

RELAZIONE SULLA PERFORMANCE

- ANNO 2023 -

1. Introduzione illustrativa

La presente relazione chiude il ciclo della performance dell'anno 2023 attivato con l'elaborazione e successiva approvazione degli atti di programmazione dell'esercizio di riferimento. Il Piano della Performance 2023 del Comune di Pederobba, ai sensi di quanto previsto dal D.P.R. n. 81/2022, è assorbito nella sezione "Performance" del Piano Integrato di Attività ed Organizzazione (PIAO), la cui sezione è stata approvata con deliberazione di Giunta comunale n. 21 del 22.03.2023, successivamente aggiornata e rimodulata con deliberazione di Giunta comunale n. 60 del 07.08.2023 e n. 82 del 29.11.2023 all'esito del monitoraggio in corso d'anno.

Con deliberazione di Giunta comunale n. 2 del 18.01.2023 è stato approvato il Piano Esecutivo di Gestione per la parte finanziaria.

Il Piano della Performance definisce gli obiettivi dell'Ente e il Piano Esecutivo di Gestione mette a disposizione le risorse in attuazione dei principali strumenti di programmazione, costituiti dal Documento Unico di Programmazione approvato con deliberazione di Consiglio comunale n. 50 del 30.12.2022 e dal Bilancio di Previsione approvato con deliberazione di Consiglio comunale n. 51 del 30.12.2022.

In via straordinaria, data la specifica natura degli Obiettivi, questi stessi sono stati definiti come "aziendali" perché hanno coinvolto – nello stesso tempo e con la medesima intensità – tutti i responsabili con i loro collaboratori sulla base di tempi previsti, di risultati attesi e di relativi indicatori per consentire di misurarne il grado di realizzazione a fine anno.

Gli obiettivi del Piano della Performance sono stati redatti secondo la metodologia vigente che prevede, per ciascun obiettivo, la redazione di una scheda obiettivo di Peg contenente obiettivi strategici e rilevanti per l'ente.

Gli obiettivi sono oggetto di "pesatura" secondo i criteri previsti nella metodologia stessa.

Il livello di raggiungimento degli obiettivi è sottoposto a valutazione secondo le modalità previste dal Sistema di misurazione e valutazione della performance dell'Ente. Con lo stesso sistema sono valutate le performance delle posizioni organizzative-alte professionalità.

La Relazione ha la finalità di illustrare ai cittadini e a tutti gli altri stakeholders, interni ed esterni, i risultati di performance ottenuti nel corso del 2023. Si conclude in questo modo il ciclo di gestione annuale della performance.

2. Il sistema di misurazione/valutazione della performance (art. 7 D.Lgs. n. 150/09)

Il Regolamento sull'ordinamento degli uffici e dei servizi prevede che tale sistema da approvare, previo parere vincolante del Nucleo di Valutazione, con atto della

Giunta Comunale, disciplini le varie attività preordinate alla gestione del ciclo della performance.

Tale sistema si integra con gli atti di programmazione riportati nell'Introduzione e con l'analisi del contesto e **delle risorse** che si ricava dal PIAO con riguardo alla struttura organizzativa del Comune e alla ripartizione delle macro-funzioni tra i servizi (funzionigramma).

3. Misurazione e valutazione degli obiettivi della sottosezione Performance del PIAO anno 2023

Il vigente sistema di misurazione e di valutazione della performance dell'Ente prevede che le Posizioni Organizzative-Alte Professionalità, coordinate dal Segretario, per ciascun Servizio effettuino la necessaria attività di rendicontazione in ordine al grado di raggiungimento degli obiettivi mediante la compilazione delle apposite schede previste dalla metodologia approvata.

Per effetto dell'attività di monitoraggio svolta nel corso dell'anno 2023 partendo dal PIAO, sottosezione Performance, i Responsabili hanno presentato la propria rendicontazione in ordine al grado di raggiungimento degli obiettivi assegnati ai rispettivi Servizi. Poiché si è trattato di Obiettivi "aziendali" perché miravano a sviluppare tematiche che dovevano coinvolgere, in maniera sinergica, l'intero Ente, le relazioni che ne sono seguite sono state tutte trasfuse in una sola relazione che qui di seguito si riporta:

Obiettivo 1 (trasversale a tutti i Servizi): Attuazione Piano triennale per la prevenzione della corruzione e della trasparenza vigente.

Descrizione: L'obiettivo consisteva nell'attuare le misure in merito alla verifica di assenza di cause di inconfiribilità ed incompatibilità nei conferimenti di incarichi ai sensi del D.Lgs. 39/2013 . Inoltre era finalizzato all'implementazione delle misure per il rispetto del D.lgs. 33/2013 e delle linee guida ANAC.

Gli Uffici hanno inteso che attraverso questo obiettivo l'Ente mirava ad attuare, a livello pratico, una misura di prevenzione del rischio di corruzione. Il momento formativo allargato a tutto il personale ha concorso, come era di fatto richiesto anche tra gli indicatori di verifica del raggiungimento dell'obiettivo, a rendere concreto lo sforzo operato. Il personale ha compreso che dopo aver identificato le aree e i processi maggiormente a rischio corruttivo è sempre necessario identificare anche le misure necessarie a "neutralizzare" o ridurre la possibilità che l'evento accada. In tal senso, la "Trasparenza", imposta per legge, non deve essere solo un mero adempimento. La Trasparenza e il rispetto delle prescrizioni ad essa collegate, sono una misura di prevenzione perché rendono maggiormente controllabili (anche dall'esterno), i processi dell'Amministrazione. Le misure di trasparenza aumentano il livello di accountability nella organizzazione e riducono gli spazi di discrezionalità che rendono possibile l'uso distorto dei processi pubblici. L'efficacia delle misure di trasparenza può essere aumentata – come prevedeva espressamente l'obiettivo – anche attraverso la verifica di precedenti condanne per reati contro la pubblica amministrazione. Non è possibile prevedere se e quando un dipendente

dell'amministrazione commetterà un illecito. Ma, certamente, un soggetto che è già stato condannato in precedenza per reati contro la pubblica amministrazione è più a rischio rispetto ad un soggetto che non ha ancora commesso reati. Per questa ragione, in attuazione ai nuovi obblighi di legge, l'Ente deve rivedere le proprie procedure e i criteri di formazione delle commissioni, di assegnazione del personale agli uffici e di conferimento degli incarichi per garantire che le persone condannate per reati contro la pubblica amministrazione (anche con sentenze non passate in giudicato): - non possano fare parte, anche con compiti di segreteria, di commissioni per l'accesso o la selezione a pubblici impieghi; - non siano assegnati agli uffici preposti alla gestione delle risorse finanziarie, all'acquisizione di beni, servizi e forniture, nonché alla concessione o all'erogazione di sovvenzioni, contributi, sussidi, ausili finanziari o attribuzioni di vantaggi economici a soggetti pubblici e privati; - non partecipino alle commissioni per la scelta del contraente per l'affidamento di lavori, forniture e servizi, per la concessione o l'erogazione di sovvenzioni, contributi, sussidi, ausili finanziari, nonché per l'attribuzione di vantaggi economici di qualunque genere; - non svolgano funzioni direttive all'interno dell'ente.

Tutte queste verifiche, inserite tra gli indicatori di risultato, sono state attuate.

Ne è derivato un opportuno approfondimento sul tema dell'"Obbligo di astensione in caso di conflitto di interessi". L'art. 1, comma 41, della L. 190/2012 ha introdotto l'art. 6 bis ("conflitto di interessi") nella L. 241/1990. La disposizione stabilisce che "Il responsabile del procedimento e i titolari degli uffici competenti ad adottare i pareri, le valutazioni tecniche, gli atti endoprocedimentali e il provvedimento finale devono astenersi in caso di conflitto di interessi, segnalando ogni situazione di conflitto, anche potenziale". La segnalazione del conflitto deve essere indirizzata dal dipendente al proprio responsabile, che, dopo aver valutato se la situazione realizza un conflitto di interesse idoneo a ledere l'imparzialità dell'agire amministrativo, deve rispondere per iscritto al dipendente medesimo, sollevandolo dall'incarico oppure motivando espressamente le ragioni che consentono comunque l'espletamento dell'attività. Allo stesso modo sono state approfondite anche le ipotesi di "inconferibilità" ed "incompatibilità". Il D.Lgs. 39/2013 (Disposizioni in materia di inconferibilità e incompatibilità di incarichi presso le pubbliche amministrazioni e presso gli enti privati in controllo pubblico) ha disciplinato: - le ipotesi di inconferibilità di incarichi dirigenziali a soggetti provenienti da enti di diritto privato regolati o finanziati dalle pubbliche amministrazioni, nonché a soggetti che sono stati componenti di organi di indirizzo politico; - le situazioni di incompatibilità specifiche per i titolari di incarichi dirigenziali e assimilati; - le ipotesi di inconferibilità di incarichi dirigenziali o assimilati per i soggetti che siano stati destinatari di sentenze di condanna per delitti contro la pubblica amministrazione. Le situazioni di inconferibilità od incompatibilità sono contestate dal Responsabile della Prevenzione. Invece, le situazioni di incompatibilità od inconferibilità riguardanti il Segretario Comunale che sia stato individuato come Responsabile della Prevenzione sono contestate dal Sindaco. L'inconferibilità non è sanabile. Invece, l'incompatibilità può essere superata con la rinuncia agli incarichi che la legge considera incompatibili, oppure con il collocamento fuori ruolo e in aspettativa. La dichiarazione dell'insussistenza di incompatibilità va resa

annualmente e, al sorgere della causa di incompatibilità, la stessa va immediatamente comunicata.

Tutto questo lavoro di approfondimento si è retto sull'attività di "Formazione generale" portata avanti dai Responsabili e rivolta a tutti i dipendenti e che ha avuto come obiettivo l'aggiornamento delle competenze, ma anche i temi dell'etica e della legalità.

Nell'ottica della prevenzione della corruzione, gli interventi di formazione devono sempre favorire la consapevolezza e la responsabilità nello svolgimento di una funzione pubblica e nell'uso del potere pubblico. Nel corso del 2023 è stata somministrata a tutto il personale in servizio e non solo ai dipendenti interessati dallo svolgimento di mansioni a carattere istruttorio, comportanti discrezionalità tecnica o amministrativa, una sessione di formazione generale e specifica sui temi sopra precisati.

Alla luce di quanto sopra, si può attestare che l'obiettivo è stato completamente raggiunto. Percentuale di raggiungimento: 100%.

Obiettivo 2 (trasversale a tutti i Servizi): Mappatura servizi e prestazioni afferenti alle diverse Aree e revisione relativa modulistica tramite avvio dello Sportello Digitale Telematico finanziato dai fondi PNRR

Descrizione: Avendo il suo incipit nel censimento dei servizi e delle prestazioni amministrative che fanno capo ad ogni Area, l'obiettivo si proponeva di implementare l'app IO e di trasformare il sito web istituzionale in una piattaforma digitale che garantisse piena accessibilità e che consentisse di gestire le fasi di alcuni procedimenti amministrativi in modalità telematica, assicurando la verifica dell'identità digitale tramite il sistema SPID/CIE e l'introito di eventuali somme dovute all'Ente grazie al sistema PAGOPA.

L'obiettivo, assegnato in maniera trasversale all'intero Ente, ha riguardato, di fatto, la transizione digitale perché mediante l'impiego delle risorse previste dal Piano Nazionale di Ripresa e Resilienza il Comune si proponeva di estendere l'utilizzo delle piattaforme nazionali di identità digitale, di potenziare i servizi mediante migrazione al cloud, migliorare l'accessibilità del sito internet e dei servizi digitali, nonché di attivare i servizi digitali dell'Ente sull'App IO.

A livello pratico gli Uffici sono stati chiamati ad una serie composita di azioni ed adempimenti che sono consistiti nella implementazione della modulistica sulla base di un'attenta ricognizione dei procedimenti effettuati dall'Ente, con l'individuazione delle fasi endoprocedimentali.

Per far questo, così come previsto negli Indicatori di risultato, ci si è attivati lavorando sulla formazione del personale dipendente prima dell'avvio di un qualsiasi servizio digitale al fine di garantire coerenza tra le tipologie di procedimenti dell'Ente e i *template* standard della modulistica presente sulla piattaforma caricata nel sito istituzionale. Tra le attività seguite vengono qui elencate quelle più agilmente riassumibili:

1. Nell'ambito della misura 1.4.4 "Estensione dell'utilizzo delle piattaforme nazionali di identità digitale", con specifico riferimento al progetto di

"integrazione CIE" è stato garantito il rispetto dei tempi previsti dall'avviso per la contrattualizzazione.

2. Nell'ambito dell'investimento 1.2 "Abilitazione al cloud per le P.A. locali" è stato garantito il rispetto dei tempi previsti dall'avviso per la contrattualizzazione.

3. Nell'ambito del contratto, previsione del passaggio al cloud del n° di servizi individuati nella domanda di partecipazione all'avviso è stato garantito il rispetto dei tempi previsti dall'avviso per la contrattualizzazione.

4. Nell'ambito della misura 1.4.1 "Esperienza del cittadino nei servizi pubblici" è stato garantito il rispetto dei tempi previsti dall'avviso per la contrattualizzazione.

5. Nell'ambito del contratto, previsione di obiettivi di miglioramento e di conformità del sito comunale, obiettivi di miglioramento di servizi digitali per il cittadino individuati nella domanda di partecipazione all'avviso è stato garantito il rispetto dei tempi previsti dall'avviso per la contrattualizzazione.

6. Nell'ambito della misura 1.4.3 "Adozione App IO" è stato garantito il rispetto dei tempi previsti dall'avviso per la contrattualizzazione.

Quanto, poi, al servizio "pagoPA", al fine di migliorare l'erogazione dei servizi per i quali è stato disposto il pagamento tramite pagoPA, è stata introdotta una "Tassonomia dei servizi erogati" che ha consentito di identificare uniformemente i servizi di incasso e le rispettive posizioni debitorie che transitano tramite la Piattaforma pagoPA. Gli Uffici hanno lavorato in accordo con il Partner Tecnologico dell'Ente per poter creare correttamente le diverse Posizioni Debitorie definite in base al tipo di entrata richiesta. Nello stesso tempo è stato portato avanti – sempre con il Partner - una capillare rivisitazione della modulistica e dell'iter di ogni procedimento in modo da affinarne i passaggi prima di renderli accessibili attraverso la modalità elettronica assicurando che la fruizione degli stessi avvenisse attraverso l'identità digitale di SPID/CIE.

Partendo da queste singole azioni, i responsabili hanno definito singoli report di performance che traducono la valutazione del grado di raggiungimento dell'obiettivo stesso.

Alla luce di quanto sopra, si può attestare che l'obiettivo è stato completamente raggiunto. Percentuale di raggiungimento: 100%.

Obiettivo 3: Test e formazione sulle competenze digitali finalizzati alla sicurezza informatica – Cybersecurity.

Descrizione: In relazione alle molteplici attività previste per la predisposizione del Piano Triennale per l'Informatica con la preparazione dei relativi target in merito a: servizi, dati, piattaforme, infrastrutture, interoperabilità, sicurezza informatica, leve per l'innovazione, governo della transizione digitale era necessario sottoporre ai dipendenti un test dell'AGID (Agenzia per l'Italia Digitale) che misurasse le competenze digitali in diversi ambiti (dati, comunicazione, sicurezza, servizi on-line, trasformazione digitale). Gli

esiti del test dovevano essere raccolti e filtrati dall'incaricato con funzioni di supporto tecnico all'RTD. La finalità era quella di accertare il grado di competenza in tema di sicurezza informatica considerato che i sistemi della Pubblica Amministrazione in questo momento hanno un buon livello di sicurezza informatica, ma che la falla più grossa a livello nazionale sono i comportamenti sbagliati del personale.

Dal punto di vista operativo era necessaria la visione di almeno 1 filmato disponibile gratuitamente nel portale XDESK per una formazione di base sulla sicurezza. I filmati disponibili avrebbero dovuto affrontare queste tematiche: (1°) le principali tipologie di attacchi informatici, (2°) cosa fare se si subisce un attacco, (3°) come preservare le prove digitali.

Una volta completata la formazione, andava effettuato il test in modo obbligatorio, con invio dell'esito all'indirizzo di posta elettronica del Segretario Comunale al fine di definire un piano specifico di formazione per ogni dipendente.

Le dinamiche organizzative e l'attento utilizzo delle economie di spesa ricavate dall'impiego dei fondi del PNRR Digitale hanno permesso di attuare una politica aziendale in tema di sicurezza informatica decisamente più vantaggiosa ed efficace di quella che era stata inizialmente pianificata e sulla base della quale era stato definito l'obiettivo di risultato assegnato in maniera trasversale a tutti i Servizi.

Invece di chiedere a ciascun dipendente di sottoporsi ad un corso specifico sul tema per certificare, attraverso un test il suo livello di competenze da porre come base per studiare una campagna di formazione adeguata, è stato organizzato un sistema di corsi durante i quali gli stessi docenti hanno potuto saggiare le competenze individuali e definire le misure formative più adeguate.

A questo step, che era di fatto previsto, quanto all'esito finale, tra i fattori di valutazione dell'obiettivo di PEG, si è aggiunto un lavoro massivo di adeguamento dell'architettura informatica dell'Ente che è stato portato avanti implementando una serie di azioni tutte volte a rafforzare la sicurezza dell'Ente.

Vengono riportate, qui di seguito, le RIFLESSIONI che hanno condotto alla parziale modifica dell'obiettivo che, nel suo complesso, all'esito delle operazioni intraprese, si può considerare pienamente raggiunto (100%).

RIFLESSIONI:

Il tema della sicurezza informatica è diventato un tema sempre più importante. Con il continuo evolvere di internet, la criminalità informatica ha costruito una rete finalizzata allo scambio di informazioni e alla commercializzazione di prodotti funzionali al compimento di attacchi cibernetici. Per questo le difese messe a punto dalla sicurezza informatica devono essere solide, stratificate e sempre aggiornate e la protezione dei sistemi informatici richiede l'adozione di diverse misure; dalle soluzioni tecnologiche alla formazione degli utenti fino all'impostazione e all'implementazione di politiche organizzative efficaci. Per evitare o ridurre i rischi informatici che derivano da attacchi cibernetici l'Ente ha lavorato a delle soluzioni ponendo attenzione a 3 concetti:

MISURE MINIME ICT: le misure minime di sicurezza pur tenendo nella massima considerazione le difese tradizionali, pongono l'accento sull'assicurare che le attività degli utenti vengano svolte in un contesto tecnologico sicuro. Le misure minime di sicurezza, quindi, devono essere implementate, attuate e costantemente monitorate per garantire una continua ed efficace prevenzione di attacchi cibernetici.

MISURE MINIME ORGANIZZATIVE: la condivisione di regole e di prassi con il personale dell'organizzazione contribuisce ad accrescere la consapevolezza del rischio cyber e incentiva l'adozione di buone pratiche comportamentali in ambito ICT. Dunque, azioni di formazione e sensibilizzazione stanno alla base della corretta adozione di modelli organizzativi.

FORMAZIONE: la formazione è una leva strategica sia per consentire lo sviluppo professionale del dipendente sia per comprendere i nuovi modelli organizzativi che vengono distribuiti e spiegati con formazione specifica a tutto il personale dell'organizzazione.

A livello concreto sono poi state attivate tutta una serie di soluzioni per proteggere l'Ente da attacchi cibernetici (CDS - CYBER DEFENSE SOLUTIONS).

Tra queste è stato operato un processo di **AUDIT & RISK ASSESSMENT** che ha permesso l'individuazione delle risorse presenti all'interno della tecnologia dell'Ente e nella sua organizzazione per una prima valutazione dello stato di ognuna di esse con lo scopo di essere compliance anche ai requisiti previsti nelle misure minime emanate dall'AgID. Questo processo mirava ad adeguare, tramite attività sistemiche, l'infrastruttura dell'Ente fornendo degli strumenti atti a rilevare i diversi assets, i prodotti software installati con le eventuali criticità e vulnerabilità e ha fornito, a valle, una mappa dello stato di attuazione delle misure minime informando tempestivamente sullo stato di salute dei sistemi.

E' stata, poi, progettata una **CAMPAGNA PHISHING**. Il phishing è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima fingendosi un Ente affidabile in una comunicazione digitale. Il malintenzionato effettua un invio massivo di messaggi che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi; tali messaggi fraudolenti richiedono di fornire informazioni riservate come, ad esempio, il numero della carta di credito o la password per accedere ad un determinato servizio.

E' stata, poi, progettata un **PENETRATION TEST** che costituisce una metodologia utilizzata per valutare la sicurezza delle infrastrutture di un Ente. Questo test consiste nell'utilizzo di tecniche simili a quelle utilizzate da eventuali attaccanti al fine di individuare vulnerabilità presenti nelle risorse digitali dell'azienda e viene condotto da un team di esperti in sicurezza informatica che lavorano in modo indipendente e utilizzano strumenti e tecniche specifiche per testare la resistenza delle infrastrutture aziendali agli attacchi informatici.

A questi strumenti di sicurezza verrà affiancata anche una vera e propria piattaforma che li collegherà e li renderà maggiormente performanti. La Piattaforma SIEM (Security Information and Event Management) messa a

disposizione delle infrastrutture critiche in ambito cloud e on-premise sarà in grado di rilevare, analizzare e rispondere alle minacce di sicurezza prima che compromettano i sistemi informatici operando attraverso la raccolta delle informazioni da più fonti come firewall, server, dispositivi di rete e sistemi di rilevamento delle intrusioni.

Alla luce di quanto sopra, si può attestare che l'obiettivo è stato completamente raggiunto. Percentuale di raggiungimento: 100%.

4. Il processo di misurazione e valutazione

Tenendo conto dei risultati relativi al grado di “*Raggiungimento degli obiettivi*” (che si articolano in obiettivi di *performance organizzativa* ed in obiettivi di *performance individuale*), e considerando gli altri elementi di valutazione presi in considerazione dal sistema di valutazione attinenti al “*Comportamento*” (competenze dimostrate, contributo alla performance generale, comportamenti professionali ed organizzativi, per i responsabili di ufficio motivazione e coordinamento collaboratori), ciascun Responsabile ha, poi, provveduto alla valutazione del personale ad esso assegnato.

I macro valori che riassumono le schede sono così riassunti:

- *Media valutazione dell'Ente (escludendo ex P.O.) = 27,49*
 - *Media valutazioni ex P.O. = 28,06*
 - *Media valutazioni ex Categoria “B” = 27,18*
 - *Media valutazioni ex Categoria “C” = 27,75*
 - *Media valutazioni ex Categoria “D” = 27,64*
-