'amministrazione aderente di uno o piu' «Responsabile Unico» (di seguito, per brevita', R.U.);

l'autenticazione sul Portale, mediante uno dei sistemi di identificazione di cui all'art. 64, commi 2-quater e 2-nonies, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, da parte del R.U.;

la compilazione da parte del R.U. di un form di richiesta in cui e' indicata la pubblica amministrazione di riferimento, con in allegato l'apposito modulo firmato digitalmente;

la trasmissione tramite il Portale della predetta richiesta unitamente al modulo firmato digitalmente, all'indirizzo di posta elettronica certificata (PEC) della pubblica amministrazione che si ricava automaticamente dall'Indice dei domicili digitali della pubblica amministrazione e dei Gestori di pubblici servizi (IPA);

il rappresentante legale dell'Amministrazione di riferimento,

ricevuta la posta elettronica certificata (PEC), provvede all'autorizzazione/diniego cliccando l'apposito link; ai fini dell'autorizzazione/diniego e' necessario che il rappresentante legale si autentichi al Portale tramite uno dei sistemi di identificazione di cui all'art. 64, commi 2-quater e 2-nonies, del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82;

una volta approvata o negata l'istanza, il rappresentante legale provvede a caricare il modulo di richiesta online, previa controfirma digitale;

il referente del Dipartimento della funzione pubblica Presidenza del Consiglio dei ministri puo' visionare attraverso una apposita consolle, a cui accede tramite uno dei sistemi di identificazione di cui all'art. 64, commi 2-quater e 2-nonies, del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, la lista delle richieste pervenute ed eventualmente operare sulle autorizzazioni/disabilitazioni dei RR. UU., anche tramite richiesta al fornitore;

al termine, il Portale notifica, via mail al R.U. e via posta elettronica certificata (PEC) all'Amministrazione, l'esito del processo di autorizzazione.

3. Ai fini del perfezionamento del processo di accreditamento, il rappresentante legale dell'Amministrazione di riferimento nomina il Dipartimento della funzione pubblica, responsabile del trattamento dei dati ai sensi dell'art. 28 del regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

4. Per l'adesione al sistema PagoPA di cui dall'art. 5 del decreto legislativo 7 marzo 2005, n. 82 si rinvia all'art. 65, comma 2, del decreto legislativo 13 dicembre 2017, n. 217 e alle istruzioni operative per l'accesso al Portale e per l'utilizzo delle relative funzionalita' che sono state definite dal Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri d'intesa con la Conferenza delle regioni e delle Province autonome, con ANCI e UPI e pubblicate nell'area riservate alle amministrazioni all'interno del Portale del reclutamento.

4. Il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri supporta le amministrazioni nell'utilizzo del Portale, anche al fine di assicurarne un adeguato e omogeneo utilizzo.

Art. 6

Modalita' di utilizzo da parte delle PA

1. Il Responsabile unico e l'Operatore, previo accesso al Portale mediante autenticazione, possono ivi effettuare, per conto dell'Amministrazione, le seguenti operazioni:

a. creazione di bandi/avvisi, inserimento delle informazioni necessarie, tra cui i requisiti di partecipazione e il termine iniziale e finale di presentazione delle candidature, e pianificazione della loro pubblicazione;

b. ricerca, gestione, monitoraggio e valutazione delle candidature e dei profili professionali di interesse;

c. acquisizione e pubblicazione degli esiti delle prove concorsuali per la visione da parte del singolo candidato e per la visione in area pubblica secondo quanto previsto dalla normativa vigente;

d. gestione delle comunicazioni verso gli utenti.

Art. 7

Comunicazioni ai candidati e pubblicazione graduatorie

1. Ogni comunicazione ai candidati concernente il concorso, compreso il calendario delle relative prove e del loro esito, e' effettuata attraverso il Portale. Le date e i luoghi di svolgimento delle prove sono resi disponibili sul Portale, con accesso da remoto

attraverso l'identificazione del candidato, nel rispetto dei termini di preavviso previsto dalle leggi.

2. La graduatoria finale del concorso elaborata dalla Commissione esaminatrice e' pubblicata, a cura dell'amministrazione procedente, nel proprio sito istituzionale, mentre sul Portale e' pubblicato un apposito avviso di avvenuta pubblicazione.

Art. 8

Conservazione dei dati raccolti e dei dati trattati

1. I dati personali conservati all'interno Portale sono trattati per il tempo strettamente necessario allo svolgimento delle finalita' indicate all'interno dell'informativa sul trattamento dei dati personali, ai sensi degli articoli 13 e 14 del regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, pubblicata sul sito http://www.inpa.gov.it/

2. Il periodo di conservazione, salvo per le finalita' di cui al comma 3, e':

a) pari a ventiquattro mesi dall'ultimo accesso al Portale, per i dati relativi:

(i) alla registrazione, di cui all'art. 3, comma 3, del presente decreto;

(ii) alla fruizione dei servizi connessi al curriculum vitae, di cui all'art. 2, comma 2, lettera a), di cui all'art. 2, comma 3, lettera a) e di cui all'art. 2, comma 4 lettera a) del presente decreto;

(iii) al monitoraggio del Portale, di cui art. 2, comma 4 lettera b) del presente decreto;

b) pari a ventiquattro mesi dalla conclusione delle relative attivita', per i dati attinenti:

(i) la ricerca, la compilazione e il salvataggio delle domande di candidatura e le relative funzioni connesse di cui all'art. 2, comma 2, lettera d) e comma 3, lettera b) e c) e di cui all'art. 4, fermo restando che le domande di candidatura non presentate saranno visibili all'amministrazione banditrice, soltanto per attivita' di supporto alla presentazione della domanda, per il periodo necessario a tale scopo con conseguente cancellazione dopo trenta giorni dalla scadenza del predetto periodo;

(ii) la proposizione e la gestione delle candidature e le relative funzioni connesse di cui all'art. 2, comma 2 lettera e) e di cui all'art. 2, comma 3, lettera d), f) e g) del presente decreto e di cui all'art. 4;

(iii) lo svolgimento delle attivita' connesse ai singoli processi di reclutamento, di cui all'articolo, 2 comma 2 lettera b), c), f) g), h) e k) e di cui all'art. 2, comma 3, lettera h) e k) del presente decreto;

(iv) lo svolgimento delle attivita' connesse alle singole procedure di scelta sedi, di cui all'art. 2, comma 2 lettera j) e art. 2, comma 3 lettera j) del presente decreto.

c) pari a ventiquattro mesi dalla richiesta di supporto tecnico sull'utilizzo del Portale, di cui all'art. 2, comma 4 lettera d) del presente decreto per i dati personali ad essi connessi;

d) pari a ventiquattro mesi dal pagamento, per i dati personali inerenti al pagamento degli oneri relativi alla proposizione di una candidatura;

e) pari a ventiquattro mesi dall'eventuale revoca o modifica dei soggetti designati dall'amministrazione a operare sul Portale per conto della stessa e comunque non oltre il termine di cinque anni da tale data di cui all'art. 5, per i dati ad essi connessi;

f) pari a ventiquattro mesi due anni, a decorrere dal momento in cui e' stata effettuata la singola operazione di accesso e autenticazione di cui all'art. 6, per i dati ad essa connessi.

3. Al raggiungimento dei termini sopra indicati, i dati personali potranno essere conservati unicamente per finalita' difesa di diritti, anche di terzi, in sede giudiziaria, per il periodo strettamente necessario al loro perseguimento, con riferimento a

contenziosi in atto o a situazioni precontenziose.

4. Al superamento dei termini sopra indicati, i dati personali verranno cancellati e/o resi anonimi in modo da impedire, anche indirettamente, l'identificazione dell'interessato.

Art. 9

Misure di sicurezza

1. Il trattamento dei dati personali mediante il Portale e' effettuato in conformita' con il regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 ed il decreto legislativo n. 196 del 2003.

2. Il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri e le amministrazioni attuano adeguate misure di sicurezza, organizzative, tecniche e fisiche per garantire che il trattamento di dati personali, operato mediante l'ausilio di strumenti manuali, informatici e telematici, sia eseguito per tutelare i dati dall'alterazione, dalla distruzione, dalla perdita, dal furto e dall'utilizzo improprio o illegittimo.

3. Le misure di sicurezza di cui al comma 2 sono rappresentate all'interno dell'Allegato tecnico, di seguito «Allegato tecnico». Il trattamento dei dati avviene nel rispetto dei principi di minimizzazione, integrita' e riservatezza dei dati personali, secondo modalita' e termini stabiliti nell'Allegato tecnico, nel quale sono riportate, anche con riferimento a categorie particolari di dati personali o dati relativi a condanne penali o reati, di cui agli articoli 9 e 10 del regolamento (UE) 2016/679.

4. In caso di malfunzionamento, anche temporaneo del Portale trova applicazione quanto previsto all'art. 3, comma 7 del decreto del Presidente della Repubblica 9 maggio 1994, n. 487, «Regolamento recante norme sull'accesso agli impieghi nelle pubbliche amministrazioni e le modalita' di svolgimento dei concorsi, dei concorsi unici e delle altre forme di assunzione nei pubblici impieghi», tenuto conto di quanto previsto dalla normativa in materia di protezione dei dati personali, ai sensi del regolamento (UE) 2016/679.

L'accertamento del malfunzionamento avviene secondo le seguenti modalita':

a) laddove il malfunzionamento della piattaforma sia tecnico e generalizzato, il Dipartimento provvede ad accertarlo con proprio atto, dandone comunicazione alle amministrazioni banditrici coinvolte e pubblicando un apposito Avviso informativo sul Portale a beneficio degli utenti;

b) laddove il malfunzionamento della piattaforma sia dovuto a problematiche tecniche o errori materiali riconducili alla singola Amministrazione banditrice, la medesima provvede tempestivamente ad informare il Dipartimento della Funzione pubblica che lo accerta con proprio atto, supportando l'Amministrazione banditrice nelle attivita' conseguenti e pubblicando un apposito Avviso informativo sul Portale a beneficio degli utenti.

Art. 10

Modalita' di adeguamento delle caratteristiche tecniche

1. Il presente decreto e il relativo allegato tecnico, che costituisce parte integrante del presente decreto, possono subire modifiche o integrazioni a seguito degli sviluppi evolutivi delle piattaforme. Le eventuali modifiche sono adottate con le medesime modalita' del presente decreto.

2. Alle attivita' di cui al presente decreto il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri provvede nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica.

Art. 11

Trattamento dei dati personali

1. Il titolare, ai sensi del regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, per i trattamenti dei dati personali finalizzati alla gestione del servizio di registrazione e di compilazione del curriculum vitae, monitoraggio del Portale, adeguamento delle caratteristiche tecniche e supporto tecnico di cui all'art. 2, comma 3 lettera a) e comma 4, di cui all'art. 3, e' la Presidenza del Consiglio dei ministri - Dipartimento della funzione pubblica, in persona del Capo pro tempore del Dipartimento della funzione pubblica, ai sensi dell'art. 3, comma 1, lettera a) del decreto del Presidente del Consiglio dei ministri 25 maggio 2018, con sede in corso Vittorio Emanuele II, 116 - 00186 Roma.

2. Il titolare del trattamento per la gestione dei dati personali relativi al processo del reclutamento, a decorrere dalla fase di compilazione della candidatura sino al termine del procedimento amministrativo, di cui all'art. 2, comma 2, e comma 4 lettera b) c) d) e) f) g) h) i) j) k) e di cui all'art. 4 e di cui all'art. 7, e' la singola Amministrazione banditrice. Le amministrazioni banditrici sono, altresi', titolari del trattamento dei dati dei soggetti di cui all'art. 5 e 6.

3. Il Dipartimento della funzione pubblica rende disponibile la propria informativa sul trattamento dei dati personali, relativa al Portale inPa, sul sito http://www.inpa.gov.it/

4. Le singole amministrazioni banditrici, di cui al comma 2 del presente articolo, rendono disponibili la propria informativa sul trattamento dei dati personali all'interno di ciascun specifico documento introduttivo del procedimento amministrativo.

5. Nei casi di cui al comma 2 del presente articolo, il Dipartimento della funzione pubblica e' Responsabile del trattamento dei dati ai sensi dell'art. 28 del regolamento (UE) 2016/679.

6. Il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri effettua una valutazione di impatto sulla protezione dei dati generale, ai sensi dell'art. 35, paragrafo 10, del regolamento (UE) 2016/679, sui trattamenti svolti mediante il Portale, nel contesto dell'adozione del presente decreto.

Art. 12

Clausola finanziaria

1. Alle attivita' di cui al presente decreto tutte le amministrazioni interessate provvedono nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica.

Roma, 3 novembre 2023

Il Ministro
per la pubblica amministrazione
Zangrillo

Registrato alla Corte dei conti il 27 novembre 2023
Ufficio di controllo sugli atti della Presidenza del Consiglio dei ministri, del Ministero della giustizia e del Ministero degli affari esteri e della cooperazione internazionale, reg. n. 3055

Allegato tecnico

1. Dati e trattamenti

I dati personali dell'interessato sono trattati per il perseguimento delle finalita' connesse all'espletamento delle attivita' demandate al Dipartimento della funzione pubblica (di seguito, «Dipartimento») dall'35-ter del decreto legislativo 30 marzo 2001, n. 165.

I dati personali vengono conservati per il tempo strettamente necessario allo svolgimento delle suesposte finalita' e, una volta scaduti i rispettivi termini, i dati personali saranno cancellati e/o resi anonimi in modo da impedire, anche indirettamente, l'identificazione dell'interessato.

1.1 Misure per assicurare l'integrita' e la riservatezza dei dati personali

Le misure di sicurezza organizzativa/procedurale messe in atto dal Dipartimento sono di seguito elencate:

Privacy policy;

Procedura di data breach;

Procedura di DPIA;

Modello di nomina dei responsabili del trattamento e relative istruzioni;

Modello di nomina dei soggetti autorizzati del trattamento e relative istruzioni;

Nomina del Responsabile della protezione dei dati.

Misure procedurali/organizzative di sicurezza adottate

Accesso controllato aree fisiche

Accesso fisico ai dati (es. armadi chiusi)

Accesso digitale ai dati (es. autenticazione e autorizzazione) Formazione

Istruzioni per il trattamento Nomina per iscritto personale Nomina Amministratore di sistema

Nomina per iscritto responsabili esterni

Policy aziendali

Policy aziendali utilizzo posta elettronica

Procedura data breach

Procedura gestione dati (variazione, cancellazione)

Misure tecniche di sicurezza adottate - Misure Digitali

Antivirus/AntiSpam Autenticazione Autorizzazione Business continuity

Data Inventory & Classification Disaster recovery

DLP (Data Loss Prevention)

Firewall/WAF (Web Application Firewall) Intrusion Detection/Intrusion Prevention Monitoraggio/Log Management

Log Amministratori di sistema

Separazione (VLAN, Virtual Local Area Network) Trattamento Dati -> Cifratura dei dati

Back Up periodici

Misure tecniche di sicurezza adottate - Misure Fisiche

Armadi/cassettiere chiusi a chiave

Autorizzazione di accesso - Badge - Sistema Biometrico Guardiania/Presidio fisico locali

Sistemi di rilevamento accessi (es: sensori di accesso) Sistemi di registrazione (es: telecamere)

1.2 Sintesi delle caratteristiche tecniche del Portale

Di seguito si riporta una sintesi delle caratteristiche tecniche rilevanti del Portale; tali caratteristiche sono da considerarsi «minime» da garantire per l'adeguamento e l'evoluzione delle caratteristiche tecniche del Portale.

La soluzione infrastrutturale presenta le seguenti caratteristiche:

Adozione di un WAF (Web Application Firewall) in cloud (SaaS - Security as a Service) al fine di avere un'efficace linea di contenimento verso le minacce piu' diffuse, come ad esempio attacchi DDoS, malware e attacchi zero-day;

Continuita' operativa garantita dall'utilizzo congiunto del Centro Servizi SPC e di un Cloud Service Provider qualificato da AgID per un'erogazione «diversificata» del servizio in termini di:

Connettivita';

Infrastruttura tecnologica.

Di seguito una sintesi dello stack tecnologico utilizzato:

Wordpress: sistema di gestione dei contenuti (CMS) per l'area pubblica del portale;

Spring Framework + Spring Boot: framework base per lo sviluppo

di tutte le componenti della piattaforma;

Spring Security: framework del progetto Spring per la gestione dell'autenticazione e della profilazione degli utenti;

Spring MVC REST + Jackson: API;

Spring Data JPA + Bean Validation: interfacciamento alla base dati;

Angular: User Interface;

Maven: compilazione, unit testing e deploy delle applicazioni;

Netflix OSS: orchestrazione e gestione dei micro-servizi.

Web Application Firewall (WAF): Il firewall per applicazioni web utilizzato e' Fortiweb basato su cloud Security as a Service (SaaS). Le sue caratteristiche riguardano:

Scalabilita' sufficiente per proteggere dagli attacchi DoS e DDoS piu' imponenti;

Performance elevate anche durante gli attacchi grazie all'architettura distribuita globalmente;

Approccio completo alla protezione delle applicazioni web tra cui IP reputation, protezione DDoS, convalida del protocollo, signature per rilevare attacchi contro le applicazioni, mitigazione dei bot e molto altro per difendere le applicazioni web da un'ampia gamma di minacce;

Apprendimento automatico che costruisce e aggiorna automaticamente un modello di comportamento normale dell'utente e utilizza tale modello per identificare il traffico benigno e dannoso delle applicazioni.

Il Portale risiede nelle sedi dei CED del Fornitore (una sede situata nell'area dell'Italia centrale e una diversa sede situata nell'area settentrionale) e sull'infrastruttura del cloud provider qualificato Amazon AWS (Irlanda). L'architettura dei Centri Servizi garantisce al Portale BC (Business Continuity) e DR (Disaster Recovery).

2. Centri Servizi del Fornitore

2.1 Infrastruttura

Gli elementi che concorrono a definire l'infrastruttura necessaria sono ospitati nel Cento Servizi che assicura i massimi livelli di sicurezza tali da consentire, in caso di malfunzionamenti HW o SW o di perdita di contenuti informativi, il ripristino tempestivo della situazione. Inoltre, le attivita' di Governo previste su tali apparati sono tali da garantire un continuo e costante aggiornamento delle soluzioni adottate.

Tutti gli elementi dell'infrastruttura del Centro Servizi sono progettati e realizzati in logica ridondata per garantire l'alta affidabilita' del servizio e senza Single Point of Failure (dispositivi, connettivita' ecc.).

2.2 Continuita' Operativa

Il Centro Servizi e' certificato ISO27001 ed e' organizzato su 3 Data Center dislocati sul territorio italiano che ospitano sia il personale sia l'infrastruttura dedicata alle amministrazioni contraenti. Due Data Center sono situati nell'area dell'Italia centrale integrati con una soluzione di «cluster metropolitano» per garantire eccellenza in termini di bilanciamento del carico elaborativo e di Business Continuity. I Data Center sono inoltre certificati ISO 20000 per l'IT Service Management, ISO 22301 per la Business Continuity, ISO 14001 e ISO 50001 per qualita'/impatto ambientale. Vi e' un terzo Data Center situato nell'Italia settentrionale che completa la soluzione di continuita' operativa implementando le funzionalita' di Disaster Recovery. Il «cluster metropolitano» offerto dal Centro Servizi costituisce una innovativa architettura di data center, che garantisce elevati livelli di scalabilita' a fronte di improvvisi picchi di carico e la massima resilienza a fronte della indisponibilita' parziale o totale delle singole componenti infrastrutturali. Complessivamente la soluzione consente:

una completa Business Continuity con parametri di RTO e RPO prossimi a zero. Gli apparati, le tecnologie e le competenze impegnate consentono di erogare gli stessi servizi indifferentemente,

dall'uno o dall'altro Data Center garantendo sempre la continuita', in caso di disastro parziale o totale di uno dei due siti;

elevati livelli di performance garantiti dal bilanciamento dinamico del carico e la conseguente massima ottimizzazione delle performance dei sistemi e degli strumenti utilizzati per l'erogazione dei servizi;

un Disaster Recovery, che si affianca al Cluster Metropolitano per garantire la continuita' operativa in caso di disastro che coinvolga entrambi i siti del cluster. L'infrastruttura messa a disposizione e le tecniche di replica dei dati adottate consentono di garantire RTO pari a 4h e RPO pari a 1h.

2.3 Sicurezza

La soluzione di sicurezza del RTI e' in grado di fornire Misure di Sicurezza su 3 livelli distinti:

Sicurezza fisica

Sicurezza logica

Sicurezza organizzativa

Sicurezza Fisica

Aree Sicure

Barriere all'ingresso

Per tutte le sedi che compongono il Centro Servizi sono previste delle barriere perimetrali (mura, pareti, cancelli ad accesso controllato, tornelli, etc.) ed ogni sito operativo dispone di un piano della sicurezza fisica in linea con lo standard ISO27001.

1. Un Centro servizi Metropolitano

L'area su cui insiste l'edificio e' interamente recintata e controllata da telecamere.

Per accedere all'edificio occorre superare uno sbarramento comandato dal personale della guardiania posto vicino al cancello d'ingresso dove avviene il riconoscimento tramite badge o documento di identita' per tutte le persone in ingresso e, successivamente, un servizio di reception presso il quale sono registrati gli ospiti e consegnati i badge magnetici temporanei.

Per entrare nelle aree del CED in cui sono presenti le macchine elaborative e gli apparati di rete, occorre superare un ulteriore sbarramento, ossia le bussole antirapina comandate attraverso il riconoscimento di badge magnetici autorizzati.

Le finestre e le porte sono antintrusione in quanto videosorvegliate e allarmate.

2. Un secondo Centro servizi Metropolitano

L'area su cui insiste l'edificio e' interamente recintata e controllata da telecamere. Per accedere all'edificio occorre superare uno sbarramento comandato dal personale della guardiania posto vicino al cancello d'ingresso dove avviene il riconoscimento tramite badge o documento di identita' per tutte le persone in ingresso e, successivamente, un servizio di reception presso il quale sono registrati gli ospiti e consegnati i badge magnetici temporanei. Per entrare nelle aree del CED in cui sono presenti le macchine elaborative e gli apparati di rete, occorre superare un ulteriore sbarramento: le bussole antirapina comandate attraverso il riconoscimento di badge magnetici autorizzati. Le finestre e le porte sono antintrusione in quanto videosorvegliate e allarmate.

3. Un Centro servizi Italia settentrionale

L'area su cui insiste il comprensorio e' interamente recintata e controllata da telecamere. Tra l'area parcheggio per il personale addetto al Data Center e per gli ospiti e l'edificio e' presente un'ulteriore separazione. Per accedere all'edificio occorre superare la reception. Per entrare nelle aree del Data Center in cui sono presenti le macchine elaborative e gli apparati di rete, occorre superare una serie di ulteriori sbarramenti tipo porta di accesso al piano e accesso alle sale CED, attraverso il riconoscimento di badge magnetici autorizzati per la disattivazione dell'allarme.

Controllo degli ingressi

Le aree da proteggere sono controllate in modo da assicurare che solamente il personale autorizzato possa accedere alle strutture.

Protezione dell'edificio e dei locali del Data Center da disastri

ambientali o provocati dall'uomo

Per tutti i Data Center che compongono il Centro Servizi sono messe in atto protezioni per far fronte a minacce di natura ambientale e minacce di disastri per opera dell'uomo quali:

- incendio
- allagamento
- terremoto
- fulmini
- esplosioni
- attentati terroristici.

In sintesi, le protezioni/misure messe in atto in tutti e tre i Data Center e per la sede operativa sono:

- costruzione antisismica
- impianto antincendio (dispositivi attivi e passivi a seconda dei locali) parafulmine
- pavimentazione delle sale rialzata e sonde per rilevazione allagamenti barriere all'ingresso a piu' livelli (misura prevista solo per i Data Center).

Sicurezza delle apparecchiature

Ubicazione sicura delle apparecchiature

Le apparecchiature presenti in tutte le sedi che compongono il Centro Servizi sono posizionate in modo da ridurre i rischi ambientali e i rischi dovuti a un accesso non autorizzato.

Impianti per la protezione delle apparecchiature e alimentazione elettrica alternativa

Per proteggere le apparecchiature sono usati impianti per garantire il funzionamento delle stesse e il mantenimento di parametri ambientali richiesti dal costruttore delle apparecchiature. Le apparecchiature e gli stessi impianti sono alimentati da corrente elettrica e quindi sono attuate adeguate protezioni da cadute di corrente.

A protezione del buon funzionamento delle apparecchiature, sono installati opportunamente gli impianti a supporto delle apparecchiature:

- impianto elettrico e alimentazione elettrica adeguati al carico richiesto;
- impianto per il condizionamento dell'aria e la ventilazione;
- impianti idraulici.

Le apparecchiature di tali impianti sono tenute costantemente sotto controllo e periodicamente testate per ridurre al minimo i rischi derivanti da un loro malfunzionamento.

Le apparecchiature sono protette nei confronti di possibili mancanze di energia elettrica o per malfunzionamenti negli apparati di controllo dei parametri indicati dai costruttori. Sono previsti gruppi di continuita' (UPS) per tutte le apparecchiature informatiche e uno o piu' generatori di corrente alternativi. Inoltre:

- gli UPS e i generatori alternativi sono regolarmente controllati;
- sono previste luci di emergenza per accedere alle apparecchiature in caso di mancanza di luce primaria;
- sono previsti sistemi di allarme per avvisare per tempo eventuali malfunzionamenti degli impianti;
- sono previsti quadri elettrici a norma che consentano la separazione dell'alimentazione elettrica nei vari ambienti.

Protezione dei cablaggi da intercettazioni o da danni fisici

I cablaggi per l'alimentazione elettrica e per la rete dati sono protetti da intercettazioni e danneggiamenti.

Sicurezza Logica

Sicurezza delle reti

Di seguito sono descritti in generale i controlli per la sicurezza delle reti:

- per la rete pubblica e' utilizzato il Sistema Pubblico di Connettivita' (SPC), che e' stato progettato per essere utilizzato anche da cittadini e imprese che siano dotati di opportune credenziali (per es. CIE e CNS). L'architettura di SPC prevede un'organizzazione articolata per la sicurezza, nella quale le

strutture operanti in ciascun dominio sono interconnesse e coordinate in modo tale da costituire virtualmente un'unica struttura operativa.

per la rete locale, le contromisure realizzate sono:

DMZ (rete demilitarizzata) su cui sono attestate le macchine raggiungibili dall'esterno (tipicamente web server);

firewall di front-end tra la DMZ e l'esterno con funzioni di filtraggio e apposite configurazioni di routing;

firewall di back-end per filtrare il traffico tra la DMZ e la rete interna;

rete interna o protetta su cui sono attestate le macchine che non devono essere raggiunte dall'esterno ma che possono essere raggiunte solamente da macchine che si trovano in DMZ o da altre macchine attestate sulla rete interna;

suddivisione della rete in VLAN per tenere separati i domini applicativi tra di loro e consentire, attraverso opportune configurazioni di apparati di rete come i firewall, solamente il transito dei dati all'interno del dominio, fatta eccezione per specifiche macchine di gateway del dominio stesso che rappresentano l'interfaccia verso l'esterno del dominio;

controllo del traffico di rete - per garantire che la rete sia utilizzata esclusivamente dall'utenza autorizzata e nelle modalita' definite dai profili di abilitazione (ovvero quali servizi di rete e' possibile usare e come) sono state realizzate misure efficaci di identificazione e autenticazione dell'utente e di controllo degli accessi ai servizi di rete, quali l'utilizzo di dispositivi firewall, dislocati nei punti di interconnessione tra reti TCP/IP distinte, che hanno il compito di controllare gli accessi alle risorse di rete interconnesse. Tale controllo e' effettuato filtrando i messaggi in transito e facendo passare solo quelli che rispondono ai requisiti definiti dalle politiche di sicurezza definite dal Cliente o dalle specifiche del servizio o, in loro assenza, dalle best practice. Le macchine firewall presso i Data Center hanno una configurazione tale da minimizzarne le vulnerabilita' a fronte di attacchi informatici che possano pregiudicare l'integrita' del software stesso. I file di log sono mantenuti per finalita' di trouble shooting, per un periodo da uno a tre mesi in relazione allo spazio occupato;

riservatezza - adozione del protocollo HTTPS (SSL), per consentire l'accesso a siti pubblici da parte di un ampio bacino di utenza proteggendo mediante cifratura le informazioni che viaggiano in rete.

integrita' - il requisito di integrita' ha l'obiettivo di proteggere dai cosiddetti attacchi attivi verificando in fase di ricezione se sono state apportate modifiche alle singole unita' dei dati o alla sequenza delle stesse. Gli attacchi attivi comportano un'alterazione o una modifica dei dati trasmessi. Presso i Data Center metropolitani i firewall esterni sono configurati in modo che e' consentito in maniera controllata il traffico verso l'esterno mentre il traffico verso la rete interna e' consentito solo in risposta a quello verso l'esterno. Il traffico proveniente da internet e' bloccato a eccezione di quello verso la DMZ che comunque viene controllato in termini di indirizzi accessibili e di protocolli consentiti. Policy e regole di routing sui firewall consentono il traffico tra DMZ e rete interna in modo controllato;

disponibilita' della rete - l'architettura SPC prevede apparati di rete ridondati o comunque disposti in modo tale che l'eventuale guasto o danneggiamento di uno di essi non possa pregiudicare il funzionamento complessivo del servizio.

autenticazione - garantisce l'entita' ricevente sull'autenticita' dell'entita' mittente e dei dati ricevuti. Il requisito e' risolto, per gli accessi da internet da parte degli utenti esterni, mediante la realizzazione di opportune VPN con autenticazione mediante UserId e Password, per gli accessi dalla rete interna, mediante connessioni realizzate esclusivamente su rete SPC Intranet.

3. Ambienti Amazon Web Service (AWS)

Gli elementi che concorrono a definire l'infrastruttura

necessaria sono ospitati nel Cloud Pubblico di AWS che assicura i massimi livelli di sicurezza e di resilienza tali da consentire, in caso di malfunzionamenti HW o SW o di perdita di contenuti informativi, il ripristino tempestivo. Inoltre, le attivita' di Governo previste su tali apparati sono tali da garantire un continuo e costante aggiornamento delle soluzioni adottate.

Tutti gli elementi dell'infrastruttura sono progettati e realizzati in logica ridondata per garantire l'alta affidabilita' del servizio e senza Single Point of Failure (dispositivi, connettivita' ecc.).

I Data Center di AWS, il Cloud Service Provider (CSP) sono stati realizzati e progettati seguendo gli standard IT definiti da normative, regolamenti, conformita' e framework e valutati qualitativamente da audit di terze parti indipendenti e certificati da enti specializzati. AWS dispone di certificazioni di conformita' ai sensi degli standard ISO/IEC 27001:2013, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 9001:2015 e CSA STAR CCM v4.0.

Rif.: https://aws.amazon. com/it/compliance/iso-certified/

Parte di provvedimento in formato grafico

4. Politica di Backup

La tabella seguente riporta le politiche di backup attuate per i data base:

Tipologia DB	TIPO RMAN: Fisico, EXDP: Logico	FREQUENZA	RETENTION
ORACLE	Archive	Giornaliera	7gg
	FULL	Settimanale	28gg
MySQL	FULL (in locale)	Giornaliero	7gg *
	Backup fisico intera MV	Giornaliero	30gg
MARIA DB	FULL (in locale)	Giornaliero	7gg
	Backup fisico intera MV	Giornaliero	30gg
MONGO DB	-	-	-
	Backup fisico intera MV	Giornaliero	30gg
POSTGRES	FULL (in locale)	Giornaliero	7gg *
	Backup fisico intera MV	Giornaliero	30gg
SQLServer	-	-	-
	Backup fisico intera MV	Giornaliero	30gg

* Per un ristretto numero di macchine legacy migrate in SPC, la cui configurazione pre esistente non aveva un dimensionamento dello storage adeguato ad attuare la politica di retention dei backup in locale definita per SPC di 7gg, e' mantenuto in linea 1 backup giornaliero.

La tabella seguente riporta le politiche di backup attuate per i server che sono gestiti tramite macchine virtuali:

Ambiente	Tipo di Backup	Frequenza	Retention
Macchine Virtuali	Full (di tipo fisico)	Giornaliera	30 giorni

Il ripristino dei dati sara' eseguito a fronte di una richiesta dell'Amministrazione o dei referenti degli altri servizi contrattuali autorizzati dall'Amministrazione medesima.

Nel caso di perdita e/o corruzione di dati segnalata dall'utente, quest'ultimo deve fornire tutte le necessarie informazioni per eseguire il restore.

Nelle attivita' di restore ci si atterra' per quanto possibile a procedure standard che prevedono, per esempio, a seconda delle necessita', attivita' di ripristino prendendo in input:

ultimo salvataggio completo

ultimo salvataggio differenziale

i salvataggi dei file successivi al salvataggio completo o a quello differenziale e comunque immediatamente precedenti alla situazione che ha causato la richiesta di ripristino.

A completamento delle operazioni di restore la procedura prevede la verifica del buon esito delle operazioni di ripristino e l'attivazione delle opportune procedure di ripartenza. In caso di esito positivo sara' comunicato all'Amministrazione o ai referenti degli altri servizi coinvolti nella richiesta l'avvenuto ripristino dei dati e/o dei sistemi.

5. Cyber Security

SOC / CSIRT

Il SOC / CSIRT garantisce il controllo della sicurezza del patrimonio informativo e la protezione attiva da minacce e incidenti di cybersecurity.

Il SOC / CSIRT e' una funzione specializzata nell'erogazione di servizi gestiti e professionali di sicurezza informatica che si avvale di risorse altamente qualificate e con una vasta gamma di certificazioni professionali di settore (ad esempio: CISSP, OPST OSSTMM e certificazioni sulle principali tecnologie per la gestione della sicurezza). Nella funzione sono presenti team che operano in sinergia con differenti modalita' operative:

un team di primo livello per il monitoraggio real time, gestione degli apparati e dei prodotti, gestione delle misure di sicurezza logica, applicative e dei dati, configuration management, patching/hardening dei sistemi, rilevazione e segnalazione di attacchi, comportamenti fraudolenti, violazioni ed eventi rilevanti; gestione delle utenze amministrative; reportistica e supporto alla gestione della continuita' operativa.

un team di analisti, architetti e specialisti di sicurezza che effettuano attivita' sia di analisi e definizione delle misure di prevenzione sia di secondo livello nella gestione degli incidenti.

Per quello che riguarda soluzioni e strumenti, il SOC si avvale di una infrastruttura tecnologica integrata come indicato nella figura seguente

Parte di provvedimento in formato grafico

I servizi erogati dal SOC/ CSIRT sono i seguenti:

Advancd Endpoint Protection

Il servizio e' erogato tramite una soluzione basata su tecnologia certificata FIPS e CC EAL 4+ per la sicurezza dei contenuti digitali per i server e fornisce le funzionalita':

Antivirus & Antimalware

La soluzione si integra con gli ambienti VMware per la protezione agentless o fornisce un agent per la difesa dei server sia fisici che

virtuali.

Host IPS e Virtual Patching

Questo modulo ha il compito di proteggere le VM da vulnerabilita' note e zero-day. Grazie al proprio database interno offre regole gia' pronte per oltre 100 applicazioni ed ha il compito di distribuire velocemente le patch inerenti eventuali zero-day rilevati. La console permette l'implementazione su larga scala in pochi minuti senza richiedere un riavvio dei sistemi impattati.

Gestione WAF

La soluzione Web Application Firewall (WAF) e' uno strumento che funge da controllore del traffico web diretto alle applicazioni da proteggere in maniera del tutto trasparente per le applicazioni stesse.

Il suo punto di forza e' riuscire ad interpretare il traffico HTTP con lo scopo di rilevare e bloccare cyber attacchi. Tale funzionalita' richiede di definire le regole di protezione dell'applicazione analizzandone il normale utilizzo. Inoltre, il WAF consente l'abilitazione di regole custom di vario tipo atte, ad esempio, a consentire l'accesso ad URL amministrative solo particolari IP oppure a disabilitare alcuni metodi http ritenuti vulnerabili oppure ancora a securizzare i cookie, crittografandoli.

Fornisce inoltre la possibilita' di monitorare in real-time il livello di sicurezza e di generare una serie di report, personalizzabili, al fine di certificare la compliance a determinati standard o per consentire analisi sul livello di protezione delle applicazioni. L'attivita' di monitoraggio si rivela particolarmente utile per individuare e risolvere in modo proattivo eventuali falsi positivi e, quindi, possibili disservizi all'utenza.

Attraverso Web Application Firewall si effettuera' il controllo del traffico HTTP, definendo regole di protezione di vario tipo quali, ad esempio, consentire l'accesso ad URL amministrative solo a particolari IP oppure disabilitare alcuni metodi http ritenuti vulnerabili oppure ancora securizzare i cookie, crittografandoli. Sara' anche possibile monitorare in real-time il livello di sicurezza e generare report atti, se necessario, a certificare la compliance a determinati standard o a consentire analisi sul livello di protezione dell'applicazione.

Anti-DDOS

Il servizio e' erogato mediante un'architettura cloud connessa con CDN dedicata al Data Center che permette di proteggere i sistemi retrostanti da possibili attacchi DDOS che, basandosi sulla generazione di un quantitativo enorme di traffico, tentano di rendere il sistema non raggiungibile. L'uso di una soluzione basata sul cloud permette di sfruttare la naturali caratteristiche di resilienza di tale infrastruttura lasciando inalterata l'infrastruttura di effettiva erogazione del servizio.

Il sistema Anti-DDOS erogato permette di intercettare molteplici tipi di attacchi DDOS, sia basati sul livello 2 che superiori della pila ISO/OSI, mettendo a disposizione strumenti personalizzabili sui limiti di sicurezza del cliente; per ogni attacco identificato permette di personalizzare una corretta reazione che varia dalla semplice annotazione sui log fino al blocco della connessione.

La protezione puo' essere attivata agendo sia sulla limitazione del traffico per singolo IP (tcp session limit rates, tcp flooding limits, http limit rates, Malicious IPs, etc.), sia proponendo una soluzione di «diversion» basato su challenge (javascript based, captcha, etc.).

Il sistema e' integrato con la piattaforma di SIEM per una gestione integrata delle segnalazioni.

Log Management / SIEM

Il servizio consente di:

Raccogliere e centralizzare i log ed archiviarli per un periodo congruo con la normativa in vigore

Effettuare il parsing e la normalizzazione degli eventi

Effettuare analisi e correlazione in real-time delle informazioni raccolte, attraverso la configurazione di regole di

correlazione e alert finalizzati all'individuazione e gestione di incident di sicurezza

Effettuare reportistica sui dati archiviati

Verranno integrati sul SIEM i sistemi in esercizio raccogliendo una tipologia di log standard per tutti (es: accesso Ads) utili sia a rispettare la compliance alla normativa sulla Privacy, sia ad alimentare un set standard di regole SIEM defnite in ambito SPC per rilevare incident di sicurezza. Per implementare la raccolta degli eventi dai sistemi per mezzo della soluzione SIEM adottata, la piattaforma necessita di essere gestita in sinergia con le procedure utilizzate per il delivery/deploy, la conduzione e la dismissione dei sistemi.

L'attivita' prevede la raccolta e archiviazione centralizzata dei log per un periodo congruo con la normativa in vigore, il parsing e la normalizzazione degli eventi, l'analisi delle informazioni raccolte, attraverso la configurazione di regole di correlazione e l'invio di alert finalizzati all'individuazione e gestione di incident di Sicurezza, con produzione di eventuali report sui dati archiviati.

Il SOC/CSIRT del Centro Servizi, rispetto ad eventi ed incidenti di Sicurezza, si interfaccera' con il SOC Sogin, secondo tempi e modalita' di comunicazione concordate in fase di avvio dei servizi.

Il SIEM del Cero servizi potra' essere configurato per l'invio in formato standard Syslog degli eventi di sicurezza al SOC indicato da Sogin.

Eventuali esigenze aggiuntive richieste dal cliente, potranno essere concordate con il team del SOC/CSIRT.

Vulnerability Assessment e Penetration Test

Il servizio di Vulnerability Assessment (VA o VA standard) si pone come scopo la definizione, identificazione, classificazione e prioritizzazione delle vulnerabilita' potenziali dei sistemi, applicazione o reti che potrebbero compromettere la riservatezza, l'integrita' e la disponibilita' dei dati. Il VA fornisce, quindi, una mappatura delle vulnerabilita' rilevate, riducendo la probabilita' d violazioni dei sistemi.

Il servizio di Vulnerability Assessment viene erogato mediante una scansione automatica mediante lo strumento di assessment in maniera tale da garantire un processo di ricerca sistematica delle vulnerabilita' del sistema e della rete oggetto di valutazione.

Il Vulnerability Assessment viene effettuato prima dell'avvio in esercizio dei sistemi e periodicamente con frequenza annuale.

Il Penetration Test Infrastrutturale ha lo scopo di verificare il livello di sicurezza degli elementi infrastrutturali (quali router, switch, etc.) e di difesa perimetrale (firewall, IPS, etc,) che costituiscono la rete. Il Penetration Test Applicativo viene svolto secondo la metodologia OWASP mediante l'esecuzione di una serie di tentativi di attacco, che coinvolgono i protocolli e le logiche di comunicazione utilizzati dagli utenti finali per interagire con le applicazioni (attacco ai web server, alla struttura applicativa, ai sistemi di autenticazione e autorizzazione, alle interfacce di gestione, ai sistemi client, ...).

Il Penetration Test e' previsto prima dell'avvio in esercizio delle applicazioni e periodicamente con frequenza annuale.

Eventuali esigenze aggiuntive richieste dal cliente, potranno essere concordate con il team del SOC/CSIRT.

6. Sicurezza Organizzativa

La componente di sicurezza e' regolata da un sistema strutturato e controllato di ruoli, responsabilita', processi e procedure del SGSI formalizzato nel Piano di Sicurezza.

Con riferimento ai principi della ISO27001, il modello logico delle responsabilita': le mansioni sono assegnate alle figure/funzioni che cooperano nell'erogazione dei processi e servizi compresi nel perimetro del SGSI e sono raggruppate in tre diverse componenti: organizzativa (assegnata ai team SGSI), operativa (assegnata ai team SOC e Continuita' Operativa), controllo e improvement (assegnata ai team SGSI). Il Comitato per la Sicurezza ha

il compito di indirizzare in modo efficace anche tutti gli aspetti organizzativi. Ad esempio, vengono definite ed attuate, in linea con le prescrizioni della ISO 27001: le procedure codificate e differenziate per l'accesso fisico agli edifici ed ai locali in cui sono situati gli apparati di erogazione dei servizi; le procedure di classificazione delle informazioni; le procedure di gestione, backup e restore, conservazione e cancellazione delle informazioni.

Il modello organizzativo per la sicurezza e' quindi articolato in:

Responsabile della Sicurezza, che coordina tutti i gruppi di lavoro in ambito security;

Comitato per la Sicurezza, un elemento di Governo in cui si concentrano competenze legali, IT, di sicurezza, procedurali;

Il team del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) che svolge le attivita' di pianificazione, implementazione delle contromisure, verifica e miglioramento continuo previsti dal sistema di gestione certificato ISO27001.