Piano Triennale per l'Informatica 2022-2024

Stazione Zoologica "Anton Dohrn"
Istituto Nazionale di Biologia, Ecologia e Biotecnologie Marine

(Approvato con delibera del Consiglio di Amministrazione n. 53 del 26/04/2022)

Piano Triennale per l'Informatica 2022-2024
Stazione Zoologica Anton Dohrn

INTRODUZIONE

Il Piano Triennale per l'informatica nella Pubblica Amministrazione (di seguito indicato Piano Triennale o Piano o PT) costituisce il documento strategico realizzato da AgID per promuovere la trasformazione digitale del Paese e, in particolare, quella della Pubblica Amministrazione italiana, in un'ottica di riqualificazione della spesa per conseguire risparmi da reimpiegare in investimenti in materia d'innovazione tecnologica fissando una serie di obiettivi e linee d'azione cui le Amministrazioni devono ispirarsi per pianificare e programmare le azioni di digitalizzazione nel corso del triennio attraverso un proprio piano.

Tale piano utilizza gli obiettivi e le linee d'azione del Piano nazionale per valutare il proprio grado di adeguatezza e per programmare le azioni nel medio periodo.

L'aggiornamento del Piano rappresenta la naturale evoluzione dei tre Piani Nazionali precedenti. La prima edizione (2017-2019) poneva l'accento sull'introduzione del modello strategico dell'informatica nella PA, la seconda edizione (2019-2021) si proponeva di dettagliare l'implementazione del modello strategico, la terza edizione (2020-2022) era focalizzata sulla realizzazione delle azioni previste (circa 200 nell'arco dei tre anni) e sul monitoraggio dei risultati.

L'aggiornamento (redatto in collaborazione con il Dipartimento per la Trasformazione Digitale e PagoPA S.p.A), rappresenta la naturale evoluzione della precedente edizione introducendo alcuni elementi di novità, tra i quali la previsione di obiettivi e risultati attesi connessi all'attuazione del Piano nazionale di Ripresa e Resilienza (PNRR) al quale il Piano si collega attraverso specifici progetti come il Single Digital Gateway (SDG) e la Piattaforma Nazionale Dati (PDND) e l'adozione di un nuovo modello di vigilanza attiva e collaborativa coerente con il nuovo mandato istituzionale dell'Agenzia in materia di accertamento delle violazioni e sanzionatorio in riferimento agli obblighi di transizione digitale.

Il presente documento rappresenta il Piano per l'informatica della Stazione Zoologica Anton Dohrn (di seguito SZN o Ente), coerentemente con gli strumenti di programmazione e gestione (DUP - PTPCT - PEG) e persegue un cambiamento sostenibile verso la trasformazione digitale attraverso specifiche linee d'azione, tenendo conto delle dotazioni d'infrastrutture fisiche e immateriali attualmente disponibili presso la SZN. Il documento, dopo una introduzione ed una disamina del contesto nel quale si colloca, è suddiviso in sette sezioni ed altrettanti obiettivi declinati rispetto alla specifica componente descritta nella sezione di riferimento (in coerenza con il PT AgID).

Il presente Piano si integra con il Regolamento Interno per l'utilizzo degli strumenti, servizi e risorse informatiche della Stazione Zoologica Anton Dohrn approvato con delibera CdA n. 27 del 12/03/2020. La redazione è affidata al Responsabile della Transizione Digitale della SZN, i cui compiti previsti dall'Art. 17 comma 1 del D.Lgs. 82 del 7 marzo 2005 sono inclusi nei compiti del Responsabile dell'Ufficio Servizi Informatici & Statistici (SIST) istituito come da Delibera del Consiglio di Amministrazione della SZN n.16 del 16 novembre 2018.

IL CONTESTO

La strategia europea, nazionale e locale

La strategia del Piano è quella di favorire lo sviluppo di una società digitale, dove i servizi mettono al centro la ricerca, i cittadini e le imprese, attraverso la digitalizzazione della pubblica amministrazione che costituisce il motore di sviluppo per tutto il Paese, promuovendo lo sviluppo sostenibile, etico ed inclusivo, attraverso l'innovazione e la digitalizzazione e contribuendo alla diffusione delle nuove tecnologie digitali.

Principi Guida

I principi guida del Piano sono:

a. *Cloud first*: le PA, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi devono adottare il cloud come prima opzione;
b. *Digital & mobile first*: i servizi, che devono essere accessibili in via esclusiva con sistemi di identità digitale definiti dalla normativa assicurando almeno l'accesso tramite SPID;
c. Inclusività ed accessibilità;
d. *Once only*: le PA non devono chiedere ai cittadini e alle imprese informazioni già fornite;
e. *Open data*: il patrimonio informativo della PA è un bene fondamentale per lo sviluppo del Paese e deve essere valorizzato e reso disponibile in forma aperta e interoperabile;
f. *Open source*: le PA devono prediligere l'utilizzo di software con codice aperto o nel caso di software sviluppato in house il codice sorgente deve essere reso disponibile.
g. *Sicurezza e privacy by design*: i servizi digitali devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali;
h. *Transfrontaliero by design*: le pubbliche amministrazioni devono rendere disponibili a livello transfrontaliero i servizi pubblici digitali rilevanti;
i. *User-centred*, *data driven* e agile: le amministrazioni sviluppano i servizi digitali, prevedendo modalità agili, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni.

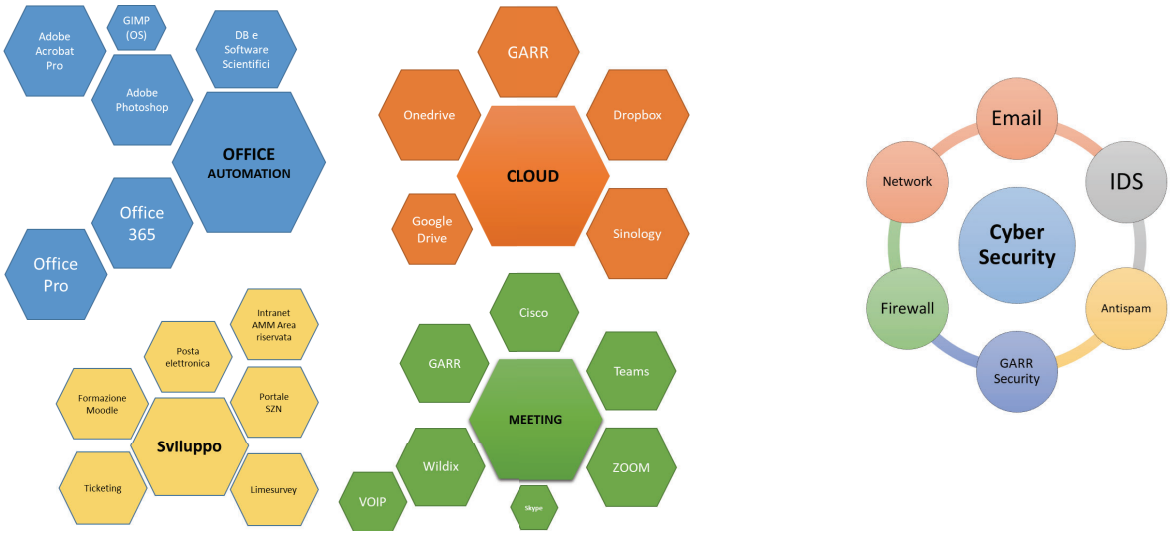
L'organizzazione dell'Ente per la trasformazione digitale

Il Piano triennale pone l'accento sul ruolo del Responsabile della Transizione al digitale per perseguire una concreta inversione del paradigma lavorativo nella PA dove è "il processo analizzato e rivisto a guidare l'informatizzazione la quale sarà, quindi, applicata ad un contesto di cambiamento organizzativo, ottenendo da una parte un effettivo risparmio e dall'altra generando fiducia nei sistemi informatici e nelle tecnologie".
Entro il mese di gennaio di ogni anno il RTD, in sede di aggiornamento del PTI, propone al Consiglio di Amministrazione una relazione sullo stato di avanzamento del PTI.
La programmazione del PTI deve essere coerente con:
- obiettivi di mappatura e digitalizzazione dei processi;
- attivazione dei servizi online;
- sensibilizzazione degli utenti all'impiego dell'identità digitale;
- migrazione/implementazione della modulistica in appositi form compilabili online;
- utilizzo dei servizi in cloud;
- potenziamento delle infrastrutture.

Tutte queste azioni integrano una maggiore tracciabilità e trasparenza dei processi per tipologia di procedimento, rispettivamente al fine della prevenzione dalla corruzione, come da ultimo evidenziato a pag. 18 – box 4 dell'All. 1 al PNA 2019 recante "Indicazioni metodologiche per la gestione dei rischi corruttivi" ed al fine di rendere realmente funzionale l'assolvimento dell'obbligo di pubblicazione nella sezione "Amministrazione trasparente" del sito web istituzionale dei contenuti obbligatori ai sensi dell'art. 35 del D.Lgs.33/2013, (tipologie dei procedimenti), distribuendo i relativi contenuti in specifiche pagine web che guidino la navigazione dell'utente verso un'esperienza di fruizione dei servizi online realmente intuitiva ed efficace.
In sede di PEG e PDO i programmi del DUP saranno declinati in specifici obiettivi di qualità, i cui indicatori di produttività dovranno consentire di misurare il grado di digitalizzazione dei processi raggiunto, oltre al grado di soddisfazione dell'utenza. Tali azioni sono quasi tutte trasversali, nel senso che non riguardano solo chi si occupa di informatica, ma tutti i diversi servizi dell'Ente.

Di seguito sono schematizzati i sistemi e le piattaforme digitali attualmente in uso alla SZN e che necessitano di implementazione come dettagliato nelle sezioni successive (sono evidenziati in giallo i sistemi che sono di prossima integrazione e che impatteranno sul bilancio di previsione dell'esercizio 2022 e del 2023).

Sistema ERP SZN 2021				
Ufficio Risorse Umane		***Ufficio Contabilità, Finanza, Bilancio e Cassa***		***Servizi Generali***
Marcatempo		Ordini		Flusso Documentale/Scrivania digitale
Tesserini e Badge		Pagamenti		Protocollo Informatico
Cedolini e CU		COAN COGE		Conservazione
Carriera		Gare		Identità Digitale
Missioni		Progetti		Firma digitale
Bandi e Concorsi		Inventario		Cartellino e Accessi
				Intranet AMM-Personale
				Performance



Enterprise Resource Planning (ERP) – L'insieme di piattaforme in cloud della SZN e l'ambiente di cyber security con dettagliati i sistemi su cui impattano i servizi.

SEZIONE 1. Le prospettive di sviluppo dei servizi nel contesto digitale dell'Ente

Il miglioramento della qualità dei servizi digitali costituisce la premessa indispensabile per l'incremento del loro utilizzo da parte sia degli utenti interni dell'Ente, che degli utenti esterni, siano essi cittadini, imprese o altre PA.

In questo processo di trasformazione digitale è essenziale che i servizi abbiano un chiaro valore per l'utente. Ciò implica anche un'adeguata semplificazione dei processi interni alle PA, con il necessario supporto di efficienti procedure digitali.

Occorre quindi agire su più livelli attraverso:

1. un utilizzo più consistente di soluzioni *Software as a Service* (SaaS) già esistenti;
2. il riuso e la condivisione di software e competenze tra le diverse amministrazioni;
3. l'adozione di modelli e strumenti validati a disposizione di tutti;
4. il costante monitoraggio da parte delle PA dei propri servizi online.

A tale scopo il presente Piano, di concerto con il CAD, pone l'accento sulla necessità di mettere a fattor comune le soluzioni applicative adottate dalle diverse amministrazioni al fine di ridurre la frammentazione che ritarda la crescita dei servizi. Si richiama quindi l'importanza di fornire servizi completamente digitali, progettati sulla base delle semplificazioni di processo abilitate dalle piattaforme di cui alla Sezione 3, del principio *cloud first*, sia in termini tecnologici, sia in termini di acquisizione dei servizi di erogazione in forma SaaS ove possibile, da preferirsi alla conduzione diretta degli applicativi. È cruciale infine il rispetto degli obblighi del CAD in materia di *open source* al fine di massimizzare il riuso del software sviluppato per conto della PA riducendo i casi di applicativi utilizzati da una singola PA e non condivisi tra più soggetti siano essi afferenti a strutture interne all'Ente siano profili trasversali tra diverse PA. Per incoraggiare tutti gli utenti a privilegiare il canale online rispetto a quello esclusivamente fisico, è necessario migliorare l'inclusività dei servizi in modo che essi siano utilizzabili da qualsiasi dispositivo.

Per il monitoraggio dei propri servizi, la SZN può utilizzare Web Analytics Italia, una piattaforma nazionale *open source* che offre rilevazioni statistiche su indicatori utili al miglioramento continuo dell'esperienza utente.
Nel caso il servizio richieda un accesso da parte dell'utente esterno alla SZN è necessario che sia consentito attraverso un sistema di autenticazione previsto dal CAD assicurando l'accesso almeno tramite SPID. Allo stesso modo, se è richiesto un pagamento, tale servizio dovrà essere reso disponibile anche attraverso il sistema di pagamento pagoPA.

SEZIONE 2. Il trattamento dei Dati

La valorizzazione del patrimonio informativo pubblico è un obiettivo strategico per la pubblica amministrazione, soprattutto per affrontare efficacemente le nuove sfide dell'economia dei dati (data economy), supportare la costruzione del mercato unico europeo per i dati definito dalla Strategia europea in materia di dati, garantire la creazione di servizi digitali a valore aggiunto per cittadini, imprese e, in generale, tutti i portatori di interesse e fornire ai data policy maker strumenti data-driven da utilizzare nei processi decisionali.

A tal fine, è necessario ridefinire una nuova *data governance* coerente con la Strategia Europea e con il quadro delineato dalla nuova Direttiva Europea sull'apertura dei dati e il riutilizzo dell'informazione del settore pubblico. È quindi opportuno individuare quanto prima le principali problematiche e sfide che l'attuale *data governance* del patrimonio informativo pubblico pone per delineare le motivazioni e gli obiettivi di una Strategia nazionale dati, anche in condivisione con i portatori di interesse pubblici e privati. Un asset fondamentale tra i dati gestiti dalle pubbliche amministrazione è rappresentato dalle banche dati di interesse nazionale (art. 60 del CAD): la *data governance* deve favorire l'accesso alle stesse per agevolare la constatazione degli stati relativi alle persone fisiche e alle persone giuridiche.

SEZIONE 3. Le Piattaforme digitali

Il Piano triennale per l'informatica nella Pubblica Amministrazione 2022-2024, riprende il concetto di Piattaforme della Pubblica Amministrazione, ossia piattaforme tecnologiche che offrono funzionalità fondamentali, trasversali, abilitanti e riusabili nella digitalizzazione dei processi e dei servizi della PA.
Le Piattaforme, attraverso i loro strumenti consentono di ridurre il carico di lavoro delle pubbliche amministrazioni, sollevandole dalla necessità di dover realizzare ex novo funzionalità, riducendo i tempi e i costi di attuazione dei servizi, garantendo maggiore sicurezza informatica ed alleggerendo la gestione dei servizi della pubblica amministrazione. Si tratta quindi di piattaforme tecnologiche che nascono per supportare la razionalizzazione dei processi di back-office della PA, al fine di migliorare l'efficienza e generare risparmi economici, per favorire la semplificazione e la riduzione degli oneri amministrativi a carico di imprese, professionisti e cittadini, nonché per stimolare la creazione di nuovi servizi digitali.

Le piattaforme favoriscono la realizzazione di processi distribuiti e la standardizzazione dei flussi di dati tra amministrazioni e all'interno dei Dipartimenti/Servizi/Uffici dell'Ente.

Infine, il concetto di Piattaforma cui fa riferimento il Piano triennale comprende non solo piattaforme abilitanti a livello nazionale e di aggregazione territoriale, ma anche piattaforme che possono essere utili per più tipologie di servizi/uffici dell'Ente o piattaforme che raccolgono e riconciliano i servizi delle amministrazioni, sui diversi livelli di competenza. È il caso, ad esempio, delle piattaforme di intermediazione tecnologica sui pagamenti disponibili sui territori regionali che si raccordano con il nodo nazionale pagoPA o le piattaforme di ticketing (vedi Obiettivo 7.1). Il Piano 2022-2024 perfeziona l'utilizzo delle piattaforme promosse nei Piani precedenti che consentono di razionalizzare i servizi per le amministrazioni ed i cittadini, quali la Piattaforma IO e la Piattaforma digitale nazionale dati (PDND) per valorizzare il patrimonio informativo pubblico attraverso l'introduzione di tecniche moderne di analisi di grandi quantità di dati (*BigData*). Il Piano prosegue inoltre nel percorso di evoluzione delle piattaforme esistenti (es. SPID, pagoPA, ecc.) e individua una serie di azioni volte a promuovere i processi di adozione, ad aggiungere nuove funzionalità e ad adeguare costantemente la tecnologia utilizzata e i livelli di sicurezza. Le linee di azione definite nella precedente edizione del Piano triennale restano valide fino al loro compimento; con la presente edizione si intendono identificare nuove opportunità ed aree di intervento.
La SZN utilizza inoltre la piattaforma messa a disposizione delle PA dall'Istituto Nazionale di Statistica per la rilevazione annuale di informazioni, dati e documenti necessari alla classificazione di unità economiche nei settori istituzionali stabiliti dal Sistema Europeo del Conti 2010.

Ognuna delle piattaforme indicate è caratterizzata dalla presenza di uno o più responsabili a livello nazionale o regionale e di diversi soggetti di riferimento che ne curano lo sviluppo, l'evoluzione e la gestione.

SEZIONE 4. Le Infrastrutture

Lo sviluppo delle infrastrutture digitali è parte integrante della strategia di modernizzazione del settore pubblico poiché queste sostengono l'erogazione sia di servizi pubblici a cittadini e imprese sia di servizi essenziali per il Paese. Tali infrastrutture devono essere affidabili, sicure, energeticamente efficienti ed economicamente sostenibili. L'evoluzione tecnologica espone, tuttavia, i sistemi a nuovi e diversi rischi, anche con riguardo alla tutela dei dati personali. L'obiettivo di garantire una maggiore efficienza dei sistemi non può essere disgiunto dall'obiettivo di garantire contestualmente un elevato livello di sicurezza delle reti e dei sistemi informativi utilizzati dalla Pubblica amministrazione.

Tuttavia, come rilevato da AGID attraverso il Censimento del Patrimonio ICT della PA, molte infrastrutture della PA risultano prive dei requisiti di sicurezza e di affidabilità necessari e, inoltre, sono carenti sotto il profilo strutturale e organizzativo. Ciò espone il Paese a numerosi rischi tra cui quello di interruzione o indisponibilità dei servizi e quello di attacchi cyber con conseguente accesso illegittimo da parte di terzi a dati (o flussi di dati) particolarmente sensibili o perdita e alterazione degli stessi dati.

Lo scenario delineato pone l'esigenza immediata di attuare un percorso di razionalizzazione delle infrastrutture per:

1. garantire la sicurezza dei servizi erogati tramite infrastrutture classificate come gruppo B, mediante la migrazione degli stessi verso data center più sicuri e verso infrastrutture e servizi cloud qualificati da AGID secondo il modello Cloud della PA;
2. evitare che le amministrazioni costruiscano nuovi data center al fine di ridurre la frammentazione delle risorse e la proliferazione incontrollata di infrastrutture con conseguente moltiplicazione dei costi.

Per approfondimenti sulla strategia governativa per il cloud è consultabile il sito https://cloud.italia.it/.

Con riferimento alla classificazione dei data center di cui alla Circolare AGID 1/2019, ai fini della strategia di razionalizzazione dei data center le categorie "infrastrutture candidabili ad essere utilizzate da parte dei PSN" e "Gruppo A" sono rinominate "A".

Al fine di consolidare e mettere in sicurezza le infrastrutture digitali delle pubbliche amministrazioni è definito il Polo Strategico Nazionale delle Infrastrutture Digitali (PSN) ovvero l'insieme delle infrastrutture digitali localizzate all'interno del territorio nazionale, ad alta disponibilità, che garantiscono elevati livelli di sicurezza, affidabilità ed efficienza energetica. Tali infrastrutture ospitano anche i beni strategici ICT conferiti al perimetro di sicurezza cibernetica nazionale dalle amministrazioni che non dispongono di data center classificati come "A". In particolare, con riferimento alla classificazione dei data center di cui alla Circolare AGID 1/2019, il percorso di razionalizzazione prevede che:

- le amministrazioni centrali che, al momento dell'approvazione del presente Piano, erogano servizi tramite infrastrutture classificate gruppo B, migrano i loro servizi verso una infrastruttura in grado di garantire requisiti di qualità sufficienti, scegliendo tra le infrastrutture del PSN e le infrastrutture e i servizi cloud qualificati da AGID;
- le amministrazioni centrali che, al momento dell'approvazione del presente Piano, erogano servizi tramite infrastrutture classificate "A" possono continuare ad erogare tali servizi tramite queste infrastrutture, potendo eventualmente consolidare nelle stesse i propri data center di gruppo B.

Al fine di facilitare le amministrazioni nell'attuazione del percorso di migrazione:

- è stato pubblicato il Manuale di abilitazione al Cloud nell'ambito del Programma nazionale di abilitazione al cloud;
- è stata pubblicata da Consip la Gara a procedura aperta per l'affidamento di un Accordo Quadro per la fornitura di servizi cloud IaaS e PaaS in un modello di erogazione pubblico nonché per la prestazione di servizi connessi, servizi professionali di supporto all'adozione del cloud, servizi professionali tecnici per le PA. L'Accordo Quadro consentirà alle PA di ridurre in modo significativo i tempi di approvvigionamento di servizi public cloud IaaS e PaaS e di servizi professionali per le PA che necessitano di reperire sul mercato le competenze necessarie per attuare quanto previsto nel manuale di abilitazione al cloud.

Per realizzare un'adeguata evoluzione tecnologica e di supportare il paradigma cloud, favorendo altresì la razionalizzazione delle spese per la connettività delle PA, è necessario anche aggiornare il modello di connettività.
Tale aggiornamento, inoltre, sarà teso a rendere disponibili alle PA servizi di connettività avanzati, atti a potenziare le prestazioni delle reti delle PA e a soddisfare la più recente esigenza di garantire lo svolgimento del lavoro agile in sicurezza.

SEZIONE 5. Sicurezza informatica

I servizi digitali erogati dalla Pubblica Amministrazione sono cruciali per il funzionamento del Paese. La minaccia cibernetica cresce continuamente in quantità e qualità, determinata anche dall'evoluzione delle tecniche informatiche volte a ingannare gli utenti finali dei servizi digitali sia interni alla PA che fruitori dall'esterno.

L'esigenza per la PA di contrastare tali minacce diventa fondamentale in quanto garantisce non solo la disponibilità, l'integrità e la riservatezza delle informazioni proprie del Sistema informativo della Pubblica Amministrazione, ma è il presupposto per la protezione del dato che ha come conseguenza diretta l'aumento della fiducia nei servizi digitali erogati dalla PA.

Punti focali di questa sezione sono le tematiche relative al Cyber Security Awareness, in quanto da tale consapevolezza possono derivare le azioni organizzative necessarie a mitigare il rischio connesso alle potenziali minacce informatiche.

Considerando quindi che il punto di accesso ai servizi digitali è rappresentato dai portali istituzionali delle pubbliche amministrazioni, al fine di realizzare un livello omogeneo di sicurezza, la sezione definisce alcune azioni concrete in tale ambito.

Infine, la sezione si prefigge di supportare le altre sezioni del piano sulle tematiche trasversali di sicurezza informatica, attraverso l'emanazione di linee guida e guide tecniche.

SEZIONE 6. Smart Working

Il lavoro agile supera la tradizionale logica del controllo sulla prestazione, ponendosi quale patto fiduciario tra l'Amministrazione e il lavoratore, basato sul principio guida "*far but close*", ovvero "lontano ma vicino" sottolineando la collaborazione tra l'Amministrazione e i lavoratori a prescindere dal luogo, dal tempo e dalle modalità che questi ultimi scelgono per raggiungere gli obiettivi perseguiti dall'Amministrazione.

Tale principio si basa sui seguenti fattori:
• Flessibilità dei modelli organizzativi;
• Autonomia nell'organizzazione del lavoro;
• Responsabilizzazione sui risultati;
• Benessere del lavoratore;
• Utilità per l'Amministrazione;
• Tecnologie digitali che consentano e favoriscano il lavoro agile;
• Cultura organizzativa basata sulla collaborazione e sulla riprogettazione di competenze e comportamenti;
• Organizzazione in termini di programmazione, coordinamento, monitoraggio, adozione di azioni correttive;
• Equilibrio in una logica *win-win*: l'amministrazione consegue i propri obiettivi e i lavoratori migliorano il proprio "Work-life balance".

Tra questi fattori, rivestono un ruolo strategico la cultura organizzativa e le tecnologie digitali in una logica di gestione del cambiamento organizzativo per valorizzare al meglio le opportunità rese disponibili dalle nuove tecnologie.

Le tecnologie digitali sono fondamentali per rendere possibili nuovi modi di lavorare; sono da considerarsi, quindi, un fattore indispensabile del lavoro agile. Il livello di digitalizzazione permette di creare spazi di lavoro digitali virtuali nei quali la comunicazione, la collaborazione e la socializzazione non dipendono da orari e luoghi di lavoro; affinché questo avvenga in modo efficace, occorre far leva sullo sviluppo di competenze digitali trasversali ai diversi profili professionali.

Ma ancor prima della digitalizzazione, le esperienze di successo mostrano come la vera chiave di volta sia l'affermazione di una cultura organizzativa basata sui risultati, capace di generare autonomia e responsabilità nelle persone, di apprezzare risultati e merito di ciascuno.

È evidente, quindi, come il tema della misurazione e valutazione della performance assuma un ruolo strategico nell'implementazione del lavoro agile, ruolo che emerge anche dalla disposizione normativa che per prima lo ha introdotto nel nostro ordinamento. È, infatti, presumibile che il SMVP debba essere aggiornato in coerenza con la nuova organizzazione del lavoro che l'amministrazione ha adottato. Una riflessione particolare è richiesta in relazione alla performance individuale. Non solo perché lo svolgimento della prestazione in modalità agile impone ancor più la necessità di individuare in maniera puntuale i risultati attesi, sia in relazione all'attività svolta che ai comportamenti, ma anche perché deve essere chiaro che il sistema di misurazione e valutazione è unico e prescinde dal fatto che la prestazione sia resa in ufficio, in luogo diverso o in modalità mista. Si possono utilizzare indicatori ad hoc per il lavoro agile, ma le dimensioni delle performance devono fare riferimento alle Linee Guida 1/2017 e 2/2017 del Dipartimento della funzione pubblica ed essere le stesse per tutte le strutture organizzative e i dirigenti e dipendenti dell'amministrazione.

Le predette criticità si sono inevitabilmente ripresentate quando l'emergenza sanitaria ha costretto le amministrazioni a utilizzare in maniera estesa il lavoro agile.

Contesto operativo e funzionale

L'emergenza epidemiologica COVID-19 ha costretto tutte le PA a sperimentare il lavoro agile (LA) senza il preventivo adattamento della struttura organizzativa e dei processi di lavoro. Dall'approfondimento realizzato dal Politecnico di Milano su incarico della Presidenza del Consiglio dei Ministri – Dipartimento per le pari opportunità nell'ambito del progetto "Lavoro agile per il futuro della PA", a valere sul PON "Governance e Capacità istituzionale" 2014/2020, Asse 1, Azione 1.3.5 ("Lavoro agile per il futuro della PA - Approfondimento delle esperienze più significative di lavoro agile realizzate a livello pubblico e privato sia in ambito nazionale sia internazionale") emerge infatti come la radice profonda del LA stia nel superamento di alcuni assunti

dell'organizzazione tradizionale e nella loro sostituzione con principi nuovi e più coerenti con le opportunità offerte dalle nuove tecnologie e le nuove esigenze di individui e organizzazioni.
Con il D.L. n. 76/2020 convertito in legge 11/09/20, N. 120, il processo di trasformazione digitale della PA, ha subito una forte accelerazione, (note agli artt. 24-37 del DL) giustificata dal fatto che il pieno ed efficace dispiegarsi del LA necessita di un'estesa digitalizzazione dei flussi documentali, per una reale evoluzione digitale del back office e del front office e la conseguente gestione e conservazione dei fascicoli informatici. Sempre lo stesso decreto (note agli artt. 12-13 del DL) in modifica alla L. 241/90, apporta significative modifiche riguardo al procedimento amministrativo e conseguenti responsabilità. All'art. 15 infine il decreto ribadisce, attualizzando i termini dell'art. 24 del D.L. 24/06/2014, n. 90, convertito, con modificazioni, dalla legge 11/08/2014, n. 114, la necessità di giungere alla predisposizione di un'"Agenda della semplificazione amministrativa e moduli standard".

Per incentivare una sensibilità culturale del dipendente verso nuovi paradigmi di "produttività" e favorire un cambiamento culturale nelle relazioni Ente-dipendente, il LA, se considerato quale modalità di lavoro a regime anche nella fase post-emergenza, potrebbe costituire un profondo elemento di innovazione della PA, purché sostenuto da un sistemico mutamento organizzativo e dall'evoluzione tecnologica dei sistemi informativi.

SEZIONE 7. Reingegnerizzazione e aggiornamento applicativi

La gestione documentale, affinché possa essere efficiente e sicura, deve essere necessariamente presidiata da specifiche procedure e strumenti informatici. La vita del documento deve seguire un percorso logico secondo i principi generali applicabili in materia di trattamento dei dati personali, anche mediante un'adeguata analisi del rischio. Un corretto processo di gestione del documento sin dalla fase di formazione rappresenta, infatti, la migliore garanzia per l'adempimento degli obblighi tipici della gestione degli archivi.

OBIETTIVI 1 - sviluppo dei servizi nel contesto digitale

Obiettivo 1.1: Migliorare la capacità di generare ed erogare servizi digitali

Adesione a Web Analytics Italia per migliorare il processo evolutivo dei propri servizi online
Status: linea d'azione da completare entro fine anno.
Note: attivare lo strumento previsto da Agid.

Principi Cloud First: SaaS First, acquisto servizi cloud solo se qualificati da AGID
Status: linea d'azione da completare entro fine anno.
Note: inserito nelle procedure di acquisizione.

Adeguamento procedure di procurement alle linee guida di AGID sull'acquisizione del software e al CAD (artt. 68 e 69)
Status: linea d'azione completata.
Note: inserito nelle procedure di acquisizione.

Adesione al programma di abilitazione al cloud
Status: linea d'azione in corso
Note: analisi del budget necessario

Utilizzo preferenziale del software *open source*
Status: linea d'azione in corso
Note: nei capitolati tecnici deve essere inserita la clausola che obbliga l'aggiudicatario al rilascio dei codici sorgenti aperti nel caso in cui il software sia commissionato e realizzato ad hoc.

Obiettivo 1.2: Migliorare l'esperienza d'uso e l'accessibilità dei servizi

Riferimento alle linee guida di design nei procedimenti di acquisizione di software
Status: linea d'azione in corso
Budget richiesto: linea d'azione svolta con risorse interne
Note: nei capitolati tecnici deve essere inserita la clausola che obbliga l'aggiudicatario ad adattare il software alle linee guida di design e visione dell'Ente.

Comunicazione ad AGID dell'esito dei test di usabilità del proprio sito istituzionale
Status: linea d'azione in corso - Pubblicazione dichiarazione di accessibilità

Pubblicare gli obiettivi di accessibilità sul proprio sito
Status: linea d'azione in corso - Comunicazione ad AGID dell'uso dei modelli per lo sviluppo web per i propri siti istituzionali

Pubblicazione della dichiarazione di accessibilità per le APP mobili
Status: linea d'azione in corso
Note: nei capitolati tecnici deve inserita la clausola che obbliga l'aggiudicatario ad adeguare le app alle prescrizioni inerenti l'accessibilità. Attualmente non sono state rilasciate app specifiche per le finalità dell'Ente.

OBIETTIVI 2 – trattamento dei dati

Obiettivo 2.1: Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese

Individuazione dei dataset di tipo dinamico da rendere disponibili in open data
Status: linea d'azione in corso
Budget richiesto: linea d'azione svolta con risorse interne
Note: sono in corso le valutazioni per la pubblicazione di dataset scientifici. L'azione deve essere svolta di concerto con la Governance della SZN ed i Direttori di Dipartimento nel rispetto della divulgazione ed in generale con le finalità di terza missione dell'Ente.

Adeguamento dei sistemi che si interfacciano alle banche dati di interesse nazionale
Status: linea d'azione in corso
Budget richiesto: linea d'azione da finanziare
Note: Nel rifacimento e ammodernamento dei sistemi informativi si terrà conto del budget necessario.

Obiettivo 2.2: Aumentare la qualità dei dati e dei metadati

Uniformazione dei propri sistemi di metadati alle specifiche nazionali
Status: linea d'azione in corso
Budget richiesto: linea d'azione svolta con risorse interne
Note: È necessario un approfondimento per valutare l'efficacia del servizio interno per la predisposizione dell'infrastruttura e pubblicazione dei dataset o se necessario affidare la commessa a terzi.

Fornitura di indicazioni sul livello di qualità dei dati
Status: linea d'azione in corso
Budget richiesto: linea d'azione svolta con risorse interne
Note: Sono in fase di valutazione i parametri per l'elaborazione degli indicatori.

Obiettivo 2.3: Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati

Definizione delle "tipologie di dati"
Status: linea d'azione in corso
Budget richiesto: linea d'azione svolta con risorse interne
Note: Devono essere individuate le figure di responsabile del data team e il personale tecnico interno da dedicare all'analisi della tipologia dei dati. È in corso di valutazione l'individuazione degli altri componenti.

Partecipazione a interventi di formazione e sensibilizzazione sulle politiche open data
Status: linea d'azione in corso
Budget richiesto: linea d'azione svolta con risorse interne
Note: Sono in corso di valutazione i corsi specialistici di formazione adeguati.

Partecipazione alla definizione di metodologie per monitorare il riutilizzo dei dati aperti
Status: linea d'azione in corso
Budget richiesto: linea d'azione svolta con risorse interne
Note: Devono essere individuate le figure necessarie.

OBIETTIVI 3 – piattaforme digitali

Obiettivo 3.1: Favorire l'evoluzione delle piattaforme esistenti ed aumentare il grado di adozione delle piattaforme abilitanti esistenti da parte delle pubbliche amministrazioni

SPID
Status: linea d'azione in corso
Budget richiesto: spesa linea d'azione già impegnata (400 Euro)
Note: Sono stati integrati con SPID i servizi che necessitano di autenticazione esterna.

Piattaforma HelpDesk Maggioli
Status: linea d'azione in corso
Budget richiesto: spesa linea d'azione canone annuo di servizio (6000 Euro)

PEC
Status: linea d'azione in corso
Budget richiesto: spesa linea d'azione già impegnata (3.400,00 Euro)
Note: servizi PEC (Legalmail Enterprise, Legalmail Massiva, Legalinvoice - servizio di fatturazione).

Concorsi
Status: linea d'azione in corso
Budget richiesto: spesa linea d'azione già impegnata (4.000,00 Euro).
Note: Rinnovo annuale piattaforma concorsi Anthesi dal 01-06-2021 al 31-05-2022. Analisi in corso per adeguare il sistema alla piattaforma U-Gov (vedi schema moduli U-Gov come di seguito riportato).

Marcatempo
Status: linea d'azione in corso
Budget richiesto: spesa linea d'azione già impegnata (858,00 Euro).
Note: Rinnovo annuale piattaforma Selesta, controllo timbrature e marcatempo dal 01-03-2022 al 31-12-2021. Analisi in corso per adeguare il sistema alla piattaforma U-Gov (vedi schema moduli U-Gov come di seguito riportato).

PagoPA
Status: linea d'azione in corso
Budget richiesto: spesa linea d'azione già impegnata.
Note: Nel 2018 è stato affidato il servizio di attivazione della piattaforma. Deve essere nominato il referente PagoPA. Analisi in corso per adeguare il sistema alla piattaforma U-Gov (vedi schema moduli U-Gov come di seguito riportato).

Piattaforma Gestione Accessi
Status: linea d'azione in corso
Budget richiesto: spesa linea d'azione già impegnata (vedi schema moduli U-Gov come di seguito riportato).
U-GOV
Status: linea d'azione in corso
Budget richiesto: spesa linea d'azione già impegnata ma non fatturata (29,916.24 Euro)
Note: servizi U-GOV Contabilità, ODS Contabilità, Gestione Progetti, Allocazione Costi).

U-GOV Modulo Compensi
Status: linea d'azione in corso
Budget richiesto: spesa linea d'azione già impegnata ma non fatturata (3,200.00 Euro)

U-GOV CSA Giuridica
Status: linea d'azione in corso
Budget richiesto: spesa linea d'azione già impegnata ma non fatturata (5,000.00 Euro)

Viene di seguito riportato un prospetto dei costi sostenuti nel 2021, nell'esercizio corrente 2022 e previsti per il 2023 in riferimento ai moduli già in uso e da attivare con la piattaforma U-Gov di Cineca. Al momento della stesura

del presente PT i servizi Cineca per il 2022 non sono stati ancora fatturati permettendoci di ipotizzare un aggiornamento del contratto in essere n° 18029002 (Atto di affidamento per Servizi di attivazione e utilizzo del sistema U-GOV: aree funzionali Contabilità, Risorse umane, Gestione documentale, Ricerca, Pianificazione e controllo - Periodo 2019 - 2023).
Lo schema dei costi 2022 e 2023 tiene dunque conto di una ipotesi di aggiornamento contrattuale in funzione dei nuovi moduli da attivare e dell'accorpamento di alcuni di essi.
Secondo tale ipotesi le spese da sostenere nel 2022, con un aumento di circa il 2% rispetto al 2021, permetterebbero di attivare 12 nuovi moduli. Nel 2023 le spese complessive si ridurrebbero del 3% e 19 moduli attivi nell'ambito del sistema integrato U-GOV dell'Amministrazione Generale.

(*) da attivare				2021	2022	2023
	Ufficio Risorse Umane		U-GOV - Modulo Compensi	3,200.00	5,528.60	5,528.60
			U-GOV - CSA Giuridica	5,000.00	2,029.04	2,029.04
*		*costo di attivazione una tantum*	U-GOV I miei documenti		4,000.00	
*			U-GOV Web Il mio profilo		3,925.00	
*			U-GOV Web dati fiscali e previdenziali		8,800.00	
*			U-GOV Web Missioni		4,400.00	
*			U-GOV Gestione organico		1,800.00	
	Ufficio Contabilità, Finanza, Bilancio e Cassa		U-GOV - Allocazione Costi	38,000.00	29,916.24	29,916.24
			U-GOV - ODS Contabilità			
			U-GOV - Gestione Progetti			
			U-GOV Contabilità			
*			U-GOV - IRIS Repos/Open Archive	11,000.00		17,741.76
*			U-GOV - IRIS Activities and Project			6,721.25
		costo di attivazione una tantum	U-GOV - PagoAtenei (PagoPA) setup		3,500.00	
*			U-GOV - PagoAtenei (PagoPA)		4,475.30	4,475.30
	Servizi Generali		U-GOV - Canone Hosting	19,560.00	azzerato	
*			U-GOV - Connettore Titulus firma Digitale	10,000.00	10,000.00	10,000.00
*			U-GOV - Titulus			
*			U-GOV - Conserva			
		costo di attivazione una tantum	U-GOV - Progetto IDM (propedeudico per Titulus) setup		2,500.00	
*			U-GOV - Progetto IDM (propedeudico per Titulus)		3,650.00	3,650.00
			U-GOV - Canone Servizi		4,000.00	4,000.00
			TOTALE	86,760.00	88,524.18	84,062.19

OBIETTIVI 4 - infrastrutture

Obiettivo 4.1: Migliorare la qualità dei servizi digitali erogati dalle amministrazioni locali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili

Migrazione in cloud servizi infrastrutturali
Status: linea d'azione in corso
Budget richiesto: 30.000 Euro di spesa di investimento, 15.000 Euro annui di spesa corrente
Note: attualmente le risorse infrastrutturali relative alla posta elettronica, gestione credenziali, e storage condiviso sono on premise mentre video conferenze, office automation, strumenti di collaborazione, e strumenti per riunioni o presentazioni online sono gestite in cloud da società terze via Consip. La linea d'azione si propone una migrazione degli strumenti ancora in house verso il cloud con l'utilizzo di una piattaforma gestita in massima sicurezza. Tale piattaforma è ideale inoltre per la gestione delle attività lavorative in smart working.

Obiettivo 4.2: Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili

Migrazione in cloud applicativi
Status: linea d'azione in corso
Budget richiesto: 40.000 Euro di spesa di investimento, 1.000 di Euro di spesa corrente annui
Note: Nel data center, oltre agli applicativi infrastrutturali trattati nell'OB.4.1 vi sono una serie di applicativi realizzati ad hoc o in licenza d'uso istallati nell'ambiente di produzione del data center. La linea di azione si propone di utilizzare in Saas gli applicativi in licenza d'uso e di migrare su una piattaforma Iaas gli applicativi realizzati ad hoc (internamente o commissionati). La spesa di investimento copre le attività di migrazione, quella corrente le licenze Saas e lo Iaas.

Obiettivo 4.3: Migliorare l'offerta di servizi di connettività e telefonia per le PA

Aumento banda connettività sede principale
Status: linea d'azione in corso
Budget richiesto: 10.000 Euro di spesa di investimento

Aggiornamento infrastruttura di rete centro stella e rack di piano
Status: linea d'azione in corso
Budget richiesto: 100.000 Euro in spesa di investimento
Note: L'intervento prevede
• l'aggiornamento apparati di rete centro stella
• L'acquisto di un Software gestione router
• l'aggiornamento apparati dei rack di piano
• Le Licenze di gestione dei router
• La stesura e configurazione di un collegamento in fibra
• La manutenzione degli apparati.

Gestione rete sede centrale
Status: linea d'azione in corso
Budget richiesto: 22.000 Euro canone annuo

Gestione rete sedi territoriali
Status: linea d'azione in corso
Budget richiesto: 150.000 Euro canone annuo
Note: L'intervento prevede il canone per le sedi: 1) Casina del Boschetto, 2) Molosiglio; 3) Portici; 4) Ischia; 5) Palermo; 6) Messina; 7) Amendolara; 8) Roma; 9) Fano; 10) Genova.

Manutenzione rete sede centrale e sedi territoriali
Status: linea d'azione in corso

Budget richiesto: 20.000 Euro

Telefonia sede principale
Status: linea d'azione in corso
Budget richiesto: 20.000 Euro annui di spese correnti.

Telefonia sedi periferiche
Status: linea d'azione in corso
Budget richiesto: 10.000 Euro di spesa corrente ulteriore rispetto all'attuale
Note: nelle sedi territoriali è necessario procedere con i seguenti interventi:
Aggiornamento e integrazione della centrale telefonica di ogni sede (implementazione voip con vlan dedicata).
Dismissione vecchi apparati

OBIETTIVI 5 – sicurezza

Obiettivo 5.1: Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle Pubbliche Amministrazioni

Riferimento alle Linee guida sulla sicurezza nel procurement ICT nei procedimenti di acquisizione di beni e servizi ICT
Status: linea d'azione in corso
Budget richiesto: linea svolta con risorse interne
Note: nei capitolati tecnici deve essere inserito il requisito obbligatorio di aderenza alle linee guida di procurement ICT.

Utilizzo tool di Cyber Risk Assessment per l'analisi del rischio e la redazione del Piano dei trattamenti
Status: linea d'azione in corso
Budget richiesto: analisi spesa in corso.
Note: per questa linea d'azione è necessario un potenziamento per la gestione della sicurezza di una figura professionale; lo strumento è in fase di studio per valutarne la modalità di utilizzo più idonea al contesto di riferimento.

Formazione sulle tematiche di Cyber Security Awareness
Status: linea d'azione in corso
Budget richiesto: analisi spesa in corso.
Note: per questa linea d'azione è necessario l'utilizzo di un servizio che, attraverso indagini e campagne di spam/phishing fittizie, individui il grado di maturità dell'utenza e in base a questa programmi interventi formativi personalizzati.

Adeguamento alle Misure minime di sicurezza ICT per le pubbliche amministrazioni
Status: linea d'azione in corso
Budget richiesto: analisi spesa in corso.
Note: per questa linea d'azione devono essere valutate le difformità rispetto alle linee guida. Tali difformità possono essere in parte procedurali e in parte infrastrutturali. Le difformità strutturali verranno in parte superate attraverso la migrazione in cloud e in parte attraverso gli interventi specificati nella sezione 4 "Infrastrutture". Per le difformità procedurali è in corso la valutazione con il supporto dell'Ufficio interno di riferimento.

Obiettivo 5.2: Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

Consultazione della piattaforma Infosec aggiornata per rilevare le vulnerabilità (CVE) dei propri asset
Status: linea d'azione in corso
Budget richiesto: linea svolta con risorse interne
Note: l'attività sarà inserita nelle attività di servizio del personale interno dell'Ufficio SIST

Costante aggiornamento dei propri portali istituzionali e applicazione delle correzioni alle vulnerabilità
Status: linea d'azione in corso
Budget richiesto: analisi spesa in corso.

Note: Identificazione del personale necessario al mantenimento di tali risorse, attualmente in numero insufficienti allo scopo.

Aggiornamento sistema di backup
Status: linea d'azione in corso
Budget richiesto: 10.000 Euro come spesa di investimento
Note: l'attuale sistema di backup non è adeguatamente performante e sicuro. Per tutti gli applicativi non migrabili in cloud è necessario disporre di uno strumento ad hoc. Sono in corso le valutazioni tecnologico-infrastrutturali per una analisi di mercato.

Licenze EDR
Status: linea d'azione in corso
Budget richiesto: 15.000 Euro annui di spesa corrente
Note: utilizzo di agent che effettuano attività approfondite di EDR su macchine client e server. La stima dei costi riguarda 200 postazioni client e 50 server

Licenze Firewall
Status: linea d'azione in corso
Budget richiesto: 10.000 Euro come spesa di investimento, 5.000 Euro annui di spesa corrente
Note: l'attuale licenza non è sufficiente a garantire un adeguato livello di protezione per la sede principale e per le sedi territoriali. Entro il 2022 utilizzo di una distribuzione software open source basata su FreeBSD adatta per essere utilizzata come firewall/router, le spese ricorrenti saranno abbattute.

OBIETTIVI 6 – smart working

Obiettivo 6.1: Aumentare il livello di sicurezza informatica del collegamento da remoto

Acquisto licenze per collegamento sicuri in VPN
Status: linea d'azione in corso
Budget richiesto: 10.000 Euro annui in spesa corrente

Acquisto licenze di un sistema di autenticazione forte
Status: linea d'azione in corso
Budget richiesto: 10.000 Euro annui in spesa corrente
Note: per garantire la sicurezza nell'autenticazione con una certa flessibilità nel tipo e numero di fattori di autenticazione è necessario poter disporre di una piattaforma sicura di gestione dell'autenticazione; è stata effettuata solo una stima dei costi di tale linea di azione.

Obiettivo 6.2: Fornire strumenti di lavoro agli smart worker

Fornitura portatili
Status: linea d'azione in corso
Budget richiesto: 30.000 Euro di spesa di investimento

Spazio cloud per archiviazione documentale
Status: linea d'azione in corso - licenze Dropbox canone annuo 28.000 Euro
Budget richiesto: linea d'azione compresa nell'obiettivo OB.4.1. e finanziato tramite tali risorse

Software Office Automation
Status: linea d'azione in corso - licenze Office 365 Crui 15.000 Euro
Budget richiesto: linea d'azione compresa nell'obiettivo OB.4.1. e finanziato tramite tali risorse

Digitalizzazione procedimenti
Status: linea d'azione in corso
Budget richiesto: linea svolta con risorse interne
Note: sono in fase di valutazione una serie di procedimenti (già dematerializzati) da reingegnerizzare per favorirne l'uso da remoto.

Acquisto firme digitali
Status: linea d'azione in corso
Budget richiesto: 2.000 Euro in spesa in canone annuo
Note: acquisto di 10 firme digitali. Tale linea d'azione favorisce la dematerializzazione completa dei procedimenti in favore dei lavoratori agili.

Obiettivo 6.3: Formazione utenti

Erogazione corsi di formazione in materia di lavoro agile e competenze informatiche
Status: linea d'azione in corso
Budget richiesto: linea d'azione già finanziata da risorse interne
Note: La SZN ha aderito a "Syllabus" per la formazione digitale della PA con l'obiettivo di promuovere l'autoverifica delle competenze digitali del proprio personale e la promozione di formazione mirata rispetto ai fabbisogni formativi rilevati.

Obiettivo 6.4: Aumentare il livello di supporto agli utenti in lavoro agile

Implementazione di un help desk dedicato
Status: linea d'azione da definire
Budget richiesto: preventivare personale aggiunto in dotazione all'organico del SIST
Note: previsti un sistemista e due operatori di supporto e *incident management* aggiuntivi rispetto alla dotazione attuale.

OBIETTIVI 7 – aggiornamento applicativi

Obiettivo 7.1: Supportare i procedimenti amministrativi e la ricerca attraverso applicativi rispondenti alle necessità

Utilizzo di un portale per controllo di gestione e misurazione performances
Status: linea d'azione in corso
Budget richiesto: 6.000,00 Euro investimento e 6.000,00 Euro per canone annuale
Note: Servizio di abbonamento per l'utilizzo del software applicativo 'STRATEGIC PA', moduli Performance e Trasparenza, per un triennio, decorrenza 15-03-2022.

Implementazione del software di gestione documentale
Status: linea d'azione in corso
Budget già stanziato: Canone annuo 1.690 Euro
Note: software DOCUMATIC - Archiviazione Elettronica Documenti, che sarà sostituito dal modulo TITULUS di CINECA (vedi nota moduli Cineca – Titulus OB 3.1)

Portale Amministrazione Trasparenza
Status: linea d'azione in corso
Budget richiesto: Canone 36 mesi dal 02-02-2021 10.000,00 Euro
Note: sviluppi e aggiornamenti in corso, accorpamento e integrazione banche dati interne per rendere più efficiente e chiara l'esposizione all'esterno ai fini della trasparenza.

Gestione, evoluzione e manutenzione del portale istituzionale della SZN
Status: linea d'azione in corso;
Budget richiesto: 7.000,00 Euro per canone annuale;

Realizzazione portale Moodle
Status: linea d'azione in corso
Budget richiesto: realizzazione con risorse interne
Note: Studio di fattibilità in corso.

Realizzazione portale Ticketing
Status: linea d'azione in corso
Budget richiesto: realizzazione con risorse interne
Note: sviluppo in corso.

Ristrutturazione Intranet
Status: linea d'azione in corso
Budget richiesto: realizzazione con risorse interne
Note: studio di fattibilità in corso.

Aggiornamento versione LimeSurvey
Status: linea d'azione in corso
Budget richiesto: realizzazione con risorse interne

SEZIONE 8. Limitazioni all'applicazione del Piano

Per l'attuazione delle linee di intervento precedentemente descritte sono necessarie ulteriori risorse economiche rispetto a quelle attualmente assegnate, esplicitate all'interno dei diversi capitoli.
In particolare gli interventi prevedono:
• spese di investimento per la realizzazione delle attività;
• spese correnti per il mantenimento e consolidamento di quanto implementato.
Di seguito è schematizzata una tabella che riepiloga tutti i costi aggiuntivi dividendo le spese per obiettivi e linee di attività. Le somme sono al netto dell'IVA.
Allo stesso tempo per la gestione di tali attività saranno necessarie ulteriori risorse umane nell'ambito dell'Ufficio, pianificate nel fabbisogno di personale a cui si rimanda e una serie di interventi di ristrutturazione della macro-organizzazione che saranno proposti alla Direzione Generale.
Resta inteso che senza tali risorse e interventi il piano non è applicabile.

Ambito	Obiettivo	Linea d'azione	Spesa di investimento	Spesa corrente annua	Note (tutte le spese sono al netto di IVA)
Le Piattaforme	Ob. 3.1: Favorire l'evoluzione delle piattaforme esistenti ed aumentare il grado di adozione delle piattaforme abilitanti esistenti da parte delle pubbliche amministrazioni	SPID		400.00 €	
		Piattaforma HelpDesk Maggioli		6,000.00 €	
		PEC		3,400.00 €	
		Concorsi		4,000.00 €	
		Marcatempo		858.00 €	
		U-GOV Contabilità		29,916.24 €	non ancora fatturate, previsione sulle spese del 2021
		U-GOV - Gestione Progetti			
		U-GOV - Allocazione Costi			
		U-GOV - ODS Contabilità			
		U-GOV - Modulo Compensi		3,200.00 €	
		U-GOV - CSA Giuridica		5,000.00 €	
	Tot Ob. 3.1			**52,774.24 €**	
Le Infrastrutture	Ob. 4.1: Migliorare la qualità dei servizi digitali erogati dalle amministrazioni locali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili	Migrazione in cloud servizi infrastrutturali	30,000.00 €	15,000.00 €	
	TOT Ob. 4.1		30,000.00 €	15,000.00 €	
	Ob. 4.2: Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone	Migrazione in cloud applicativi	40,000.00 €	1,000.00 €	

Ambito	Obiettivo	Linea d'azione	Spesa di investimento	Spesa corrente annua	Note (tutte le spese sono al netto di IVA)
	l'aggregazione e la migrazione su infrastrutture sicure ed affidabili				
	TOT Ob. 4.2		40,000.00 €	1,000.00 €	
	Ob.4.3: Migliorare l'offerta di servizi di connettività e telefonia per le PA	Aumento banda connettività sede principale	10,000.00 €		
		Aggiornamento infrastruttura di rete centro stella e rack di piano	100,000.00 €		
		Gestione rete sede centrale		22,000.00 €	
		Gestione rete sedi territoriali	66,300.00 €	150,000.00 €	una tantum per Molosiglio e la Casina del Boschetto
		Manutenzione rete sede centrale e sedi territoriali		20,000.00 €	
		Telefonia sede principale		20,000.00 €	
		Telefonia sedi periferiche	10,000.00 €		
	TOT Ob.4.3		186,300.00 €	212,000.00 €	
TOT Infrastrutture			**256,300.00 €**	**228,000.00 €**	
Sicurezza informatica	Ob. 5.2: Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione	Aggiornamento sistema di backup	10,000.00 €		
		Licenze EDR		15,000.00 €	
		Licenze Firewall	10,000.00 €		
	TOT Ob.5.2		20,000.00 €	15,000.00 €	
Smart Working	Ob. 6.1: Aumentare il livello di sicurezza informatica del collegamento da remotoOB.7.1: Aumentare il livello di sicurezza informatica del collegamento da remoto	Acquisto licenze per collegamento sicuri in VPN		10,000.00 €	
		Acquisto licenze di un sistema di autenticazione forte		10,000.00 €	
	TOT Ob.6.1			20,000.00 €	
	Ob.6.2: Fornire strumenti di lavoro agli smart worker	Fornitura portatili	30,000.00 €		
		Spazio cloud per archiviazione documentale		28,000.00 €	

Ambito	Obiettivo	Linea d'azione	Spesa di investimento	Spesa corrente annua	Note (tutte le spese sono al netto di IVA)
		Software Office Automation		15,000.00 €	
		Acquisto firme digitali		2,000.00 €	
	TOT Ob.6.2		30,000.00 €	53,000.00 €	
TOT Smart Working			**30,000.00 €**	**73,000.00 €**	
Reingegnerizzazione e aggiornamento applicativi	Ob. 7.1: Supportare i procedimenti amministrativi e la ricerca attraverso applicativi rispondenti alle necessità	Portale per controllo di gestione e misurazione performances	6.000 €	6,000.00 €	
		Implementazione del software di gestione documentale		1,690.00 €	
		Portale Amministrazione Trasparenza		10,000.00 €	
		Portale istituzionale della SZN		7,000.00 €	
	TOT Ob.7.1		**6.000 €**	**24,690.00 €**	
TOT			292,300.00 €	378,464.24 €	

Appendice I - Acronimi

- AGID: Agenzia per l'Italia digitale;
- ANPR: Anagrafe Nazionale della Popolazione Residente, la banca dati nazionale nella quale è confluita l'anagrafe dell'Ente;
- API: Application Programming Interface (https://innovazione.gov.it/it/progetti/api/);
- BDNCP: Banca Nazionale Contratti Pubblici;
- CAD: Codice dell'Amministrazione digitale;
- Carta Nazionale Dei Servizi (CNS): il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni;
- CED: Centro Elaborazione Dati;
- CIE: Carta d'identità Elettronica, il documento d'identità munito di elementi per l'identificazione fisica del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare;
- Cittadinanza Digitale: l'insieme di diritti/doveri che, grazie al supporto di una serie di strumenti (l'identità, il domicilio, le firme digitali) e servizi, mira a semplificare il rapporto tra cittadini, imprese e pubblica amministrazione tramite le tecnologie digitali;
- Cloud Marketplace: è la piattaforma di AgID che espone i servizi e le infrastrutture qualificate da AgID secondo quanto disposto dalle Circolari AgID n. 2 e n.3 del 9 aprile 2018 (https://cloud-pa.readthedocs.io/it/latest/). All'interno del Cloud Marketplace è possibile visualizzare la scheda tecnica di ogni servizio che mette in evidenza le caratteristiche tecniche, il modello di costo e i livelli di servizio dichiarati dal fornitore in sede di qualificazione;
- Dichiarazione: l'atto giuridico con il quale un privato attesta alle pubbliche amministrazioni determinati stati, fatti o qualità che assumono rilevanza nell'ambito di procedimento amministrativo;
- Documento Amministrativo: ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa;
- Documento Analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti;
- Documento Informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
- DUP: Documento Unico di Programmazione;
- EDR: Endpoint Detection and Response;
- ENTE: la pubblica amministrazione che redige ed approva il presente piano di informatizzazione;
- Gestione Informativa Dei Documenti: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dall'Ente, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici;
- IaaS (Infrastructure-as-a-Service): modello nel quale vengono messi a disposizione risorse hardware virtualizzate, affinché l'utilizzatore possa creare e gestire, secondo le proprie esigenze, una propria infrastruttura sul cloud, senza preoccuparsi di dove siano allocate le risorse (https://docs.italia.it/italia/piano-triennale-ict/cloud-docs/it/stabile/cloud-della-pa.html#servizi-iaas-e-paas);
- ICT: Tecnologie dell'informazione e della comunicazione (Information and Comunication Tecnology);
- IO: applicazione del Ministero dell'Innovazione, finalizzata a fornire a tutti i cittadini dotati di smartphone servizi pubblici nazionali e locali. È un progetto Open Source in fase di sviluppo (https://developers.italia.it/it/io/);
- iPA: Indice dei domicili digitali della Pubblica Amministrazione;
- Istanza: l' atto giuridico con il quale un privato chiede alla pubblica amministrazione di avviare un procedimento amministrativo;
- Obiettivi Di Accessibilità (https://www.agid.gov.it/it/design-servizi/accessibilita/obiettivi-accessibilita) ;
- PaaS (Platform-as-a-Service): modello nel quale vengono situati i servizi di piattaforme online, grazie al quale un utente, di solito uno sviluppatore, può effettuare il deployment di applicazioni e servizi web che intende fornire. In questo caso l'utilizzatore può sviluppare ed eseguire le proprie applicazioni attraverso gli strumenti forniti dal provider, il quale garantisce il corretto funzionamento dell' infrastruttura sottostante;
- PAC: Pubblica Amministrazione Centrale;
- PDO: Piano dettagliato degli obiettivi;
- PEG: Piano Esecutivo di Gestione;
- Piano: il piano di completa informatizzazione delle istanze, dichiarazioni e richieste che possono essere inoltrate all'Ente in base a quanto previsto dal comma 3-bis dell'articolo 24 del D.L. 24/06/2014 n. 90, convertito, con modifiche, in L. 11/08/2014 n. 114;

- Posta Elettronica Certificata (PEC): il sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi;
- Procedimento Amministrativo: una sequenza di atti e attività posta in essere da una Pubblica amministrazione, finalizzata all'emanazione di un provvedimento amministrativo;
- PSN: Polo Strategico Nazionale;
- PTPCT: Piano triennale di prevenzione della corruzione e della trasparenza;
- SaaS (Software-as-a-Service): modello che racchiude applicativi e sistemi software, accessibili da un qualsiasi tipo di dispositivo (computer, smartphone, tablet, ecc.), attraverso il semplice utilizzo di un'interfaccia client. In questo modo, l'utilizzatore non deve preoccuparsi di gestire le risorse e l'infrastruttura, in quanto controllati dal provider che li fornisce (https://www.agid.gov.it/it/infrastrutture/cloud-pa/qualificazione-saas);
- Segnalazione: un atto giuridico con il quale un privato porta a conoscenza delle Pubbliche amministrazioni determinate situazioni che possono avviare o comunque avere rilevanza nell'ambito di un procedimento amministrativo;
- SGPA: Sistema di gestione dei procedimenti amministrativi (https://www.agid.gov.it/it/piattaforme/sistema-gestione-procedimenti-amministrativi);
- SMVP: Sistema di Misurazione e Valutazione delle Performances;
- SNA: Scuola Nazionale delle Amministrazioni;
- SPC: Sistema Pubblico di Connettività (https://www.agid.gov.it/it/infrastrutture/sistema-pubblico-connettivita);
- SPID: Sistema Pubblico di Identità Digitale dei cittadini e delle imprese, mediante il quale le pubbliche amministrazioni potranno consentire l'accesso in rete ai propri servizi (https://www.agid.gov.it/it/piattaforme/spid);
- TOIP: Text over IP.

Appendice II - Contesto normativo e strategico

App II.1 - Sezione 1 - Le prospettive di sviluppo dei servizi nel contesto digitale dell'Ente

Riferimenti normativi italiani:

- Legge 9 gennaio 2004, n. 4, recante "*Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici*";
- Decreto legislativo 7 marzo 2005, n. 82, recante "*Codice dell'amministrazione digitale*" (in breve CAD), artt. 7, 68, 69 e 71;
- Decreto Legislativo 10 agosto 2018, n. 106, recante "*Riforma dell'attuazione della direttiva (UE) 2016/2102 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici*";
- Decreto Legge 18 ottobre 2012, n. 179, recante "*Ulteriori misure urgenti per la crescita del Paese*", art. 9, comma 7;
- Linee Guida AGID per il design dei servizi digitali della Pubblica Amministrazione;
- Linee Guida AGID sull'accessibilità degli strumenti informatici;
- Linee Guida AGID sull'acquisizione e il riuso del software per la Pubblica Amministrazione;
- Circolare AGID n.2/2018, recante "*Criteri per la qualificazione dei Cloud Service Provider per la PA*";
- Circolare AGID n.3/2018, recante "*Criteri per la qualificazione di servizi SaaS per il Cloud della PA*".

Riferimenti normativi europei:

- Regolamento (UE) 2018/1724 del Parlamento Europeo e del Consiglio del 2 ottobre 2018 che istituisce uno sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e che modifica il regolamento (UE) n. 1024/2012;
- Direttiva UE 2016/2102 del Parlamento Europeo e del Consiglio del 26 ottobre 2016 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici.

App II.2 - Sezione 2 - Il trattamento dei dati

Riferimenti normativi italiani:

- Decreto legislativo 30 giugno 2003, n. 196, recante "*Codice in materia di protezione dei dati personali*";
- Decreto legislativo 7 marzo 2005, n. 82, recante "*Codice dell'amministrazione digitale*" (in breve CAD);
- Decreto legislativo 24 gennaio 2006, n. 36, recante "*Attuazione della direttiva UE 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico che ha abrogato la direttiva 2003/98/CE*";
- Decreto legislativo 27 gennaio 2010, n. 32, recante "*Attuazione della direttiva 2007/2/CE, che istituisce un'infrastruttura per l'informazione territoriale nella Comunità europea (INSPIRE)*";
- Decreto legislativo 14 marzo 2013, n. 33, recante "*Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*";
- Decreto legislativo 18 maggio 2015, n.102, recante "*Attuazione della direttiva 2013/37/UE che modifica la direttiva 2003/98/CE, relativa al riutilizzo di documenti nel settore pubblico*";
- Decreto della Presidenza del Consiglio dei Ministri 10 novembre 2011, recante "*Adozione del Sistema di riferimento geodetico nazionale*";
- Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico, rese dall'Agenzia per l'Italia Digitale;
- Linee guida per i cataloghi dati;
- Linee guida per l'implementazione della specifica GeoDCAT-AP;
- Manuale RNDT: Guide operative per la compilazione dei metadati RNDT, reso dall'Agenzia per l'Italia Digitale.

Riferimenti normativi europei:

- Regolamento (CE) 2008/1205 del 3 dicembre 2008 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda i metadati;
- Regolamento (UE) 2010/1089 del 23 novembre 2010 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda l'interoperabilità dei set di dati territoriali e dei servizi di dati territoriali;

- Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (in breve GDPR);
- Direttiva (UE) 2019/1024 del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico;
- Decisione (UE) 2019/1372 del 19 agosto 2019 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda il monitoraggio e la comunicazione;
- Comunicazione della Commissione 2014/C 240/01 del 24 luglio 2014, recante "*Orientamenti sulle licenze standard raccomandate, i dataset e la tariffazione del riutilizzo dei documenti*";
- Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni COM(2020) del 19 febbraio 2020 – Una strategia europea per i dati.

App II.3 - Sezione 3 - Le Piattaforme digitali

Fonti Generali:

- Decreto legislativo 7 marzo 2005, n. 82, recante "*Codice dell'amministrazione digitale*" (CAD), artt. 5, 50- ter, 62, 64, 64*bis*;
- Decreto legislativo 30 giugno 2003, n. 196, recante "*Codice in materia di protezione dei dati personali*".

Riferimenti normativi europei:

- Regolamento (UE) n. 910/2014 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (eIDAS);
- Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR).

NoiPA:

- Legge 27 dicembre 2006, n. 296, recante "*Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato*" (legge finanziaria 2007) art. 1 commi 446 e 447;
- Legge 23 dicembre 2009, n. 191, recante "*Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato*" (legge finanziaria 2010) art. 2, comma 197;
- Legge 19 giugno 2019, n. 56, recante "*Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo*";
- Decreto Legge 6 luglio 2011, n. 98, recante "*Disposizioni urgenti per la stabilizzazione finanziaria*", art. 11, comma 9;
- Decreto Ministeriale del Ministro dell'Economia e delle Finanze del 31 ottobre 2002, recante "*Modifiche delle norme sull'articolazione organizzativa del Dipartimento per le politiche di sviluppo e di coesione del Ministero dell'Economia e delle Finanze*";
- Decreto Ministeriale del Ministro dell'Economia e delle Finanze del 6 luglio 2012, recante "*Contenuti e modalità di attivazione dei servizi in materia stipendiale erogati dal Ministero dell'Economia e delle Finanze*".

App II.4 - Sezione 4 - Le Infrastrutture

Riferimenti normativi italiani:

- Legge 27 dicembre 2019, n. 160, recante "*Bilancio di previsione dello Stato per l'anno finanziario 2020 e bilancio pluriennale per il triennio 2020-2022*" art. 1 commi 407, 610 e 611;
- Decreto legislativo 7 marzo 2005, n.82, recante "*Codice dell'amministrazione digitale*";
- Decreto legislativo 18 maggio 2018, n. 65, recante "*Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*";
- Decreto legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221;
- Decreto legge 21 settembre 2019, n. 105, recante "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*".
- Decreto legge 17 marzo 2020, n. 18, recante "*Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19*", art. 75;

- Circolare AGID n. 1/2019, del 14 giugno 2019, recante "*Censimento del patrimonio ICT delle Pubbliche Amministrazioni e classificazione delle infrastrutture idonee all'uso da parte dei Poli Strategici Nazionali*";
- Strategia italiana per la banda ultralarga (http://presidenza.governo.it/GovernoInforma/Documenti/piano_banda_ultra_larga.pdf).

Riferimenti normativi europei:

- Programma europeo CEF Telecom (https://ec.europa.eu/inea/en/connecting-europe-facility);
- Strategia europea sui dati, Commissione Europea 19.2.2020 COM(2020) 66 final;
- European Commission Cloud Strategy, Cloud as an enabler for the European Commission Digital Strategy, 16 May 2019.

App II.5 - Sezione 5 – Sicurezza informatica

Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82, recante "*Codice dell'amministrazione digitale*" (in breve CAD), art. 51;
- Decreto Legislativo 18 maggio 2018, n. 65, recante "*Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*";
- Decreto Legge 21 settembre 2019, n. 105, recante "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*";
- Decreto del Presidente del Consiglio dei Ministri 8 agosto 2019, recante "*Disposizioni sull'organizzazione e il funzionamento del computer security incident response team: CSIRT italiano*";
- Piano Nazionale per la Protezione Cibernetica 2017.

Riferimenti normativi europei:

- 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.

App II.6 - Sezione 6 - Smart Working

Riferimenti normativi italiani:

- Legge 7 agosto 2015 n. 124, recante "*Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche*";
- Legge 22 maggio 2017 n. 81, recante "*Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato*";
- Legge 17 luglio 2020 n. 77, recante "*Conversione in legge, con modificazioni, del decreto legge 19 maggio 2020, n. 34, recante misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19*";
- Decreto Legge 30 aprile 2019 n. 34, recante "*Misure urgenti di crescita economica e per la risoluzione di specifiche situazioni di crisi*";
- Decreto Legge 17 marzo 2020 n. 18, recante "*Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19*";
- Legge 24 aprile 2020 n. 27, recante "*Conversione in legge, con modificazioni, del decreto legge 17 marzo 2020, n. 18, recante misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19. Proroga dei termini per l'adozione di decreti legislativi*".

App II.7 - Sezione 7 - Reingegnerizzazione e aggiornamento applicativi

Riferimenti normativi italiani:

- RD 1163/1911, che approva l'annesso Regolamento per gli archivi di Stato;

- DPR 1409/1963, recante "*Norme relative all'ordinamento ed al personale degli archivi di Stato*";
- DPR 854/1975, recante "*Attribuzioni del Ministero dell'interno in materia di documenti archivistici non ammessi alla libera consultabilità*";
- Legge 241/1990, recante "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*";
- DPR 445/2000, recante "*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*";
- DPR 37/2001, recante "*Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato*";
- D.lgs 196/2003 recante "*Codice in materia di protezione dei dati personali*";
- D.lgs 82/2005, recante "*Codice dell'amministrazione digitale*";
- D.lgs 33/2013, recante "*Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*";
- DPCM 22 febbraio 2013, recante "*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*";
- DPCM 21 marzo 2013, recante "*Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni*";
- DPCM 29 agosto 2014, n. 171, recante "*Regolamento di organizzazione del Ministero dei beni e delle attività culturali e del turismo, degli uffici della diretta collaborazione del Ministro e dell'Organismo indipendente di valutazione della performance, a norma dell'articolo 16, comma 4, del decreto-legge 24 aprile 2014, n. 66, convertito, con modificazioni, dalla legge 23 giugno 2014, n. 89*";
- Regolamento UE 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
- Circolare n. 65 del 10 aprile 2014, recante "*Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82*";
- Circolari nn. 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi, recanti "*Autorizzazione alla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 e conservati secondo le regole tecniche di cui al DPCM 13.12.2013"*;
- Regolamento UE 679/2016, 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;
- Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale, recante "*Misure minime di sicurezza ICT per le pubbliche amministrazioni*";
- Circolare n. 2 del 9 aprile 2018, recante i criteri per la qualificazione dei Cloud Service Provider per la PA;
- Circolare n. 3 del 9 aprile 2018, recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA.
-
- Linee Guida Agid in materia di gestione del documento informatico
- D.lgs. 82/05, recante "*Codice dell'amministrazione digitale*";
- D.lgs. 150/09, recante "*Attuazione della legge 4 marzo 2009, n. 15 in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni*".

Appendice III - Valutazione Comparativa nell'Acquisizione e Riuso di Software

Come previsto dal CAD, le pubbliche amministrazioni prima di procedere all'acquisto secondo le procedure del codice dei contratti devono effettuare una valutazione comparativa delle diverse soluzioni disponibili sulla base dei seguenti criteri:
a) costo complessivo del programma o soluzione quale costo di acquisto, di implementazione, di mantenimento e supporto;
b) livello di utilizzo di formati di dati e di interfacce di tipo aperto nonché di standard in grado di assicurare l'interoperabilità e la cooperazione applicativa tra i diversi sistemi informatici della pubblica amministrazione;
c) garanzie del fornitore in materia di livelli di sicurezza, conformità alla normativa in materia di protezione dei dati personali, livelli di servizio tenuto conto della tipologia di software acquisito.
Alla luce delle modalità indicate dall'AgID nelle linee guida di riferimento (https://www.agid.gov.it/it/design-servizi/riuso-open-source/linee-guida-acquisizione-riuso-software-pa), viene di seguito riportato uno schema per effettuare la valutazione per l'acquisto di un software in un'ipotesi in cui risulti impossibile accedere a soluzioni già disponibili all'interno della PA, o a software liberi o a codici sorgente aperti adeguati alle esigenze da soddisfare.
Il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri mette a disposizione due strumenti di ausilio per effettuare la valutazione comparativa (https://developers.italia.it/it/software/agid-agid-ccros-valcomp.html).

MACRO-FASE 1: INDIVIDUAZIONE DELLE ESIGENZE

1.1. ANALISI DEL FABBISOGNO

1.1.1. Studio del contesto attraverso la descrizione delle caratteristiche dell'amministrazione: finalità, struttura ed organizzazione.
1.1.2. Descrizione dei flussi operativi interessati dal software da acquisire, che la pubblica amministrazione mette in atto per dare seguito alle procedure amministrative.
1.1.3. Ipotesi di ottimizzazione dei flussi in relazione al software da acquisire.
1.1.4 Identificazione degli «strumenti» (definizione degli obiettivi) necessari alla realizzazione dei processi operativi individuati.
1.1.5. Enunciazione dei requisiti, dei bisogni a cui il software deve rispondere, differenziando tra requisiti indispensabili e non.

1.2. INDIVIDUAZIONE DEI VINCOLI

1.2.1. Disponibilità di bilancio.
1.2.2. Tempistiche.
1.2.3. Vincoli normativi.

MACRO-FASE 2: ANALISI DELLE SOLUZIONI A RIUSO E DELLE SOLUZIONI OPEN SOURCE

2.1. Individuazione delle soluzioni a riuso delle PPAA o delle soluzioni Open Source disponibili.
2.1.1. Ricerca di soluzioni riusabili per la PA.
2.1.2 Valutazione della soluzione a riuso.
2.1.3. Determinazione sulla scelta della soluzione a riuso e conclusione della valutazione.

MACRO-FASE 3: ANALISI DELLE ALTRE SOLUZIONI

Premessa: Caratteristiche del software.
Fase 3.1 Soluzioni proprietarie.
Fase 3.2 Realizzazione in house o ex novo.
Fase 3.3 Comparazione tra soluzioni proprietarie e realizzazione ex novo.

SZN Misure Minime di sicurezza ICT

Il presente documento redatto dal RTD della Stazione Zoologica Anton Dohrn, in allegato al Piano Triennale per l'Informatica 2022-2024 della Stazione Zoologica Anton Dohrn, è una implementazione del documento ufficiale AgID reperibile al seguente indirizzo:

https://www.agid.gov.it/sites/default/files/repository_files/documentazione/misure_minime_di_sicurezza_v.1.0.pdf

Acronimi utilizzati nelle Circolari ufficiali e nel resto del presente documento

Sigla	Significato	Note
ABSC	AgID Basic Security Control(s)	Controlli di sicurezza previsti dall'AgID
CSC	Critical Security Control(s)	Controlli di sicurezza critici, ritenuti fondamentali
CSSC	CIS - Critical Security Controls for Effective Cyber Defense	Controlli di sicurezza critici per una protezione funzionale dagli attacchi cibernetici

Livelli di sicurezza utilizzati nel presente documento

Nel documento, per ogni singola implementazione tecnica, è indicato il livello di sicurezza relativo. Le misure previste dal livello minimo devono essere messe in atto quanto prima, poiché ritenute necessarie dall'AgID.

Sigla	Significato	Note
M	Minimo	Livello sotto il quale nessuna amministrazione può scendere: i controlli indicati debbono riguardarsi come **obbligatori**
S	Standard	Base di riferimento per un livello di sicurezza completo. Rappresenta il primo step a cui tendere per la protezione della propria infrastruttura informatica
A	Alto	Obiettivo finale a cui tendere, al completamento del piano di sicurezza

Nel corso del documento sono state evidenziate con diversi colori le singole misure previste, in modo da fornire un veloce colpo d'occhio su quanto sia:

- strettamente necessario: rosso
- da programmare: azzurro
- obiettivo finale: verde

Tempi di implementazione

La tabella proposta dall'AgID è stata integrata con una colonna che permette all'Amministrazione di specificare i tempi di messa in opera di ogni misura di sicurezza.

Sigla	Descrizione
II	Implementazione **Immediata**. Da mettere in atto quanto prima per raggiungere il livello minimo richiesto
ID	Implementazione in itinere, **durante** la validità del piano di sicurezza informatica
IS	Implementazione a **scadenza**, da realizzarsi entro il termine di validità del piano di sicurezza informatica

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Tempi
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	L'inventario è gestito conservato ad opera del collega responsabile dei beni inventariabili dell'Ente. Viene utilizzata una repository all'interno del database "SZNINV" presente sul server AS400 ed in copia ridondante su un server dell'amministrazione centrale. Tramite interrogazione da terminale è possibile ottenere in tempo reale l'elenco dei dispositivi informatici collegati alla rete (IPSCAN). L'inventario è aggiornato mensilmente o comunque viene inserita una nuova voce non appena viene registrato l'ingresso del bene con consegna al posto della segreteria generale. Vengono registrati: PC, laptop, server, fotocopiatrici/fotocopiatrici di rete, smartphone aziendali, telefoni VOIP, switch ed apparati di rete, router. Per ogni dispositivo sono utilizzati dei campi univoci che corrispondono a:- numero di serie SZN assegnato all'apparato;- descrizione breve del tipo di dispositivo;- MAC Address; - collocazione e persona alla quale è assegnato; eventuale IP statico o dinamico ricorrente (DHCP in range di VPN dedicata). L'inventario permette la creazione di un report settimanale che esporta i dati contenenti l'inventario in un file con formato foglio di calcolo. Il documento riporta la data di ultimo aggiornamento. NON sono stati ancora implementati sistemi automatici di catalogazione. L'amministratore di rete della SZN fornisce elenco dei server, dei PC e dei dispositivi (stampanti, scanner, NAS, Access Point, switch) presenti nella rete	II
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	DA IMPLEMENTARE	IS
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	IN CORSO DI PERFEZIONAMENTO. Una unità di personale è stata dedicata all'implementazione di uno strumento software (script) in fase di sviluppo (analisi dei pacchetti in corso, previsto rilascio, fine 2021)	IS
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	L'amministratore di rete della SZN installa uno strumento hardware/software che periodicamente controlla i dispositivi presenti in rete	IS
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	L'amministratore di rete della SZN attiva i LOG del server DHCP, sepresente	IS
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	L'amministratore di rete della SZN verifica periodicamente i log e liconfronta con i propri elenchi di dispositivi	ID
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'amministratore di rete della SZN aggiorna la documentazione	II
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	L'amministratore di rete della SZN aggiorna la documentazione	IS
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	L'amministratore di rete della SZN aggiorna la documentazione	II
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	L'amministratore di rete della SZN aggiorna la documentazione	IS
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	L'amministratore di rete della SZN aggiorna la documentazione e verificaperiodicamente i log dei dispositivi che hanno utilizzato la rete	IS
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	L'amministratore di rete della SZN verifica che nelle reti WIFI sia presenteun sistema di autenticazione Captive Portal basato su account singoli e non su chiave WPA/WPA2 comune	IS
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	L'amministratore verifica l'esistenza (ove possibile) di certificati lato client.	IS

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Tempi
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	L'amministratore di rete della SZN aggiorna la documentazione	II
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	L'amministratore di rete della SZN aggiorna la documentazione	IS
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	L'amministratore di rete della SZN aggiorna la documentazione	IS
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	L'amministratore di rete della SZN utilizza strumenti hardware/software di checksum sui repository software	IS
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	L'amministratore di rete della SZN verifica le applicazioni installate	II
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	L'amministratore di rete della SZN aggiorna la documentazione	IS
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	L'amministratore di rete della SZN predispone su un server apposito degli strumenti per l'analisi delle configurazioni software dellarete	IS
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	L'amministratore di rete della SZN verifica se esistono applicazioni di questo tipo e predispone i dovuti accorgimenti di protezione	IS

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Tempi
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	L'amministratore di rete della SZN impartisce istruzioni su come gestire i singoli sistemi operativi e fornisce un manualecontenente le istruzioni sull'utilizzo corretto della rete edelle risorse di rete	II
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	L'amministratore di rete della SZN, all'atto dell'installazione di una nuova postazione, verifica che siano rispettate le proceduredi hardening: - eliminazione account non necessari - disabilitazione servizi non necessari - chiusura porte di rete non necessarie	ID
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	L'amministratore di rete della SZN mantiene un archivio aggiornatodelle immagini dei sistemi installati	IS
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	L'amministratore di rete della SZN redige un documento in cui si definisce la configurazione standard delle workstation dellarete	II
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	L'amministratore di rete della SZN definisce le procedure di ripristino	II
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	L'amministratore di rete della SZN definisce le procedure di ripristino	IS
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	L'amministratore di rete della SZN mantiene un archivio aggiornatodelle immagini dei sistemi installati	II
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	L'amministratore di rete della SZN mantiene un archivio aggiornatodelle immagini dei sistemi installati	IS

3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	L'amministratore di rete della SZN verifica che su server e workstation siano utilizzati solo strumenti di amministrazione remota cherispettino i protocolli di connessione protetta	II
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	L'amministratore di rete della SZN utilizza strumenti di checksum sui repository software	IS
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	L'amministratore di rete della SZN utilizza strumenti di checksum sui repository software	IS
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	L'amministratore di rete della SZN utilizza strumenti di checksum sui repository software	IS
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	L'amministratore di rete della SZN utilizza strumenti di checksum sui repository software	IS
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	L'amministratore di rete della SZN utilizza strumenti di checksum sui repository software	IS
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	L'amministratore di rete della SZN utilizza strumenti di checksum sui repository software	IS

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Tempi
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	L'amministratore di rete della SZN verifica che siano impostateoperazioni pianificate di verifica delle vulnerabilità (Antivirus, antimalware, etc)	II
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	L'amministratore di rete della SZN verifica che siano impostateoperazioni pianificate di verifica delle vulnerabilità (Antivirus, antimalware, etc)	ID
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	L'amministratore di rete della SZN predispone un sistemahardware/software SCAP di monitoraggio	IS
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	L'amministratore di rete della SZN predispone un sistemahardware/software SCAP di monitoraggio	ID
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	L'amministratore di rete della SZN predispone un sistema hardware/software SCAP di monitoraggio	ID
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	L'amministratore di rete della SZN predispone un sistemahardware/software SCAP di monitoraggio	ID
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	L'amministratore di rete della SZN predispone un sistema hardware/software SCAP di monitoraggio	ID
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	L'amministratore di rete della SZN predispone un sistemahardware/software SCAP di monitoraggio	ID

4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	L'amministratore di rete della SZN verifica che siano attivi gli aggiornamenti automatici degli strumenti di scansione	II
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	L'amministratore di rete della SZN certifica di essere abbonato a unservizio online di informazioni sulla cybersicurezza	ID
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	L'amministratore di rete della SZN verifica che siano attivi gliaggiornamenti automatici dei sistemi	II
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	L'amministratore di rete della SZN verifica che siano attivi gli aggiornamenti automatici dei sistemi e provvede ad aggiornare i sistemi non collegati direttamente alla rete	II
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	L'amministratore di rete della SZN verifica i i log delle attività	ID
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	L'amministratore di rete della SZN verifica che siano attivi gliaggiornamenti automatici dei sistemi	II
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	L'amministratore di rete della SZN verifica che siano attivi gli aggiornamenti automatici dei sistemi e decide i livelli di rischio in base ai risultati emersi	ID
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	L'amministratore di rete della SZN stila un elenco delle modalità digestione dei rischi	II
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	L'amministratore di rete della SZN stila un elenco delle modalità digestione dei rischi	II

4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	L'amministratore di rete della SZN stila un elenco delle modalità digestione dei rischi	ID
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	L'amministratore di rete della SZN certifica di essere in possesso diambienti di test su cui valuta l'impatto di prodotti non standard sugli apparati della rete	IS

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Tempi
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	L'amministratore di rete della SZN verifica i privilegi degli account utente.	II
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	L'amministratore di rete della SZN verifica i privilegi degli accountutente.	II
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	L'amministratore di rete della SZN verifica i privilegi degli accountutente. Vedi punto 5.1.1M	ID
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	L'amministratore di rete della SZN installa sui server un sistema di controllo dei log degli accessi.	ID
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	L'amministratore di rete della SZN redige la documentazione della rete.	II

5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	L'amministratore di rete della SZN redige la documentazione della retee la mantiene aggiornata tramite strumenti software	IS
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	L'amministratore di rete della SZN verifica i privilegi degli accountutente	II
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	L'amministratore di rete della SZN installa sui server un sistema di controllo dei log degli accessi.	ID
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	L'amministratore di rete della SZN installa sui server un sistema dicontrollo dei log degli accessi	IS
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	L'amministratore di rete della SZN installa sui server un sistema dicontrollo dei log degli accessi	IS
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	L'amministratore di rete della SZN installa sui server un sistema dicontrollo dei log degli accessi	IS
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	L'amministratore di rete della SZN verifica le modalità degli accessiamministrativi	IS

5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	L'amministratore di rete della SZN verifica che la complessità delle password delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del Dlgs 196/2003. Verifica o meno del doppio accesso 1. Inserimento data generale di scadenza password 2. Numero di gg massimi per la validità del codice di accesso 3. Numero massimo di gg da ultimo accesso per consentire ancora lo stesso 4. Lunghezza minima del codice di accesso (in questo caso 14) 5. Numero minimo dei caratteri minuscoli 6. Numero minimo dei caratteri maiuscoli 7. Numero minimo dei caratteri numerici 8. Numero minimo dei caratteri speciali	II
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	L'amministratore di rete della SZN verifica che la complessità dellepassword delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del Dlgs 196/2003.	ID
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	L'amministratore di rete della SZN verifica che la complessità dellepassword delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del Dlgs 196/2003. Vedi parametri indicati nel punto 5.7.1.M	II
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	L'amministratore di rete della SZN verifica che la complessità delle password delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del Dlgs 196/2003.	II

5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	L'amministratore di rete della SZN verifica che la complessità dellepassword delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del DIgs 196/2003	ID
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	L'amministratore di rete della SZN verifica che la complessità dellepassword delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del DIgs 196/2003	ID
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	L'amministratore di rete della SZN verifica le modalità degli accessi amministrativi	IS
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	L'amministratore di rete della SZN verifica le modalità degli accessiamministrativi	IS
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	L'amministratore di rete della SZN verifica le modalità degli accessi amministrativi	II
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	L'amministratore di rete della SZN verifica le modalità degli accessi amministrativi	II
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	L'amministratore di rete della SZN verifica le modalità degli accessiamministrativi	II

5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	L'amministratore di rete della SZN verifica le modalità degli accessiamministrativi	ID
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	L'amministratore di rete della SZN verifica le modalità degli accessi amministrativi.	II
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	L'amministratore di rete della SZN verifica le modalità degli accessiamministrativi	II

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Tempi
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	L'amministratore di rete della SZN verifica la presenza di sistemiantivirus e firewall software locali	II
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	L'amministratore di rete della SZN verifica la presenza di sistemiantivirus e firewall software locali	II
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	L'amministratore di rete della SZN installa e configura un sistema digestione centralizzata dei log	IS
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	L'amministratore di rete della SZN verifica che gli antivirus localisiano gestibili attraverso un sistema centralizzato	ID
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	L'amministratore di rete della SZN verifica che gli antivirus localisiano gestibili attraverso un sistema centralizzato	ID
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	L'amministratore di rete della SZN verifica che gli antivirus localisiano gestibili attraverso un sistema centralizzato	ID
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	L'amministratore di rete della SZN verifica l'utilizzo di dispositiviesterni	II
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	L'amministratore di rete della SZN verifica l'utilizzo di dispositiviesterni	IS
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	L'amministratore di rete della SZN installa e predispone adeguatistrumenti hardware/software IDS, DEP, ASLR	IS
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	L'amministratore di rete della SZN installa e predispone adeguatistrumenti hardware/software IDS, DEP, ASLR	ID
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	L'amministratore di rete della SZN installa e predispone adeguatistrumenti hardware/software IDS, DEP, ASLR	IS
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	L'amministratore di rete della SZN installa e predispone adeguatistrumenti hardware/software IDS, DEP, ASLR	IS
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	L'amministratore di rete della SZN installa e predispone adeguatistrumenti hardware/software IDS, DEP, ASLR	IS
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	L'amministratore di rete della SZN predispone adeguate GroupPolicies sui server di dominio	II
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	L'amministratore di rete della SZN predispone adeguate GroupPolicies sui server di dominio	II
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	L'amministratore di rete della SZN predispone adeguate GroupPolicies sui server di dominio	II
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	L'amministratore di rete della SZN predispone adeguate GroupPolicies sui server di dominio	II
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	L'amministratore di rete della SZN predispone adeguate GroupPolicies sui server di dominio	II
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	L'amministratore di rete della SZN predispone adeguate GroupPolicies sui server di dominio	II
8	9	2	M	Filtrare il contenuto del traffico web.	L'amministratore di rete della SZN installa e predispone adeguatistrumenti hardware/software IDS, DEP, ASLR	II
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	L'amministratore di rete della SZN installa e predispone adeguatistrumenti hardware/software IDS, DEP, ASLR	II
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	L'amministratore di rete della SZN installa e predispone adeguatistrumenti hardware/software IDS, DEP, ASLR	ID
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	L'amministratore di rete della SZN installa e predispone adeguatistrumenti hardware/software IDS, DEP, ASLR	IS

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Tempi
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	L'amministratore di rete della SZN predispone e mette in atto un piano di backup e disaster recovery adeguato. - Backup del log delle transazioni ogni 30 minuti - Backup completo ogni giorno alle 2.00 circa - Retention dei backup 8/10 gg	II
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	L'amministratore di rete della SZN predispone e mette in atto un piano di backup e disaster recovery adeguato.	IS
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	L'amministratore di rete della SZN predispone e mette in atto un piano di backup e disaster recovery adeguato.	IS
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	L'amministratore di rete della SZN predispone e mette in atto un piano di backup e disaster recovery adeguato.	ID
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	L'amministratore di rete della SZN predispone e mette in atto un piano di backup e disaster recovery adeguato.	II
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	L'amministratore di rete della SZN predispone e mette in atto un piano di backup e disaster recovery adeguato.	II

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Tempi
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	L'amministratore di rete della SZN verifica che i dati siano trattati inconformità con quanto richiesto dall'Allegato B del Dlgs 196/2003	II
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	L'amministratore di rete della SZN verifica che i dati siano trattati inconformità con quanto richiesto dall'Allegato B del Dlgs 196/2003	IS
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale perdita di informazioni.	L'amministratore di rete della SZN installa e predispone adeguatistrumenti hardware/software IDS, DEP, ASLR	IS
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	L'amministratore di rete della SZN installa e predispone adeguatistrumenti hardware/software IDS, DEP, ASLR	IS
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	L'amministratore di rete della SZN verifica che i dati siano trattati inconformità con quanto richiesto dall'Allegato B del Dlgs 196/2003	IS
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	L'amministratore di rete della SZN verifica la presenza di siffatti dispositivi e li include nella lista dei dispositivi autorizzatisulla rete	IS
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	L'amministratore di rete della SZN installa e predispone adeguatistrumenti hardware/software IDS, DEP, ASLR	IS
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	L'amministratore di rete della SZN installa e predispone adeguatistrumenti hardware/software IDS, DEP, ASLR	IS
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	L'amministratore di rete della SZN installa e predispone adeguatistrumenti hardware/software IDS, DEP, ASLR	IS
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	L'amministratore di rete della SZN verifica che il firewall in uso sullarete permetta le gestione di blacklist e whitelist	II
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	L'amministratore di rete della SZN predispone che i sistemi di copiatura mantengano le regole di controllo sui dati e verifica che i software in uso consentano l'applicazione ditali regole	IS