RAPORT

INSTYTUCJE PUBLICZNE

WEJDŹ NA WYŻSZY POZIOM CYFRYZACJI

Wyniki pierwszej fali badania poziomu cyfryzacji przez INEA.

Spis treści



01
Dlaczego INEA mówi o transformacji cyfrowej?

02
Cyfrowy obraz badanych instytucji

03
Jak badaliśmy cyfrową dojrzałość instytucji?

04
Cyfrowa dojrzałość badanych instytucji

05
Łączność i chmura jako cyfrowy fundament

06
Cyfrowa dostępność i komunikacja z odbiorcami

07
Cyfrowy obieg spraw i dokumentów

08
Technologie wspierające instytucję i jej otoczenie

09
Od zabezpieczeń do odporności

10
Co spowalnia kolejny krok i co jest potrzebne do rozwoju?

11
Od diagnozy do działania

12
Metodologia i źródła

Wprowadzenie

Transformacja cyfrowa instytucji publicznych ma bardzo konkretny, społeczny wymiar. Wpływa na to, czy mieszkaniec może łatwo znaleźć potrzebną informację, rodzic sprawnie skontaktować się ze szkołą, a urzędnik szybko dotrzeć do danych niezbędnych do podjęcia decyzji. Decyduje również o dostępności usług dla osób ze szczególnymi potrzebami oraz o zdolności instytucji do działania w sytuacji awarii, cyberataku lub innego zakłócenia.

Dlatego cyfryzacji sektora publicznego nie można sprowadzać do wdrażania kolejnych systemów. Jej rzeczywistą miarą jest to, czy technologia upraszcza codzienne sprawy, skraca czas obsługi, ułatwia pracę i pozwala lepiej odpowiadać na potrzeby lokalnej społeczności. Jednocześnie zmiana nie może prowadzić do powstawania nowych barier. Usługi cyfrowe powinny zwiększać dostępność instytucji, a nie wykluczać osoby, które mają mniejsze kompetencje cyfrowe, ograniczony dostęp do technologii lub wymagają innej formy kontaktu.

Zdecydowaliśmy się na diagnozę, ponieważ każda instytucja rozpoczyna cyfrową zmianę z innego miejsca. Jedne mają już rozbudowane systemy i szukają sposobu na ich integrację, inne koncentrują się na cyfrowym obiegu dokumentów, dostępności usług lub bezpieczeństwie danych. Bez rozpoznania tego punktu wyjścia łatwo inwestować w rozwiązania, które nie odpowiadają na najważniejsze potrzeby organizacji i jej użytkowników.

Ta diagnoza nie jest rankingiem ani obrazem całego sektora publicznego w Polsce. Pokazuje sytuację badanej grupy i ma służyć jako punkt wyjścia do rozmowy o dalszym rozwoju. Pomaga zobaczyć, które fundamenty są już mocne, gdzie technologia wspiera jedynie fragment procesu oraz w jakich obszarach kolejna zmiana może przynieść największą wartość pracownikom, mieszkańcom i innym użytkownikom usług publicznych.

Wierzymy, że dobrze zaplanowana transformacja zaczyna się od właściwego rozpoznania potrzeb. Dopiero później przychodzi czas na wybór technologii, połączenie systemów i określenie skali wdrożenia.

Mamy nadzieję, że ten raport pomoże instytucjom spojrzeć na cyfryzację nie jak na cel sam w sobie, lecz jak na narzędzie budowania bardziej dostępnych, sprawnych i odpornych usług publicznych.



Maciej Hojszyk
Commercial B2B Director INEA

Maciej Piechociński
Prezes Zarządu INEA

Raport przedstawia ciekawe spojrzenie na cyfrową transformację instytucji publicznych, a przy tym wyróżnia się rzetelnością rzadko spotykaną w opracowaniach branżowych. Uważam, że jego wartością jest wskazanie, iż wdrożenie technologii nie gwarantuje zmiany sposobu działania – w raporcie widać to dobrze na przykładzie obiegu dokumentów, jak i cyberbezpieczeństwa. Cenne jest także przejście od logiki zabezpieczeń do logiki odporności zwracające uwagę na działania proaktywne oraz fakt, iż błąd pracownika jest częstszą przyczyną utraty danych niż atak hakerski. Za bardzo wartościowe uważam też rekomendacje, które zamiast presji na kolejne wdrożenia proponują mierzalną ścieżkę zmiany, dopasowaną do punktu wyjścia z którego rozpoczyna dana instytucja. Szczególnie wymowny jest paradoks lidera - niemal połowa instytucji osiąga najwyższy poziom dojrzałości, a zarazem automatyzację decyzji deklarują pojedyncze podmioty. Pokazuje to, że bariera dalszego rozwoju ma przede wszystkim charakter organizacyjny. Już w latach 90. XX wieku Hammer zwracał uwagę, że automatyzowanie istniejących procedur bez ich przeprojektowania nie przynosi poprawy efektywności. To gruntowne przemyślenie modelu działania możliwe dzięki nowym technologiom cyfrowym oraz rozwój kompetencji pracowników będą kluczowe dla uzyskania przełomowych efektów cyfrowej transformacji.



dr hab. Grzegorz Bełz
prof. Uniwersytetu Ekonomicznego we Wrocławiu



01

Dlaczego INEA mówi o transformacji cyfrowej?

01

Dlaczego INEA mówi o transformacji cyfrowej?

Transformacja cyfrowa instytucji publicznych zaczyna się od infrastruktury, ale na niej się nie kończy. Stabilne połączenie z siecią umożliwia korzystanie z systemów, pracę w wielu lokalizacjach, elektroniczny obieg dokumentów i rozwój usług dostępnych online. Dopiero sposób połączenia technologii, procesów i danych decyduje jednak o tym, czy cyfryzacja rzeczywiście poprawia funkcjonowanie instytucji i jakość obsługi jej użytkowników.

W sektorze publicznym efekty transformacji są odczuwalne znacznie szerzej niż wewnątrz samej organizacji. Dotyczą mieszkańców, uczniów i rodziców, pacjentów, przedsiębiorców, pracowników urzędów oraz wszystkich osób korzystających z lokalnych usług. **Technologia wpływa na to, czy informacja jest dostępna i zrozumiała, czy sprawę można przeprowadzić bez zbędnych etapów oraz czy instytucja potrafi zachować ciągłość działania w sytuacji awarii lub zagrożenia.**

Cyfryzacja ma więc również wymiar społeczny. Może ułatwiać dostęp do usług osobom mieszkającym dalej od siedziby instytucji, mającym ograniczoną mobilność lub potrzebującym kontaktu poza standardowymi godzinami pracy.

Powinna jednocześnie uwzględniać potrzeby osób ze szczególnymi potrzebami oraz tych, które nie korzystają swobodnie z kanałów cyfrowych. **Dobrze zaprojektowana usługa poszerza dostęp, zamiast przenosić istniejące bariery do internetu albo tworzyć nowe.**

INEA od lat współpracuje z samorządami, szkołami oraz innymi podmiotami publicznymi. Punktem wyjścia tej współpracy była infrastruktura telekomunikacyjna, jednak wraz z rozwojem usług cyfrowych zmieniały się również potrzeby instytucji. Coraz częściej dotyczą one nie tylko parametrów łącza, lecz także bezpiecznego dostępu do danych, chmury, ciągłości działania, ochrony systemów oraz integracji wykorzystywanych rozwiązań. Ta perspektywa pozwala dostrzec zależności niewidoczne przy analizowaniu pojedynczych technologii: elektroniczny formularz nie usprawni obsługi, jeśli dane trzeba później ręcznie przenieść do innego systemu, a kopia zapasowa nie zapewni ciągłości działania, jeśli instytucja nie potrafi sprawnie odtworzyć danych.

Rola partnera technologicznego nie polega na decydowaniu za instytucję, jak powinna realizować swoje zadania. **Samorząd, szkoła czy urząd najlepiej znają potrzeby swojej społeczności i uwarunkowania własnej pracy.**

INEA może jednak pomóc przełożyć te potrzeby na wymagania technologiczne oraz spojrzeć na infrastrukturę, procesy, dane i bezpieczeństwo jako na elementy jednego środowiska.

Dlatego przedstawiona w raporcie diagnoza nie wskazuje jednego modelu właściwego dla wszystkich. Ma pomóc instytucjom określić punkt wyjścia i rozpoznać obszary, w których technologia może zwiększyć dostępność usług, usprawnić pracę, wzmocnić odporność i lepiej odpowiadać na potrzeby mieszkańców.



02

Cyfrowy obraz badanych instytucji

02

Cyfrowy obraz badanych instytucji

Badane instytucje dysponują mocnymi podstawami technologicznymi, a wiele z nich wykorzystuje już rozwiązania cyfrowe w codziennych procesach i zarządzaniu infrastrukturą. Jednocześnie wysoki poziom łączności nie zawsze przekłada się na równie szerokie zastosowanie chmury, pełną integrację procesów czy gotowość do szybkiego odtworzenia działania po awarii.

Wyniki pokazują więc obraz grupy aktywnej cyfrowo, ale niejednorodnej. Część instytucji może już rozwijać automatyzację i rozwiązania oparte na danych, podczas gdy dla innych ważniejszym zadaniem pozostaje uporządkowanie obiegu informacji, zwiększenie dostępności usług lub wzmocnienie odporności.

niemal **50%** badanych instytucji

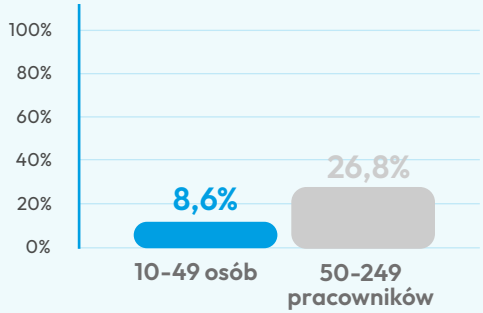
osiągnęło poziom Lidera Cyfrowej Transformacji. Prawie połowa badanej grupy znalazła się na najwyższym poziomie dojrzałości. Wynik odzwierciedla jednak profil próby, obejmującej instytucje aktywnie rozwijające rozwiązania cyfrowe, i nie powinien być odnoszony do całego sektora publicznego.

99%

ma dostęp do internetu stacjonarnego. Stałe łącze jest w badanej grupie rozwiązaniem niemal powszechnym, a 82,9% instytucji deklaruje przepustowość na poziomie co najmniej 100 Mbit/s. Główne wyzwanie przesuwa się zatem z samego dostępu do jakości, przewidywalności i dopasowania parametrów usługi do liczby użytkowników oraz wykorzystywanych systemów.

Wyniki odnoszą się do 82 badanych instytucji. Próba została dobrana celowo i obejmowała podmioty pozostające w kontakcie z INEA, dlatego wyników nie należy uogólniać na cały sektor publiczny.

Technologie są obecne, ale nie wszystkie rozwijają się w tym samym tempie



Źródło: badanie INEA 2026.

63%

korzysta z elektronicznego obiegu dokumentów. Cyfrowy obieg dokumentów funkcjonuje już w większości badanych instytucji. Nie oznacza to jednak automatycznie pełnej cyfryzacji procesu – poszczególne etapy sprawy mogą nadal wymagać ręcznej obsługi, przenoszenia danych albo korzystania z kilku niepołączonych systemów.

46%

wykorzystuje rozwiązania internetu rzeczy. Niemal połowa instytucji korzysta z urządzeń i systemów umożliwiających automatyczne zbieranie danych. Internet rzeczy wspiera przede wszystkim konkretne zadania związane z monitorowaniem infrastruktury, bezpieczeństwem i zarządzaniem zasobami, a jego wartość zależy od powiązania danych z decyzjami i codziennymi procesami.

21%

korzysta z usług chmurowych. Chmura pozostaje jednym z obszarów o największej przestrzeni do rozwoju. Korzystanie z niej wyraźnie rośnie wraz z wielkością instytucji: deklaruje je 8,6% podmiotów zatrudniających 10–49 osób i 26,8% instytucji zatrudniających 50–249 pracowników.

Wyniki odnoszą się do 82 badanych instytucji. Próba została dobrana celowo i obejmowała podmioty pozostające w kontakcie z INEA, dlatego wyników nie należy uogólniać na cały sektor publiczny.

30,5%

stosuje backup zgodny z regułą 3-2-1. Podstawowe zabezpieczenia sieci są szeroko rozpowszechnione, ale pełna odporność wymaga również możliwości szybkiego odtworzenia danych i systemów. Regułę 3-2-1, zakładającą przechowywanie kilku kopii danych na różnych nośnikach, w tym jednej poza główną lokalizacją, stosuje mniej niż jedna trzecia badanych instytucji.

Reguła 3-2-1

- **3** kopia danych
- **2** różne nośniki
- **1** kopia poza główną lokalizacją





03

Jak badaliśmy cyfrową dojrzałość instytucji?

Wyniki pierwszej fali badania poziomu cyfryzacji przez INEA.

Jak badaliśmy cyfrową dojrzałość instytucji?

Raport powstał na podstawie badania przeprowadzonego przez INEA od 17 lipca 2025 r. do 6 lipca 2026 r. W badaniu zarejestrowało się 99 respondentów, a 82 osoby wypełniły ankietę w całości; wszystkie kompletne ankiety włączono do analizy. Respondentów zapraszano mailowo lub telefonicznie. Badanie miało charakter celowy i objęło instytucje pozostające w kontakcie z INEA, w tym wielu jej wieloletnich klientów. Wyniki pokazują więc sytuację badanej grupy i nie są reprezentatywnym obrazem całego sektora publicznego w Polsce.

Odpowiedzi udzielały osoby znające sposób wykorzystania technologii w danej instytucji, m.in. przedstawiciele jej kierownictwa oraz osoby odpowiedzialne za informatykę i cyfryzację. Odpowiedzi miały charakter deklaratywny i nie były niezależnie weryfikowane.

82 **podmioty**
objęte diagnozą

17.07.2025 → 06.07.2026
okres diagnozy

Trzy perspektywy diagnozy

Kwestionariusz obejmował trzy uzupełniające się obszary:

Technologie wspierające procesy i tworzenie wartości

Infrastruktura teleinformatyczna

Bezpieczeństwo cyfrowe

Jak powstał wynik?

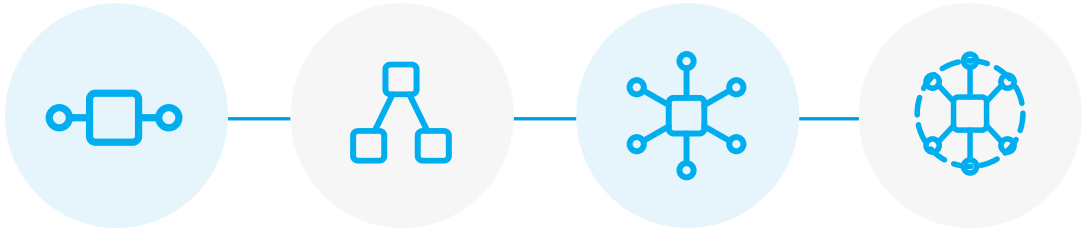
Poziom cyfryzacji został określony na podstawie pięciu grup rozwiązań wspierających funkcjonowanie instytucji:

01	02	03	04	05
strony internetowej i jej dostępności	komunikacji online	elektronicznego obiegu dokumentów	internetu rzeczy	sztucznej inteligencji
25 pkt	**10 pkt**	**35 pkt**	**15 pkt**	**15 pkt**

Sposób przyznawania punktów zależał od charakteru pytania. Uwzględniano fakt korzystania z danego rozwiązania, zakres jego wykorzystania, a w wybranych przypadkach także stopień integracji z innymi rozwiązaniami lub procesami oraz osiągane efekty. Wyższy wynik mógł więc wynikać zarówno z wykorzystania większej liczby technologii, jak i z szerszego lub bardziej zaawansowanego sposobu ich zastosowania.

Cztery poziomy cyfryzacji

Łącznie instytucja mogła uzyskać 100 punktów. Na tej podstawie przypisywano ją do jednego z czterech poziomów:



podstawowy	średnio-zaawansowany	zaawansowany	Lider Cyfrowej Transformacji
0-19	20-39	40-59	60-100

0 pkt ——————————→ 100 pkt

Wagi poszczególnych technologii oraz granice poziomów zostały ustalone przez ekspertów INEA na podstawie ich wiedzy i doświadczenia związanego z cyfryzacją organizacji. Progi nie są równomiernym podziałem skali, lecz odpowiadają kolejnym etapom rozwoju cyfrowego: przejście na wyższy poziom oznacza szersze lub bardziej zaawansowane wykorzystanie rozwiązań objętych modelem. Model ma charakter diagnostyczny – pomaga zdefiniować punkt wyjścia instytucji i wskazać możliwe kierunki dalszego rozwoju.

Model B2P różni się od modelu zastosowanego w badaniu przedsiębiorstw zakresem analizowanych obszarów, ich wagami i progami. Dlatego wartości indeksu oraz udziałów poszczególnych poziomów w obu raportach nie należy ze sobą bezpośrednio porównywać.

Infrastruktura, usługi chmurowe i cyberbezpieczeństwo nie zwiększały bezpośrednio wyniku dojrzałości. W badaniu potraktowano je jako fundament umożliwiający bezpieczne i stabilne korzystanie z technologii wspierających procesy. Samo miejsce przetwarzania danych – lokalnie lub w chmurze – nie przesądza bowiem o poziomie cyfryzacji. W kwestionariuszu B2P nie pytano również o wykorzystanie konkretnych systemów i aplikacji w modelu chmurowym, dlatego ten aspekt nie mógł stanowić odrębnego elementu punktacji.

Poziom nie jest oceną instytucji ani miejscem w rankingu. Pokazuje jej aktualny punkt wyjścia. Wysoki wynik nie oznacza również zakończenia cyfrowego rozwoju: kolejnym krokiem może być modernizacja rozwiązań, ich integracja, szersze wykorzystanie lub lepsze mierzenie osiąganych efektów.

Model nie zakłada, że każda instytucja powinna wdrożyć wszystkie dostępne technologie. Znaczenie ma przede wszystkim to, czy rozwiązania odpowiadają na jej rzeczywiste potrzeby, usprawniają procesy i przynoszą wartość pracownikom oraz użytkownikom usług publicznych.



04

Cyfrowa dojrzałość badanych instytucji

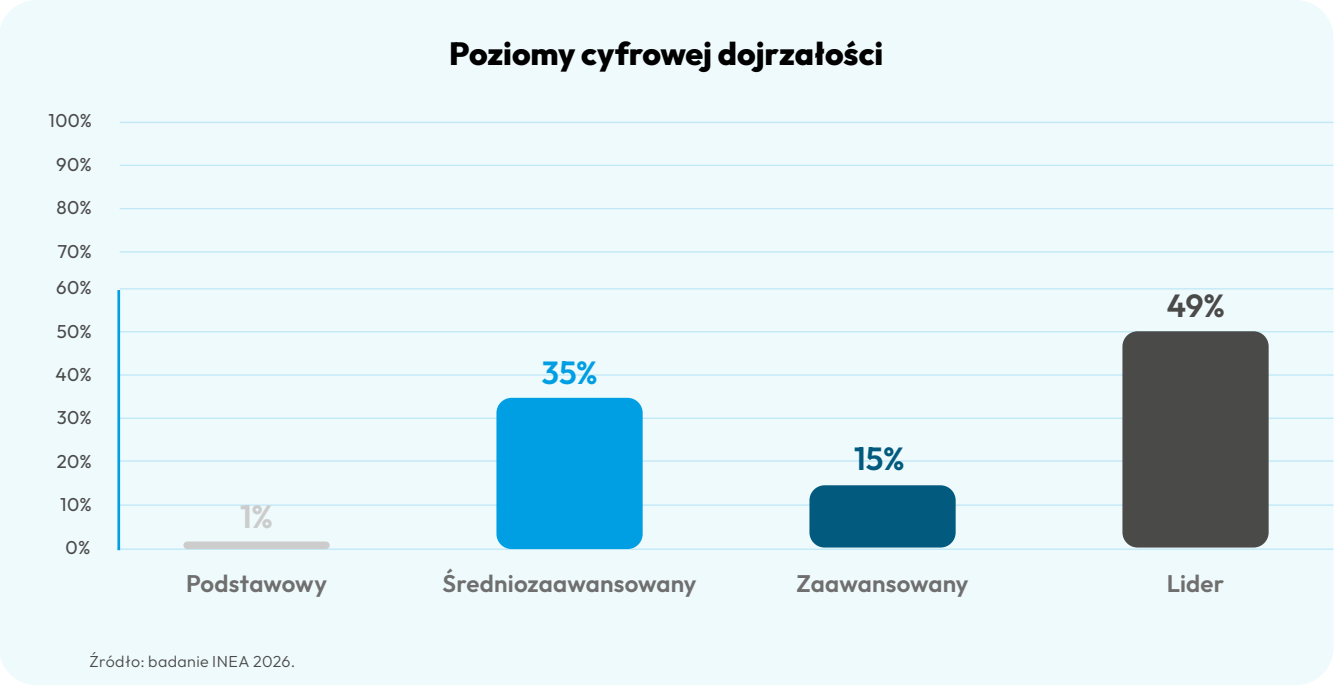
04

Cyfrowa dojrzałość badanych instytucji

Po omówieniu sposobu badania i konstrukcji modelu kolejnym etapem jest obraz cyfrowej dojrzałości analizowanych instytucji. Wyniki pokazują grupę, która w dużej części ma już rozwinięte podstawy cyfrowego działania, a niemal połowa została zakwalifikowana do poziomu lidera.

Wysoki udział liderów wymaga spojrzenia na wyniki szczegółowe

Model dojrzałości syntetyzuje odpowiedzi dotyczące procesów, dostępności usług i wykorzystania narzędzi cyfrowych. Ogólny poziom pokazuje zakres cyfryzacji działania, lecz nie rozstrzyga jeszcze o jakości poszczególnych wdrożeń ani o równowadze między obszarami.



Źródło: badanie INEA 2026.

Niemal połowa instytucji znalazła się w grupie liderów, co należy odczytywać w kontekście celowego doboru próby. Wynik opisuje przede wszystkim punkt startowy respondentów: wiele z tych jednostek ma już narzędzia, a dalszy rozwój zależy od ich integracji, konsekwentnego wykorzystania i mierzenia rezultatów.

Jednocześnie wysoka pozycja w modelu może współistnieć z konkretnymi lukami. Wyniki cząstkowe pokazują, że usługi dla odbiorców, odporność, obieg informacji i nowe modele pracy nie w każdej instytucji rozwijają się w tym samym tempie.

Dlatego ogólny poziom warto czytać razem z rezultatami w kolejnych częściach raportu. Takie zestawienie pozwala odróżnić obszary już uporządkowane od tych, w których potrzebne są inwestycje, standaryzacja albo zmiana sposobu organizacji pracy.

Pierwszym obszarem szczegółowej analizy jest infrastruktura. Stabilna łączność i dostęp do zasobów tworzą warunki dla rozwoju usług, ale dopiero kolejne rozdziały pokażą, jak te podstawy przekładają się na procesy, dane i odporność instytucji.



05

Łączność i chmura jako cyfrowy fundament

05

Łączność i chmura jako cyfrowy fundament

Cyfrowe usługi i sprawna praca instytucji opierają się na stabilnej łączności oraz bezpiecznym dostępie do danych i systemów. Sama infrastruktura nie tworzy jeszcze wartości, ale usuwa bariery utrudniające obsługę użytkowników, współpracę zespołów i rozwój kolejnych usług.

Na cyfrowy fundament składają się parametry i niezawodność połączenia, mobilność pracowników oraz sposób korzystania z chmury. Kluczowe pytanie dotyczy nie liczby rozwiązań, lecz tego, czy infrastruktura odpowiada potrzebom instytucji i zapewnia ciągłość działania.

Cyfrowy fundament budują:



parametry i niezawodność połączenia



mobilność pracowników

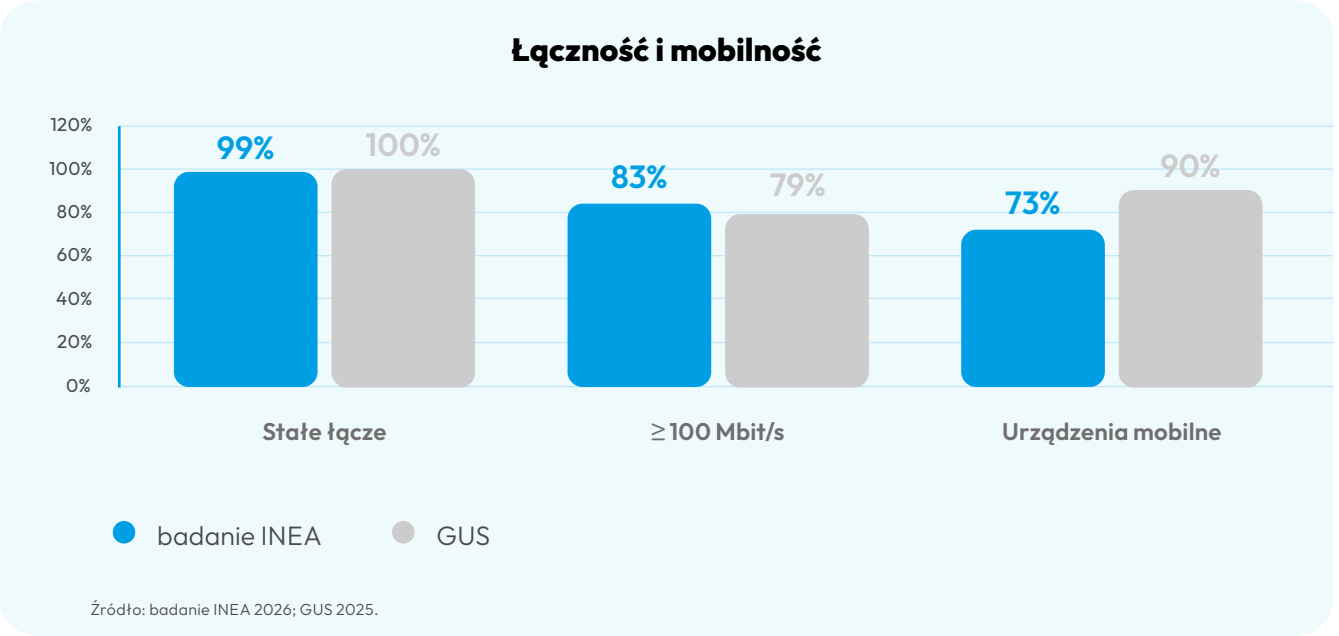


sposób korzystania z chmury

05.1 **Cyfrowy fundament: łączność i mobilność**

Cyfrowy fundament: łączność i mobilność

Sprawna łączność warunkuje działanie usług cyfrowych, systemów obsługujących konkretne obszary działalności instytucji (systemów dziedzinowych) oraz pracę poza jej siedzibą. Znaczenie ma nie tylko dostęp do sieci, lecz także jakość, przewidywalność i odporność połączenia na awarie.



Źródło: badanie INEA 2026; GUS 2025.

Dostęp do internetu stacjonarnego jest w badanej grupie niemal powszechny, a zdecydowana większość instytucji deklaruje łącze o przepustowości co najmniej 100 Mbit/s. Bariera podstawowego dostępu jest więc niewielka. Coraz większego znaczenia nabierają natomiast parametry usługi, dopasowanie przepustowości do liczby użytkowników i systemów oraz możliwość skalowania infrastruktury.

Na tle danych GUS badane instytucje osiągają zbliżony poziom dostępu do stałego łącza i nieco częściej deklarują przepustowość co najmniej 100 Mbit/s. Wyraźniejsza różnica dotyczy urządzeń mobilnych dla pracowników – w badanej grupie korzysta z nich 73% instytucji wobec 90% w danych GUS.

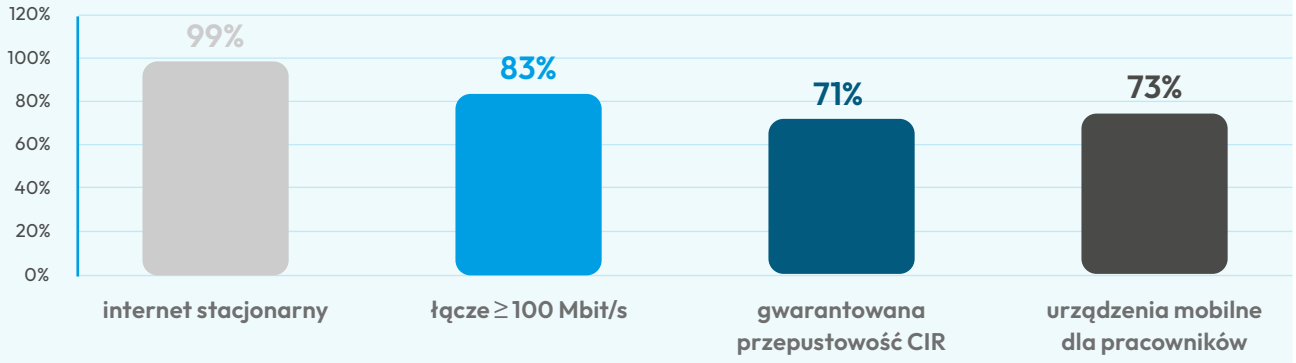
05.1 **Cyfrowy fundament: łączność i mobilność**

Szybkość nie wystarcza, gdy usługi muszą działać bez przerw

Gwarantowany poziom przepustowości łącza (CIR) deklaruje większość respondentów. Ma on znaczenie szczególnie tam, gdzie obsługa użytkowników, systemy chmurowe i dostęp do danych zależą od ciągłości połączenia. Jakość łącza warto więc oceniać razem z rozwiązaniami zapasowymi i praktykami zapewniania ciągłości działania.

Urządzenia mobilne są wykorzystywane w większości badanych instytucji, ale sama ich obecność nie zapewnia mobilności organizacji. Znaczenie mają również bezpieczny dostęp do systemów, odpowiednie procedury, kompetencje i procesy możliwe do realizacji poza tradycyjnym stanowiskiem pracy.

Łączność i mobilność badanych instytucji



Źródło: badanie INEA 2026.

Chmura: potencjał większy niż obecna skala wykorzystania

Usługi chmurowe pozwalają korzystać z infrastruktury, oprogramowania i przestrzeni na dane bez utrzymywania wszystkich zasobów we własnej serwerowni. Dla instytucji publicznych mogą oznaczać łatwiejsze skalowanie usług, szybsze uruchamianie nowych rozwiązań oraz większą elastyczność pracy. Warunkiem pozostają jednak właściwy dobór modelu, bezpieczeństwo danych i zgodność z wymaganiami prawnymi.

Chmura obliczeniowa

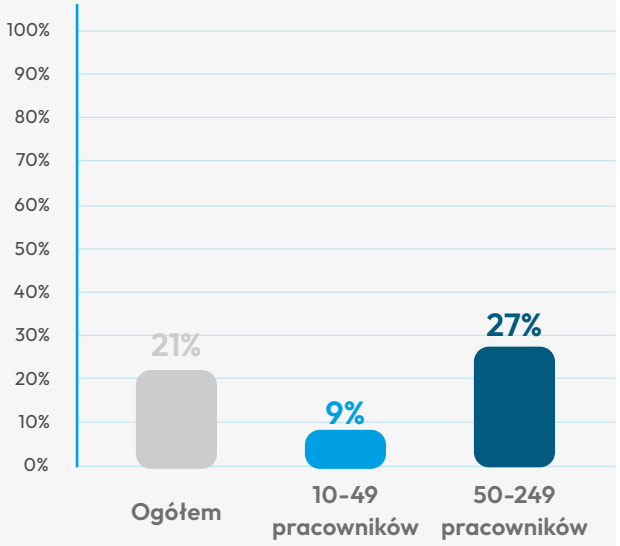
Co to jest?

Chmura obliczeniowa umożliwia korzystanie przez internet z aplikacji, systemów, przestrzeni na dane i innych zasobów IT udostępnianych przez zewnętrznego dostawcę. Instytucja nie musi utrzymywać wszystkich potrzebnych serwerów i rozwiązań we własnej infrastrukturze.

Co instytucja może zyskać?

- możliwość skalowania zasobów bez rozbudowy własnej infrastruktury;
- dostęp do danych i aplikacji z różnych lokalizacji oraz urządzeń;
- szybsze uruchamianie nowych usług i możliwość ograniczenia części kosztów utrzymania IT.

Wykorzystanie usług chmurowych



Uwaga: nie pokazano grup <10 i 250+ ze względu na małe liczebności.
Źródło: badanie INEA 2026.

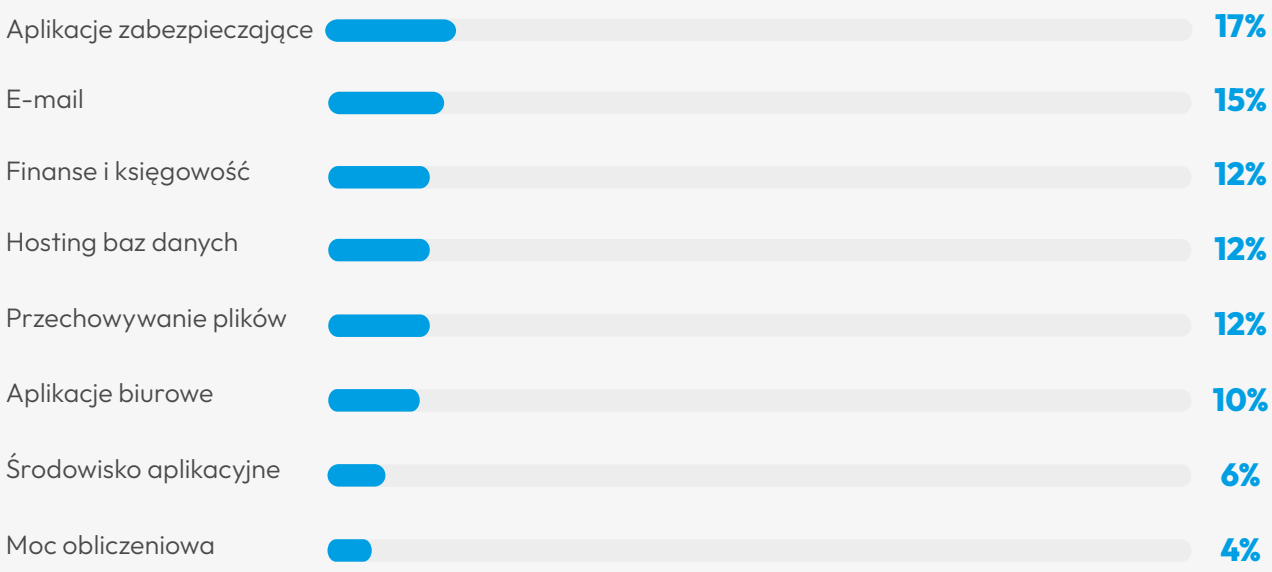
05.2 **Chmura: potencjał większy niż obecna skala wykorzystania**

Z usług chmurowych korzysta 20,7% badanych jednostek. Na tle niemal powszechnego dostępu do internetu jest to wyraźnie niższy wynik. Pokazuje, że rozwój infrastruktury dostępowej nie prowadzi automatycznie do zmiany sposobu utrzymywania systemów i zasobów. Przejście do chmury jest decyzją organizacyjną, finansową i prawną, a nie tylko technologiczną.

Różnice w badanej grupie sugerują, że znaczenie ma również skala instytucji. W dwóch najliczniejszych grupach chmura jest wyraźnie częściej wykorzystywana przez jednostki zatrudniające od 50 do 249 osób niż przez podmioty zatrudniające od 10 do 49 osób.

Wśród wskazywanych zastosowań pojawiają się aplikacje zabezpieczające, poczta elektroniczna, systemy finansowo-księgowe, hosting baz danych, przechowywanie plików i aplikacje biurowe. Taki układ pokazuje dwa możliwe punkty wejścia: przeniesienie do chmury usług powszechnych i łatwych do wydzielenia albo wykorzystanie jej do obsługi wyspecjalizowanych zasobów i systemów.

Zastosowania usług chmurowych



Źródło: badanie INEA 2026.

Chmura zmienia sposób utrzymania usług i podział odpowiedzialności

Przeniesienie usługi poza własną serwerownię oznacza inny model zarządzania, a nie przekazanie całej odpowiedzialności dostawcy. Znaczenie mają architektura rozwiązania, zasady dostępu, możliwość przenoszenia i odtworzenia danych oraz procedury na wypadek niedostępności. Dopiero tak przygotowane zaplecze pozwala rozwijać usługi widoczne dla odbiorców.



06

Cyfrowa dostępność i komunikacja z odbiorcami

06

Cyfrowa dostępność i komunikacja z odbiorcami

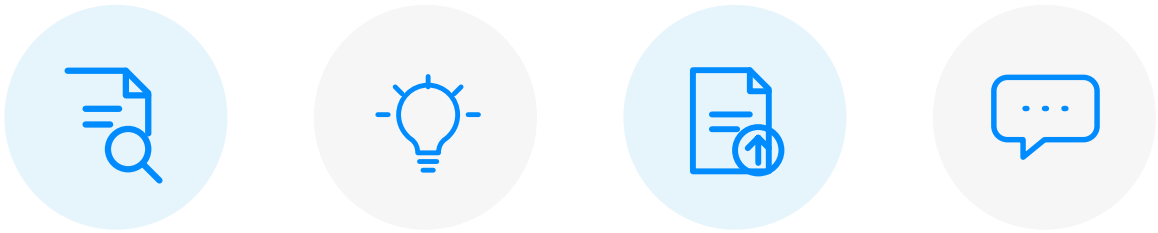
Sprawna infrastruktura tworzy warunki do uruchamiania usług, ale o ich użyteczności decyduje sposób, w jaki instytucja kontaktuje się z odbiorcami. Dla wielu użytkowników strona internetowa jest pierwszym miejscem tego kontaktu: powinna pomagać znaleźć właściwą usługę, zrozumieć wymagania, przekazać dokument i wybrać dogodny kanał komunikacji.

Wyniki badania pokazują dwie uzupełniające się perspektywy. Pierwsza dotyczy korzystania przez instytucje z wybranych kanałów komunikacji, druga – deklarowanego spełniania wymagań dostępności cyfrowej przez poszczególne elementy strony internetowej lub aplikacji mobilnej.

Samo wykorzystywanie danego kanału nie przesądza o jego dostępności ani jakości obsługi. Z kolei deklarowane spełnianie wymagań dostępności nie jest równoznaczne z pełną dostępnością całej strony, dokumentów i formularzy. Nie mówi też, czy użytkownik może łatwo dotrzeć do potrzebnych treści i przeprowadzić całą sprawę online.

Kolejnym etapem rozwoju jest więc nie tylko poszerzanie zakresu komunikacji cyfrowej, lecz także sprawdzanie, czy poszczególne kanały i treści są dostępne, aktualne i użyteczne dla odbiorców.

Funkcje strony internetowej



znalezienie właściwej usługi

zrozumienie wymagań

przekazanie dokumentów

wybranie dogodnego kanału komunikacji

Nie wszystkie elementy w takim samym stopniu spełniają wymagania dostępności

Najwyższy odsetek deklaracji spełniania wymagań dostępności cyfrowej dotyczy deklaracji dostępności oraz danych kontaktowych i BIP. Niższe wyniki odnotowano w przypadku nawigacji, dokumentów i formularzy, narzędzi kontaktu oraz informacji kryzysowych. Są to deklaracje badanych instytucji, a nie wyniki niezależnego audytu dostępności.

Z perspektywy użytkownika liczy się ciągłość całej drogi: od znalezienia informacji, przez kontakt i przekazanie dokumentów, po otrzymanie odpowiedzi. Pojedyncze funkcje zyskują znaczenie wtedy, gdy tworzą spójną ścieżkę obsługi, a nie zbiór odrębnych elementów serwisu.

Platformy społecznościowe poszerzają zasięg, ale nie zastępują e-usług

Sieci społecznościowe wykorzystuje zdecydowana większość badanych instytucji. Multimedia i aplikacje dla mieszkańców są mniej powszechne. Pokazuje to, że komunikacja w popularnych kanałach rozwija się szybciej niż dedykowane narzędzia cyfrowej obsługi.

Aplikacje dla mieszkańców

Co to jest?

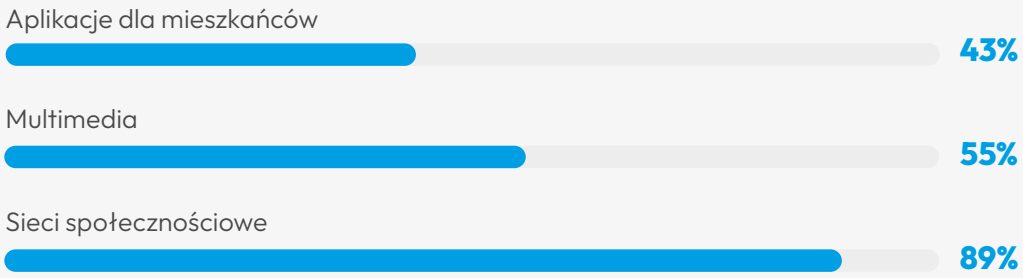
Aplikacja dla mieszkańców to cyfrowy kanał łączący instytucję z lokalną społecznością. Może służyć do przekazywania informacji i powiadomień, przyjmowania zgłoszeń, udostępniania usług oraz ułatwiania kontaktu z urzędem lub inną jednostką publiczną. Przykładem takiego rozwiązania oferowanego przez INEA jest Hello City.

Co instytucja może zyskać?

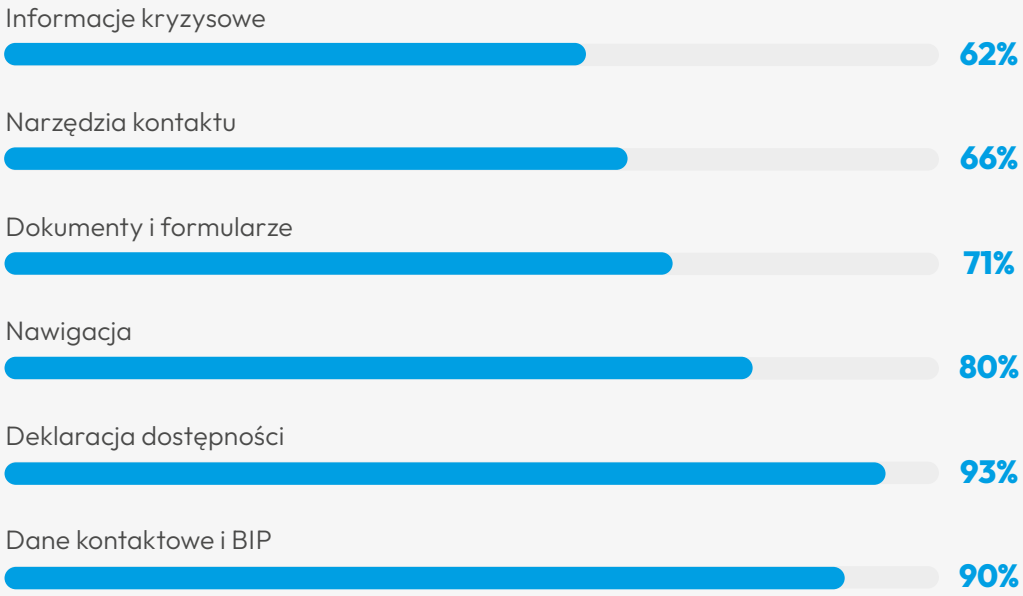
- szybsze docieranie do mieszkańców z informacjami, również w sytuacjach kryzysowych;
- wygodniejszy dostęp do usług, zgłoszeń i kontaktu z instytucją;
- lepsze rozpoznawanie potrzeb mieszkańców dzięki informacjom zwrotnym i zgłoszeniom.

06 **Cyfrowa dostępność i komunikacja z odbiorcami**

Wykorzystanie kanałów komunikacji



Deklarowane spełnianie wymagań dostępności cyfrowej



Uwaga: pierwsze trzy wskaźniki pokazują odsetek instytucji korzystających z poszczególnych kanałów komunikacji. Pozostałe pokazują odsetek wszystkich badanych instytucji deklarujących spełnianie wymagań dostępności cyfrowej przez wskazane elementy strony internetowej lub aplikacji mobilnej. Wyniki mają charakter deklaratywny i nie stanowią audytu dostępności. Źródło: badanie INEA 2026.

Zestawienie łączy dwie perspektywy, których nie należy porównywać jak jednego rankingu. Pierwsze trzy wskaźniki pokazują wykorzystanie kanałów komunikacji, a pozostałe – deklarowane spełnianie wymagań dostępności cyfrowej. Nie każda instytucja potrzebuje własnej aplikacji, a sam fakt korzystania z danego kanału nie przesądza o jakości obsługi.

Spójność komunikacji oznacza, że strona, BIP, media społecznościowe i aplikacje powinny prowadzić użytkownika do tego samego procesu, choć każdy kanał pełni inną funkcję: informuje, przyjmuje zgłoszenie albo umożliwia realizację formalnej sprawy. W tym miejscu doświadczenie odbiorcy łączy się już bezpośrednio z wewnętrznym obiegiem dokumentów i decyzji.



07

Cyfrowy obieg spraw i dokumentów

07

Cyfrowy obieg spraw i dokumentów

Cyfrowy kontakt z użytkownikiem jest tylko początkiem. O jakości obsługi decyduje również to, co dzieje się po przekazaniu formularza lub dokumentu do instytucji. Elektroniczny obieg dokumentów może skrócić czas przekazywania spraw, ułatwić kontrolę terminów i ograniczyć zależność od dokumentacji papierowej. Korzyści pojawiają się jednak dopiero wtedy, gdy system obejmuje rzeczywisty przebieg pracy, a pracownicy konsekwentnie korzystają z niego na kolejnych etapach procesu.

Korzystanie z elektronicznego obiegu dokumentów deklaruje 63,4% badanych jednostek. Rozwiązanie jest więc obecne w większości analizowanej grupy, ale nie stanowi jeszcze powszechnego standardu. Badanie nie pokazuje natomiast, w jakim zakresie pozostałe instytucje wykorzystują dokumenty papierowe, pocztę elektroniczną lub inne narzędzia do obsługi spraw.

Elektroniczny obieg dokumentów

Co to jest?

Elektroniczny obieg dokumentów porządkuje i automatyzuje drogę dokumentu: od jego utworzenia lub rejestracji, przez przekazanie, weryfikację, akceptację i podpis, aż po archiwizację. Nie jest wyłącznie repozytorium plików – wspiera zarządzanie przebiegiem spraw i odpowiedzialnością za poszczególne etapy.

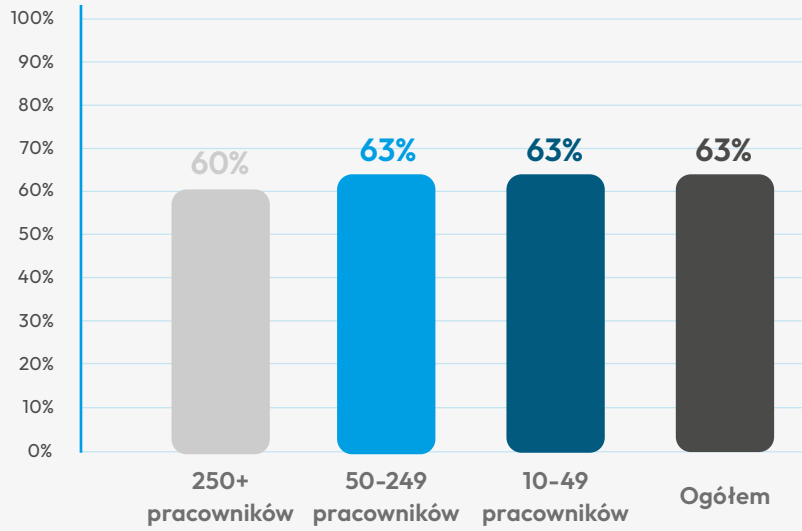
Co instytucja może zyskać?

- krótszy czas realizacji spraw i mniej czynności wykonywanych ręcznie;
- łatwiejszy dostęp do dokumentów oraz aktualnej informacji o statusie sprawy;
- większą kontrolę nad terminami, uprawnieniami i zgodnością procesu z procedurami.

07 **Cyfrowy obieg spraw i dokumentów**

W instytucjach zatrudniających 10–49 oraz 50–249 osób wynik jest niemal identyczny.

W instytucjach zatrudniających 10–49 oraz 50–249 osób wynik jest niemal identyczny. W tej próbie wielkość instytucji nie różnicuje więc wyraźnie samego faktu korzystania z elektronicznego obiegu dokumentów. Nie przesądza to jednak o zakresie wdrożenia ani stopniu wykorzystania systemu.



Źródło: badanie INEA 2026.

07 **Cyfrowy obieg spraw i dokumentów**

Od elektronicznej rejestracji do cyfrowego przebiegu sprawy

System może służyć wyłącznie do rejestracji dokumentów, podczas gdy ich dalsza obsługa nadal odbywa się poza nim. Pełniejsza cyfryzacja opiera się na zdefiniowanych ścieżkach akceptacji, odpowiedzialności i terminach, a także uporządkowanych uprawnieniach, metadanych, archiwizacji i zasadach podpisywania dokumentów.

Znaczenie ma także integracja z innymi narzędziami. Jeżeli korespondencja wpływa cyfrowo, ale dane trzeba ręcznie przenosić do systemów obsługujących poszczególne obszary działalności, część korzyści znika. Podobny problem pojawia się wtedy, gdy użytkownik może przesłać formularz online, lecz dalszy przebieg sprawy pozostaje niewidoczny i wymaga kontaktu telefonicznego.

Pełny obraz daje dopiero przebieg sprawy od początku do końca

O stopniu wykorzystania systemu więcej niż sam fakt wdrożenia mówi udział spraw prowadzonych w pełni cyfrowo, liczba rzeczywistych użytkowników, integracja z innymi rozwiązaniami oraz możliwość monitorowania czasu i wyniku procesu.

Takie podejście przesuwa uwagę z zakupu technologii na efekt organizacyjny. Elektroniczny obieg dokumentów staje się wtedy narzędziem usprawniania obsługi, a nie wyłącznie cyfrowym odpowiednikiem papierowego archiwum. Gdy proces jest uporządkowany i zintegrowany, kolejnym krokiem staje się wykorzystanie danych do monitorowania zjawisk i wspierania decyzji.

Pełny obraz daje dopiero przebieg sprawy od początku do końca.





08

Technologie wspierające instytucję i jej otoczenie

08

Technologie wspierające instytucję i jej otoczenie

Uporządkowane procesy i dane tworzą podstawę do wykorzystania technologii, które nie tylko cyfryzują istniejące czynności, ale także wspierają obserwowanie otoczenia i podejmowanie decyzji. W badanej grupie taką rolę pełnią przede wszystkim internet rzeczy i sztuczna inteligencja.

Internet rzeczy jest stosowany przede wszystkim tam, gdzie można zbierać dane z fizycznego otoczenia. Zastosowania AI koncentrują się natomiast na pracy z tekstem i mową. Znacznie rzadziej technologia przejmuje całe sekwencje działań lub wspiera automatyzację decyzji.



publiczne

Internet rzeczy: dane z infrastruktury wspierają konkretne zadania

Internet rzeczy, czyli sieć połączonych urządzeń i czujników, pozwala automatycznie zbierać oraz przekazywać dane o obiektach i procesach. Z takich rozwiązań korzysta 46,3% badanych instytucji. Wynik wskazuje, że internet rzeczy jest obecny w niemal połowie analizowanej grupy, choć zakres wdrożeń może być bardzo różny.

Internet rzeczy – IoT

Co to jest?

Internet rzeczy obejmuje połączone z siecią urządzenia, maszyny i czujniki, które automatycznie zbierają oraz wymieniają dane. Pozwala monitorować infrastrukturę, środowisko i przestrzeń publiczną, a także reagować na zmieniające się warunki.

Co instytucja może zyskać?

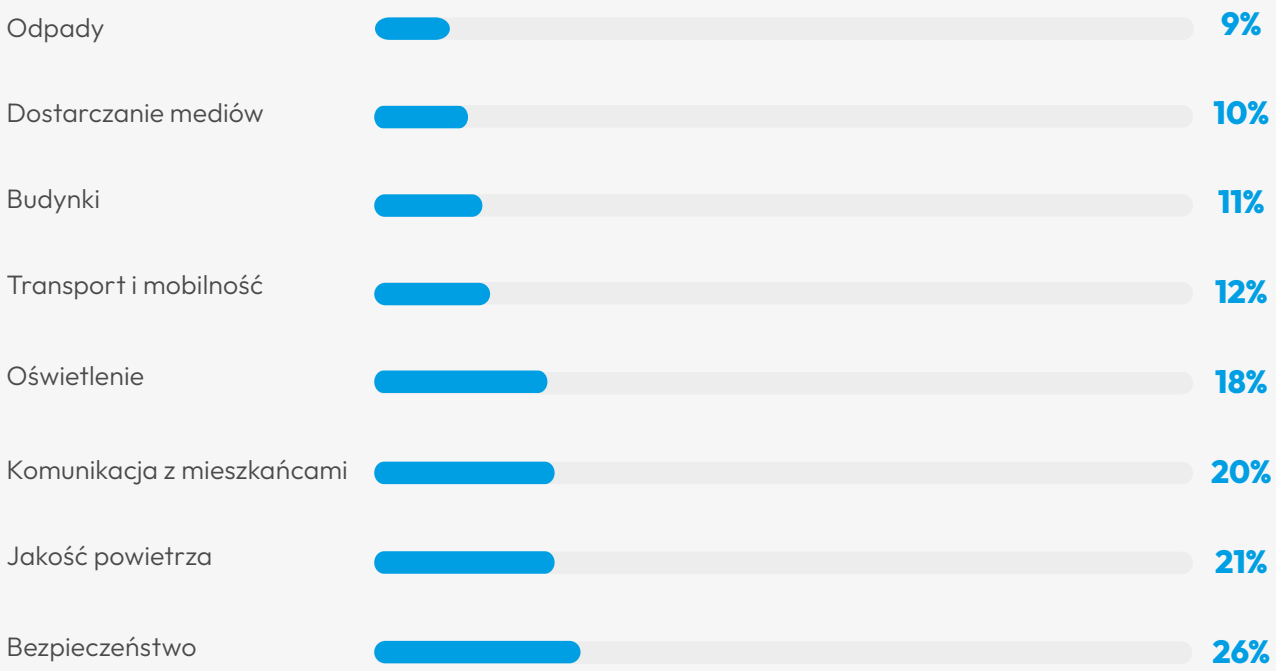
- szybsze wykrywanie awarii, zagrożeń i nieprawidłowości;
- efektywniejsze zarządzanie energią, wodą, transportem i innymi zasobami;
- aktualne dane wspierające planowanie działań i podejmowanie decyzji.

Najczęściej wskazywanym zastosowaniem internetu rzeczy jest bezpieczeństwo. Do częstszych zastosowań należą również monitorowanie jakości powietrza, komunikacja z odbiorcami usług oraz zarządzanie oświetleniem. Pokazuje to praktyczny charakter wdrożeń: technologia służy przede wszystkim obserwowaniu warunków i reagowaniu na zdarzenia.

Rzadziej internet rzeczy wspiera transport i mobilność, zarządzanie budynkami, dostarczanie mediów oraz gospodarkę odpadami. Nie tworzy to rankingu ważności: poszczególne zastosowania zależą od zakresu zadań i infrastruktury pozostającej pod kontrolą danej instytucji.

08.1 **Internet rzeczy: dane z infrastruktury wspierają konkretne zadania**

Zastosowania internetu rzeczy



Uwaga: pytanie o zastosowania internetu rzeczy dopuszczało wiele odpowiedzi; wartości nie sumują się do 100%.
Źródło: badanie INEA 2026.

Bez integracji i jasno opisanej obsługi alertów rośnie liczba informacji, ale niekoniecznie skuteczność działania instytucji.

Dane z urządzeń mają znaczenie dopiero w konkretnym procesie

Czujnik dostarcza sygnału, lecz rezultat zależy od dalszego przebiegu informacji. Dane powinny trafiać do systemu, w którym można je analizować, określać progi alarmowe i kierować zgłoszenia do osób odpowiedzialnych za reakcję. Bez integracji i jasno opisanej obsługi alertów rośnie liczba informacji, ale niekoniecznie skuteczność działania instytucji.

Sztuczna inteligencja: najpierw język, dopiero później automatyzacja

Najczęstsze zastosowania sztucznej inteligencji w badanej grupie dotyczą pracy z językiem. Rozwiązania zamieniające mowę na tekst wykorzystuje 20,7% instytucji; rzadziej wskazywane są analiza tekstu i generowanie języka. Funkcje te mogą wspierać przygotowywanie treści, porządkowanie dokumentów, transkrypcję oraz wyszukiwanie informacji.

Sztuczna inteligencja – AI

Co to jest?

Sztuczna inteligencja obejmuje technologie, które analizują dane, rozpoznają wzorce, przetwarzają tekst, obrazy i mowę, generują treści lub automatyzują wybrane zadania. W instytucjach publicznych jej wykorzystanie wymaga odpowiedniego nadzoru człowieka oraz jasnych zasad dotyczących danych i odpowiedzialności.

Co instytucja może zyskać?

- odciążenie pracowników od części powtarzalnych i czasochłonnych czynności;
- sprawniejszy dostęp mieszkańców i pracowników do potrzebnych informacji;
- lepsze wykrywanie błędów, zależności i obszarów wymagających reakcji.



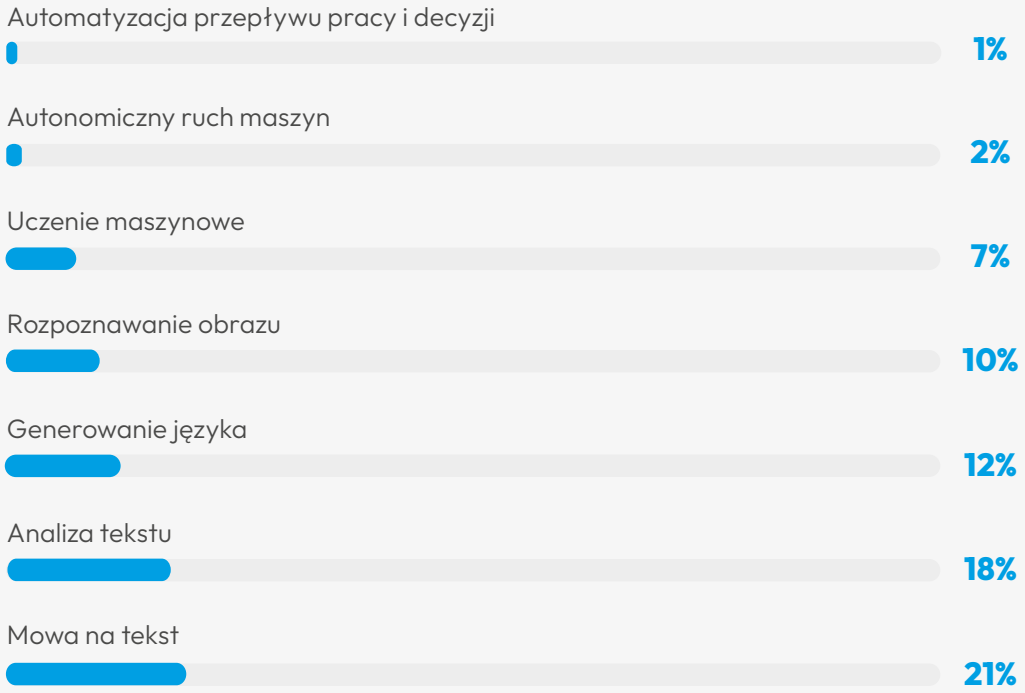
08.2 **Sztuczna inteligencja: najpierw język, dopiero później automatyzacja**

Rozwiązania zamieniające mowę na tekst są wykorzystywane przez instytucje najczęściej. Rozpoznawanie obrazu i uczenie maszynowe są wskazywane rzadziej. Zastosowania bezpośrednio ingerujące w przebieg procesów pozostają jednostkowe: automatyzację przepływu pracy i podejmowania decyzji deklaruje 1,2% badanych instytucji.

Obecny układ zastosowań pokazuje, że AI pełni najczęściej rolę pomocniczą: usprawnia konkretne zadanie, ale nie przejmuje całego procesu. Przejście do automatyzacji wymaga już uporządkowanych danych, jednoznacznych reguł, kontroli jakości i odpowiedzialności za rezultat.

W instytucjach publicznych szczególnego znaczenia nabierają ochrona danych, przejrzystość działania narzędzia i możliwość zweryfikowania wyniku przez człowieka. Wraz ze wzrostem wpływu technologii na sytuację użytkownika rośnie potrzeba nadzoru, dokumentowania procesu oraz jasnych zasad użycia. Zależność od danych i systemów prowadzi zarazem do pytania o odporność całego środowiska cyfrowego.

Zastosowania sztucznej inteligencji



Uwaga: pytanie dopuszczało wiele odpowiedzi; wartości nie sumują się do 100%.
Źródło: badanie INEA 2026.



09

Od zabezpieczeń do odporności

09

Od zabezpieczeń do odporności

Wraz z rosnącą liczbą systemów, urządzeń i danych bezpieczeństwo cyfrowe nie kończy się na blokowaniu ataków. Instytucja odporna potrafi również wykryć incydent, ograniczyć jego skutki, odtworzyć dane i utrzymać najważniejsze usługi. Wyniki badania pokazują wyraźną różnicę między powszechnym stosowaniem podstawowych zabezpieczeń a praktykami, które przygotowują organizację na sytuację, gdy ochrona okaże się niewystarczająca.

Bezpieczeństwo cyfrowe to również

- wykrywanie incydentów
- ograniczanie jego skutków
- odtworzenie danych
- utrzymanie najważniejszych usług



09.1 **Zabezpieczenia techniczne są powszechne**

Zabezpieczenia techniczne są powszechne

Programy antywirusowe i zapory sieciowe są w badanej grupie niemal powszechne, a dostęp przez VPN również należy do często stosowanych rozwiązań. Bardziej zaawansowane narzędzia służące do wykrywania i blokowania zagrożeń oraz ochrony usług internetowych są mniej powszechne; pełny rozkład wyników pokazuje wykres.

Wyniki pokazują wielowarstwowy charakter ochrony w badanej grupie. Nie pozwalają jednak ocenić jakości konfiguracji, zakresu monitorowania ani szybkości reakcji na alerty. Samo wdrożenie narzędzia nie jest równoznaczne z jego skutecznym wykorzystaniem.

Ochrona Anty-DDoS

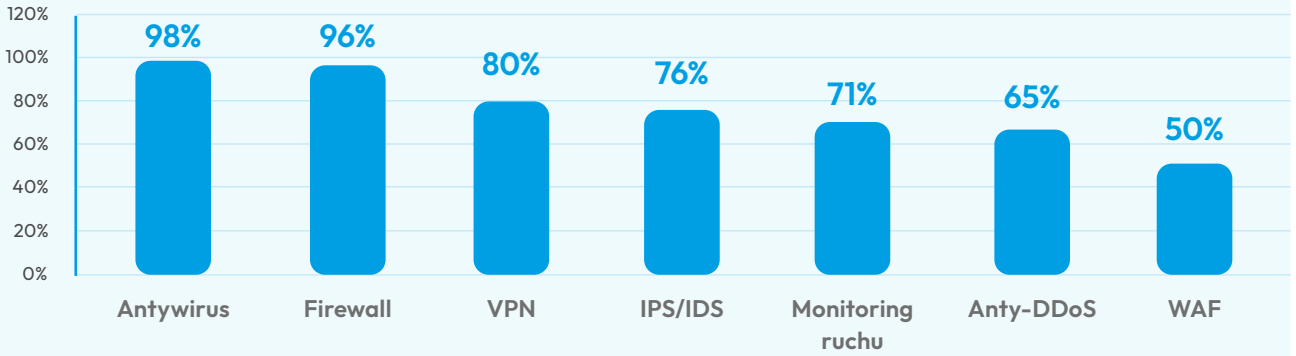
Co to jest?

Anty-DDoS chroni sieć i usługi internetowe przed atakami polegającymi na przeciążeniu ich bardzo dużą liczbą zapytań. Rozwiązanie rozpoznaje i filtruje szkodliwy ruch, umożliwiając dostęp do usług uprawnionym użytkownikom.

Co instytucja może zyskać?

- większą dostępność stron, systemów i usług cyfrowych podczas próby ataku;
- ograniczenie ryzyka przerw w obsłudze mieszkańców i realizacji zadań publicznych;
- szybsze ograniczenie skutków incydentu i większą odporność infrastruktury.

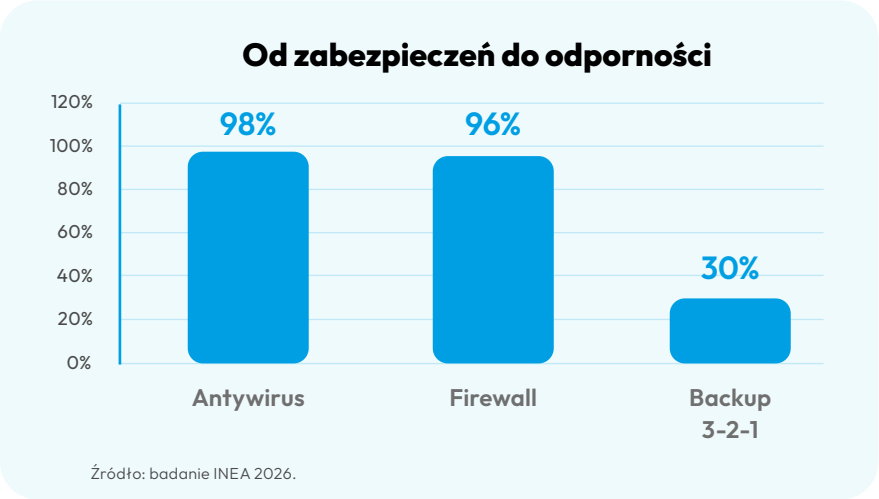
Warstwy ochrony sieci



Uwaga: wskaźniki opisują deklarowane stosowanie rozwiązań, a nie ocenę ich konfiguracji lub skuteczności. Źródło: badanie INEA 2026.

Odporność zaczyna się tam, gdzie ochrona może zawieść

Regułę backupu 3-2-1 deklaruje 30,5% badanych instytucji. Zakłada ona utrzymywanie trzech kopii danych, na dwóch rodzajach nośników, przy czym jedna kopia znajduje się poza podstawową lokalizacją. Na tle niemal powszechnego używania oprogramowania antywirusowego i zapory sieciowej wynik ten pokazuje, że działania związane z odtworzeniem danych są znacznie mniej rozpowszechnione niż narzędzia ochrony podstawowej.



Źródło: badanie INEA 2026.

Kopia zapasowa ma wartość wtedy, gdy jest kompletna, odseparowana od środowiska produkcyjnego i możliwa do odtworzenia w wymaganym czasie. O dojrzałości decydują więc także regularność backupu, testy odtworzeniowe, odpowiedzialność za proces oraz jego powiązanie z planem ciągłości działania.

Szkolenie jest częste, praktyczne testowanie znacznie rzadsze

Szkolenia z bezpieczeństwa prowadzi 82,9% badanych instytucji. Symulowane ataki deklaruje natomiast 30,5%. Różnica pokazuje, że przekazywanie wiedzy jest znacznie częstsze niż sprawdzanie zachowania pracowników w warunkach zbliżonych do rzeczywistego incydentu.

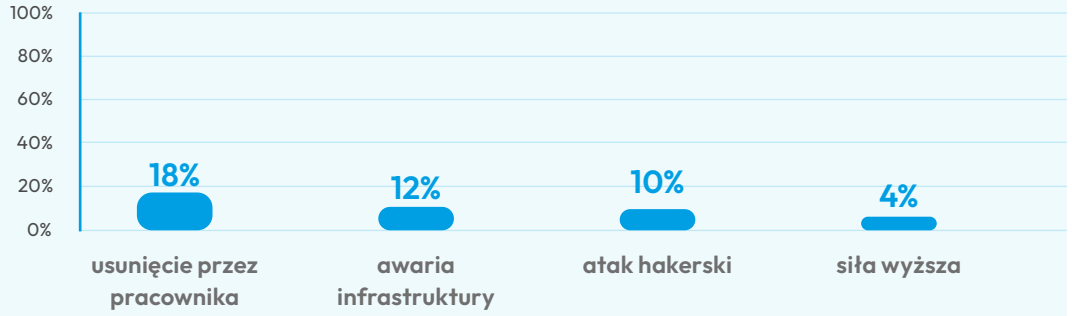
Obie praktyki pełnią inne funkcje. Szkolenie pomaga zrozumieć zasady i rozpoznawać zagrożenia, natomiast symulacja pokazuje, czy pracownicy potrafią zastosować tę wiedzę. Powtarzane testy pozwalają też wskazać procesy i grupy wymagające dodatkowego wsparcia bez sprowadzania bezpieczeństwa do jednorazowego obowiązku szkoleniowego.

Utrata danych nie zawsze zaczyna się od ataku

Usunięcie danych przez pracownika wskazuje 18,3% badanych instytucji, niemal dwa razy więcej niż atak hakerski (9,8%). Wśród deklarowanych przyczyn pojawiają się również awarie infrastruktury i zdarzenia związane z siłą wyższą.

Odporność obejmuje zarówno zagrożenia zewnętrzne, jak i codzienne błędy oraz awarie. Ograniczenie ryzyka wspierają właściwe uprawnienia, przywracanie wcześniejszych wersji, monitoring operacji na danych, prosty sposób zgłaszania incydentów i regularne testy odtwarzania.

Deklarowane przyczyny utraty danych



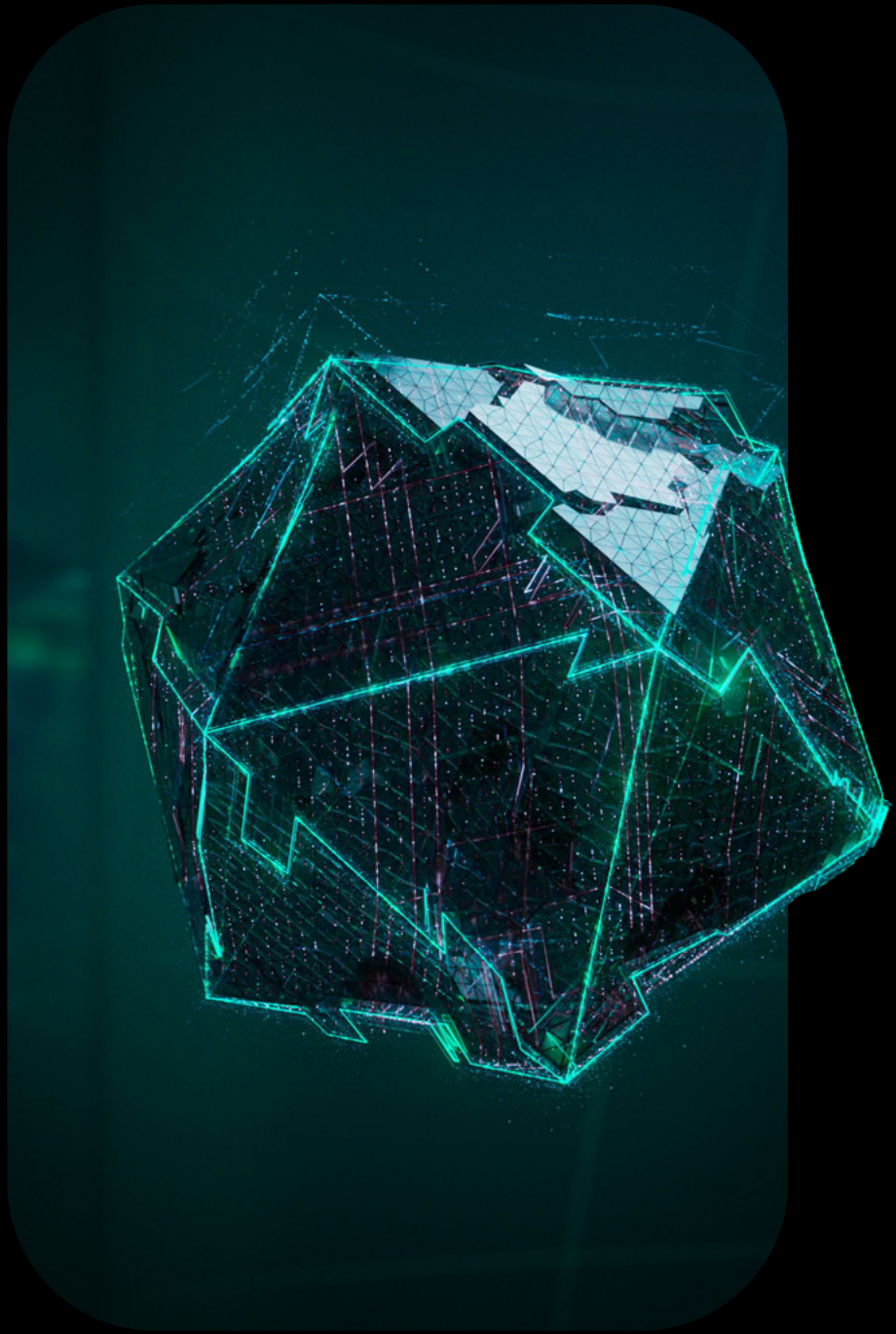
Uwaga: pytanie o przyczyny utraty danych dopuszczało wiele odpowiedzi; wartości nie sumują się do 100%.
Źródło: badanie INEA 2026.

Odporność łączy technologię, procesy i przygotowanie ludzi

Dojrzałe podejście łączy profilaktykę, wykrywanie, reakcję i odtworzenie działania. Wymaga wspólnego planu dla technologii, procesów i ludzi: określenia usług krytycznych, dopuszczalnego czasu niedostępności, odpowiedzialności za decyzje oraz sposobu komunikacji podczas incydentu.

Praktyczny obraz odporności dają trzy pytania: co wydarzy się po przełamaniu zabezpieczeń, jak szybko instytucja wykryje problem i w jakim czasie przywróci najważniejsze usługi. Odpowiedzi odsłaniają zarazem bariery organizacyjne, kompetencyjne i finansowe, które wpływają na tempo dalszego rozwoju.





10

Co spowalnia kolejny krok i co jest potrzebne do rozwoju?

10

Co spowalnia kolejny krok i co jest potrzebne do rozwoju?

Rozwój cyfrowy nie zależy wyłącznie od liczby wdrożonych systemów. Nawet przy rozwiniętej infrastrukturze i zabezpieczeniach tempo zmian mogą ograniczać prawo, kompetencje, jakość danych, możliwości integracji i koszty. Rozpoznanie tych uwarunkowań pozwala lepiej dobrać kolejny krok.

Prawo i odpowiedzialność

+

Kompetencje

+

Integracja i jakość danych

+

Poufność i bezpieczeństwo

+

Koszty i możliwość utrzymania rozwiązania



Bariery ograniczające tempo zmian

Pięć barier, które ograniczają tempo zmian

Badanie pokazuje, że ograniczenia cyfryzacji nie sprowadzają się do budżetu. W różnych obszarach powracają kwestie prawa, kompetencji, integracji, poufności danych i kosztów. Zestawienie ma charakter przekrojowy: bariery wskazywano w odniesieniu do różnych technologii, a poszczególne pytania kierowano do instytucji, które nie korzystały z danego rozwiązania. Nie należy go więc traktować jako rankingu, lecz jako mapę powtarzających się typów ograniczeń.

Bariery ograniczające tempo zmian

01

Prawo i odpowiedzialność – niepewność dotycząca zasad wykorzystania nowych technologii utrudnia podejmowanie decyzji, szczególnie w obszarach związanych ze sztuczną inteligencją, danymi użytkowników i automatyzacją działań.

02

Kompetencje – instytucja potrzebuje nie tylko specjalistów technicznych, lecz także pracowników, którzy potrafią opisać proces, ocenić jakość danych, korzystać z rozwiązania i rozpoznać ryzyko.

03

Integracja i jakość danych – nowe narzędzie nie usprawni pracy, jeżeli informacje pozostają rozproszone, są wielokrotnie wprowadzane albo nie można ich bezpiecznie przekazać między systemami.

04

Poufność i bezpieczeństwo – obawy dotyczące ochrony danych mogą spowalniać wykorzystanie chmury, usług zewnętrznych i sztucznej inteligencji. Praktyczną odpowiedzią są jasny podział odpowiedzialności, kontrola dostępu i ocena ryzyka.

05

Koszty i możliwość utrzymania rozwiązania – znaczenie ma nie tylko wydatek początkowy, lecz także integracja, szkolenia, wsparcie, bezpieczeństwo i późniejsze utrzymanie. Oceniając koszt, warto uwzględnić również oczekiwany efekt oraz ryzyko związane z pozostawieniem procesu bez zmian.

Cztery elementy gotowości do dalszego rozwoju

1 Stabilne fundamenty i ciągłość działania

Pierwszym elementem gotowości jest infrastruktura zdolna utrzymać działanie usług. Powszechny dostęp do internetu i wysoki udział szybkich łączy tworzą dobrą bazę, lecz o ciągłości decydują również gwarantowane parametry, rozwiązania zapasowe, regularnie wykonywane i testowane kopie danych oraz procedury odtworzenia na wypadek awarii.

Zakres tej gotowości zależy od punktu wyjścia instytucji. W jednych jednostkach luką pozostają podstawowe zabezpieczenia i łącza zapasowe, w innych — zależności między rosnącą liczbą usług, urządzeń i danych, które mogą tworzyć nowe pojedyncze punkty awarii.

2 Proces cyfrowy od początku do końca

Drugim elementem jest ciągłość procesu. Elektroniczny obieg dokumentów działa w większości badanych jednostek, lecz zakres gotowości pokazuje dopiero połączenie kanału dostępnego dla użytkownika z wewnętrzną obsługą, systemami dziedzinowymi, akceptacją, podpisem i archiwizacją.

Sygnałem braku gotowości są opóźnienia, wielokrotne wprowadzanie tych samych danych oraz konieczność przechodzenia między papierem, pocztą elektroniczną i kilkoma systemami. To właśnie w tych miejscach ujawnia się luka między obecnością narzędzi a rzeczywiście cyfrowym procesem.

10.2 **Cztery elementy gotowości do dalszego rozwoju**

3 Dane, które prowadzą do decyzji i działania

Kolejnym elementem jest gotowość danych. Internet rzeczy jest obecny w znacznej części badanej grupy, a sztuczna inteligencja najczęściej wspiera pojedyncze zadania związane z tekstem i mową. Szersze wykorzystanie staje się możliwe, gdy dane są uporządkowane, możliwe do połączenia i osadzone w konkretnym procesie decyzyjnym.

Gotowość można rozpoznać po tym, czy instytucja potrafi wskazać problem, osobę lub zespół odpowiedzialny za reakcję i miernik rezultatu. Bez tych ustaleń technologia zwiększa liczbę danych i alertów, ale nie tworzy pewnego związku między informacją a poprawą jakości usług lub pracy instytucji.

4 Kompetencje, odpowiedzialność i zasady korzystania z technologii

Czwarty element ma charakter organizacyjny. Gotowość wymaga jasnego wskazania osób lub zespołów odpowiedzialnych za utrzymanie systemu, przebieg procesu i osiągane rezultaty. Ważne są również kompetencje pracowników, czytelny podział ról, właściwe zarządzanie uprawnieniami oraz zasady dotyczące bezpieczeństwa, jakości danych i wykorzystania sztucznej inteligencji.

Nawet dobrze dobrana technologia nie zmieni sposobu działania instytucji, jeśli nikt nie odpowiada za przeprowadzenie zmiany od diagnozy do oceny rezultatów. Potrzebna jest osoba lub zespół, który połączy perspektywę użytkowników, pracowników i technologii, ustali priorytety oraz zadba o współpracę między jednostkami. Nie musi to oznaczać tworzenia nowego stanowiska. Kluczowe są wyraźny mandat do działania i możliwość podejmowania decyzji.

O gotowości świadczy również przygotowanie użytkowników i faktyczne wejście rozwiązania do codziennej pracy. Technicznie poprawne uruchomienie nie daje trwałej zmiany, jeżeli pracownicy omijają system, korzystają tylko z części jego możliwości albo nie wiedzą, kto odpowiada za efekt.

Tak rozumiana gotowość domyka diagnozę: pokazuje nie tylko, czego brakuje, lecz także w którym miejscu instytucja może rozpocząć zmianę możliwą do wdrożenia i oceny w praktyce.

Case study

Transformacja cyfrowa gminy Grodzisk Wielkopolski

Współpraca gminy Grodzisk Wielkopolski z INEA rozpoczęła się w 2013 roku od rozwoju usług telekomunikacyjnych dla jednostek samorządowych, w tym placówek oświatowych i kulturalnych. Zapewnienie stabilnej łączności oraz transmisji danych pomiędzy jednostkami stworzyło fundament do dalszej cyfryzacji gminy.

W kolejnych latach współpraca była rozwijana etapami. Połączenie jednostek gminnych w jedną sieć umożliwiło korzystanie z kolejnych rozwiązań cyfrowych, takich jak telefonia IP, elektroniczny obieg dokumentów czy monitoring miejski. Równolegle rozwijano dostęp mieszkańców do internetu, między innymi poprzez hotspoty w przestrzeni publicznej i działania ograniczające występowanie białych plam.

Projekt pokazuje, że transformacja samorządu nie musi oznaczać jednego dużego wdrożenia. Może rozwijać się krok po kroku, wraz z potrzebami instytucji i mieszkańców – od zapewnienia niezawodnej łączności, przez cyfryzację procesów, po rozwiązania wspierające dostępność usług i bezpieczeństwo przestrzeni publicznej.

„Współpraca ta pokazała, że przy wspólnej wizji i elastycznym podejściu można wdrożyć nowoczesne rozwiązania nawet w środowisku, które wcześniej było analogowe. Wspólnym wysiłkiem zbudowano podstawy cyfrowej transformacji całej lokalnej administracji”.

Artur Judek
Naczelnik Wydziału Informatyzacji i Cyfryzacji Urzędu Miejskiego w Grodzisku Wielkopolskim

KOMENTARZ INEA

Najważniejszą lekcją z Grodziska Wielkopolskiego jest etapowość transformacji. Infrastruktura była punktem wyjścia, ale kolejne rozwiązania pojawiały się wraz z konkretnymi potrzebami gminy i jej mieszkańców. Takie podejście pozwala ograniczać ryzyko, utrzymywać spójność środowiska technologicznego i rozwijać te obszary, w których zmiana przynosi rzeczywistą wartość.



Agnieszka Ciemniejewska
B2P Director INEA



11

Od diagnozy do działania

11

Od diagnozy
do działania

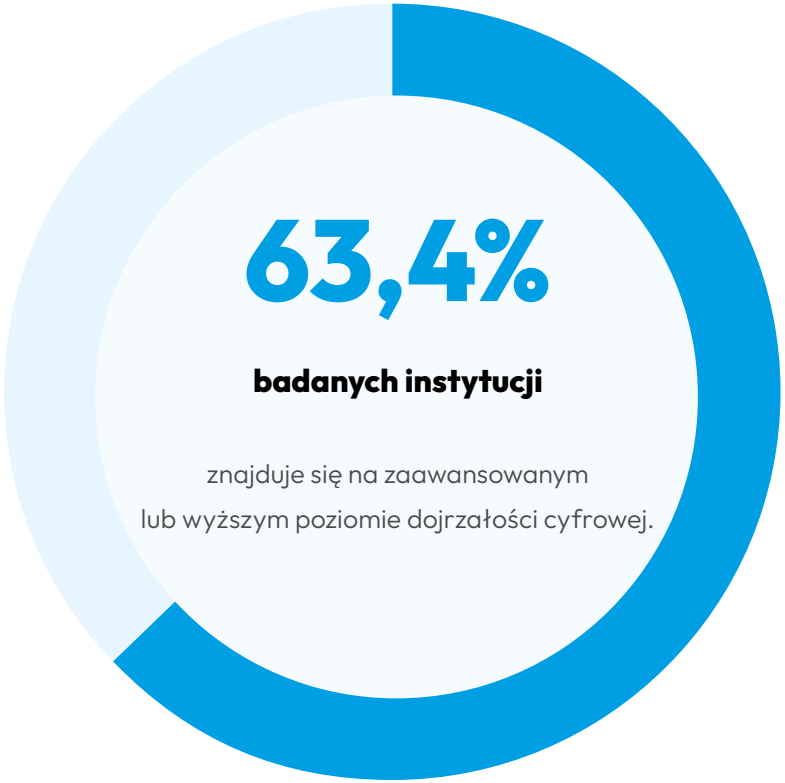
Końcowa część raportu przekłada wyniki na wybór działania. Cyfrowa transformacja rzadko wymaga rozpoczęcia od zera: większość badanych instytucji ma już rozwiniętą łączność, podstawowe zabezpieczenia i narzędzia wspierające pracę. Decyzja dotyczy więc takiego zakresu zmiany, który odpowiada punktowi wyjścia, rozwiązuje konkretny problem i daje efekt możliwy do sprawdzenia.

14,6%

poziom zaawansowany

48,8%

Lider Cyfrowej Transformacji



W badanej grupie 48,8% instytucji osiągnęło poziom Lidera Cyfrowej Transformacji, a kolejne 14,6% – poziom zaawansowany. Do grupy średniozaawansowanej należy 35,4% badanych, natomiast poziom podstawowy reprezentuje 1,2%. Wynik odzwierciedla profil próby, w której znalazły się instytucje już aktywnie rozwijające rozwiązania cyfrowe. Nie oznacza jednak, że wszystkie elementy ich środowiska technologicznego są równie rozwinięte.

spójność procesów → **dostępność danych** → **ciągłość działania**

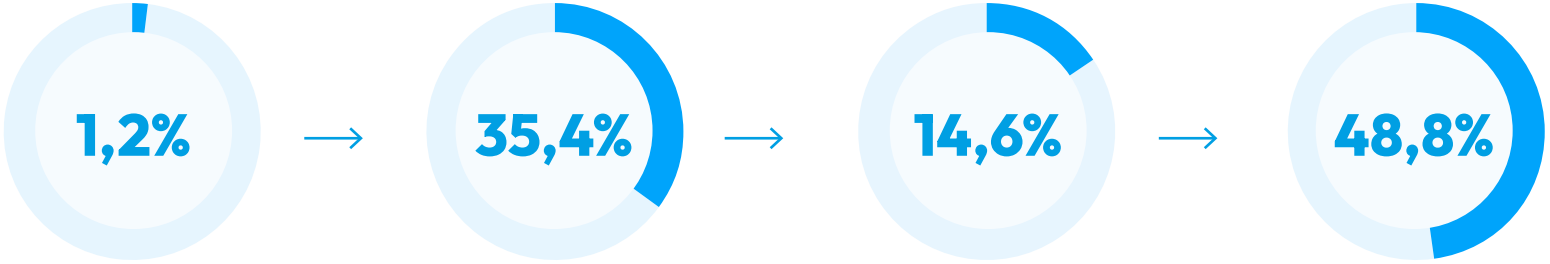
11.1 **Cztery punkty wyjścia, cztery kolejne kroki**

Cztery punkty wyjścia, cztery kolejne kroki

Cyfrowa dojrzałość nie sprowadza się do liczby posiadanych systemów. O pozycji instytucji decyduje również to, czy technologie wspierają cały przebieg sprawy, czy dane są dostępne tam, gdzie są potrzebne, oraz czy organizacja potrafi utrzymać działanie usług w sytuacji awarii lub cyberataku.

Dojrzałość cyfrowa nie wyznacza jednej obowiązkowej ścieżki rozwoju.

Pokazuje raczej, z jakiego miejsca instytucja rozpoczyna kolejną zmianę i na jakiego rodzaju działania jest obecnie najlepiej przygotowana.



Poziom podstawowy

Najważniejszy cel:
zapewnić podstawowe warunki cyfrowego działania.

Poziom średniozaawansowany

Najważniejszy cel:
ograniczyć rozproszenie procesów i informacji.

Poziom zaawansowany

Najważniejszy cel:
wykorzystać technologię do usprawnienia konkretnych zadań.

Lider Cyfrowej Transformacji

Najważniejszy cel:
ocenić jakość cyfrowych procesów i pełniej wykorzystać istniejące rozwiązania.

11.1 Cztery punkty wyjścia, cztery kolejne kroki

01

Poziom podstawowy



Najważniejszy cel: **zapewnić podstawowe warunki cyfrowego działania.**



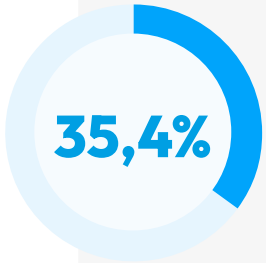
W tej grupie kolejny krok powinien dotyczyć obszarów niezbędnych do codziennego funkcjonowania: stabilnego dostępu do sieci, bezpiecznego przechowywania informacji i ograniczenia procesów wykonywanych wyłącznie ręcznie. Punktem wyjścia nie musi być kompleksowy program cyfryzacji. Większą wartość może przynieść rozwiązanie jednego konkretnego problemu, który regularnie utrudnia pracę lub dostęp do usług.

Kolejny krok

Instytucja powinna wskazać proces możliwy do uporządkowania w stosunkowo krótkim czasie, określić osobę odpowiedzialną za zmianę i ustalić podstawowy miernik jej powodzenia. Może nim być skrócenie czasu obsługi, łatwiejszy dostęp do dokumentów albo ograniczenie liczby błędów.

02

Poziom średniozaawansowany



Najważniejszy cel: **ograniczyć rozproszenie procesów i informacji.**



Na tym poziomie technologie są już obecne w wielu obszarach, lecz nie zawsze współpracują ze sobą. Część spraw może być inicjowana elektronicznie, a następnie obsługiwana ręcznie. Dane bywają przechowywane w odrębnych systemach, co wymusza ich ponowne wprowadzanie i utrudnia uzyskanie pełnego obrazu procesu.

Kolejny krok

Przed kolejną inwestycją warto prześledzić drogę wybranej sprawy od momentu kontaktu użytkownika z instytucją do jej zakończenia. Taka analiza pozwoli wskazać miejsca, w których proces traci ciągłość. Następnym krokiem może być połączenie dwóch kluczowych systemów, uporządkowanie obiegu informacji albo rozszerzenie jednej usługi tak, aby większa część obsługi odbywała się cyfrowo.

11.1 Cztery punkty wyjścia, cztery kolejne kroki

03



Poziom zaawansowany


analityka


automatyzacja


internet rzeczy



sztuczna inteligencja

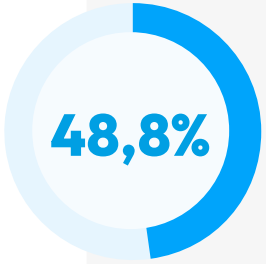
Najważniejszy cel: **wykorzystać technologię do usprawnienia konkretnych zadań.**

Instytucje zaawansowane mają warunki, aby szerzej korzystać z automatyzacji, analityki, internetu rzeczy i sztucznej inteligencji. **Z rozwiązań IoT korzysta już 46,3%** całej badanej grupy, między innymi w monitorowaniu infrastruktury, zarządzaniu zasobami i bezpieczeństwie. Potencjał tych technologii zależy jednak od jakości danych oraz od tego, czy ich zastosowanie odpowiada na jasno nazwany problem.

Kolejny krok

Zamiast rozpoczynać szerokie wdrożenie, warto wybrać proces, w którym efekt można szybko sprawdzić. Pilotaż powinien mieć określony zakres, właściciela i miernik rezultatu. Dopiero po ocenie użyteczności rozwiązania, bezpieczeństwa danych oraz kosztów jego utrzymania można podjąć decyzję o rozszerzeniu zastosowania.

04



Lider Cyfrowej Transformacji


mierzenie rezultatów


wzmocnienie odporności


bezpieczne eksperymentowanie

Najważniejszy cel: **ocenić jakość cyfrowych procesów i pełniej wykorzystać istniejące rozwiązania.**

Wysoki wynik w modelu pokazuje szeroki zakres wykorzystania technologii, ale nie przesądza jeszcze o jakości cyfrowych procesów ani efektach poszczególnych wdrożeń. Dla liderów kolejnym krokiem powinna być więc ocena, czy wykorzystywane rozwiązania tworzą spójne środowisko, rzeczywiście poprawiają dostępność usług i usprawniają pracę oraz nie wprowadzają zbędnej złożoności.

Wniosek

Kolejnym kierunkiem powinno być systematyczne mierzenie rezultatów, wzmacnianie odporności i tworzenie warunków do bezpiecznego eksperymentowania. Nowe rozwiązania warto oceniać nie na podstawie ich innowacyjności, lecz wpływu na jakość obsługi, dostępność informacji, ciągłość działania i zdolność instytucji do reagowania na zmieniające się potrzeby.

Sześć kroków od potrzeby do mierzalnego rezultatu



Wyniki badania pokazują, że największe wyzwania pojawiają się nie przy samym dostępie do technologii, lecz na etapie ich łączenia, wykorzystywania danych i przekładania wdrożeń na mierzalne rezultaty. Dlatego transformację warto prowadzić według sześciu zasad.

Sześć kroków

01 → **Określ cel**
co ma działać lepiej

02 → **Zdiagnozuj potrzeby i proces**

03 → **Wybierz priorytet**

04 → **Sprawdź fundamenty i bezpieczeństwo**

05 → **Przetestuj rozwiązanie**

06 **Zmierz efekt i zdecyduj o skali**

11.2 **Sześć kroków od potrzeby do mierzalnego rezultatu**

01 Nazwij cel

Określ zmianę, którą instytucja chce osiągnąć: krótszy czas realizacji sprawy, większą dostępność usługi, mniej błędów, lepszą informację albo wyższą odporność działania.

02 Zdiagnozuj obecny sposób pracy

Prześledź proces, przepływ danych, wykorzystywane narzędzia i role pracowników. Wskaż ręczne czynności, przestoje, brak aktualnej informacji i miejsca, w których użytkownik napotyka trudności.

03 Wybierz jeden priorytet

Nie wszystkie luki trzeba zamykać równocześnie. Pierwszeństwo powinien otrzymać problem o największym znaczeniu dla użytkowników, działania instytucji, bezpieczeństwa lub możliwości dalszego rozwoju.

04 Sprawdź fundamenty

Oceń jakość danych, łączność i infrastrukturę, możliwość integracji, zabezpieczenia, wymagania prawne oraz kompetencje zespołu. Ustal odpowiedzialność za proces, wdrożenie i późniejsze utrzymanie rozwiązania.

05 Przetestuj rozwiązanie w ograniczonej skali

Pilotaż powinien obejmować konkretny proces, odpowiedzialną osobę, grupę użytkowników oraz warunki powodzenia. Pozwala sprawdzić rozwiązanie w praktyce, przygotować użytkowników i ograniczyć koszt błędnej decyzji.

06 Zmierz efekt i zdecyduj, co dalej

Jeszcze przed rozpoczęciem pilotażu ustal wskaźnik poprawy – na przykład czas realizacji sprawy, liczbę błędów, dostępność usługi, czas odtworzenia danych albo satysfakcję użytkownika. Wynik powinien przesądzać o rozszerzeniu, zmianie lub zakończeniu wdrożenia.

Wsparcie dopasowane do zakresu zmiany

Zmiana może łączyć łączność, chmurę, bezpieczeństwo, integrację systemów i nowy sposób pracy. Dlatego wsparcie warto projektować tak, aby uwzględniało cały proces, wymagania instytucji oraz zależności między rozwiązaniami, a nie tylko wybór pojedynczego narzędzia.

Przy ocenie wsparcia warto sprawdzić, czy obejmuje ono diagnozę, projekt rozwiązania, integrację, bezpieczeństwo i pomoc po uruchomieniu.



Spójny zakres odpowiedzialności ułatwia później ocenę efektów oraz rozwój wdrożenia.

01 **DIAGNOZA** | rozpoznanie potrzeb i obecnej sytuacji

02 **PROJEKT ROZWIĄZANIA** | dopasowanie technologii do wymagań instytucji

03 **INTEGRACJA** | połączenie rozwiązań i procesów

04 **BEZPIECZEŃSTWO** | ochrona danych i ciągłość działania

05 **WSPARCIE PO URUCHOMIENIU** | pomoc w działaniu i dalszym rozwoju

Cel badania

Badanie zostało przeprowadzone w celu rozpoznania sposobu wykorzystania technologii cyfrowych przez podmioty publiczne oraz określenia ich punktu wyjścia do dalszej cyfryzacji. Narzędzie miało wspierać diagnozę obszarów rozwiniętych, luk technologicznych i możliwych kierunków dalszych działań.

DIAGNOZA → **PUNKT WYJŚCIA** → **DALSZY ROZWÓJ**

Badanie nie służyło stworzeniu rankingu instytucji ani ocenie jakości realizowanych przez nie zadań publicznych. Przyjęty model porządkuje zakres wykorzystania wybranych technologii i wspiera rozmowę o kolejnych etapach rozwoju cyfrowego.

12.2 **Badana grupa**

Badana grupa

Badanie przeprowadzono od 17 lipca 2025 r. do 6 lipca 2026 r. W systemie zarejestrowano 99 respondentów, z których 82 wypełniło ankietę w całości. Do analizy włączono wszystkie 82 kompletne ankiety. Jedna obserwacja odpowiadała jednej instytucji.

99	82	82	0
zarejestrowanych respondentów	kompletne ankiety 82,8% wszystkich rejestracji	instytucje w analizie	ankiet wykluczonych

1 odpowiedź = 1 instytucja

Jedna odpowiedź mogła obejmować również jednostki organizacyjne, jeśli prowadziły wspólną politykę cyfryzacji i były objęte wspólnym zarządzaniem rozwiązaniami cyfrowymi.

Jakie instytucje znalazły się w badaniu?

- administracja publiczna
- edukacja
- ochrona zdrowia
- kultura
- gospodarka wodna i odpadowa
- zarządzanie nieruchomościami

Struktura badanej grupy według zatrudnienia

1	mniej niż 10 osób
35	od 10 do 49 osób
41	od 50 do 249 osób
5	co najmniej 250 osób

Badanie objęło instytucje pozostające w kontakcie z INEA, dlatego badana grupa może być bardziej zaawansowana technologicznie niż ogół instytucji.

Ze względu na niewielką liczebność grup <10 osób (n=1) oraz ≥250 osób (n=5) nie powinny one stanowić samodzielnej podstawy do wnioskowania o całych segmentach instytucji publicznych.

Kontrola danych

Ankieta wykorzystywała numer REGON do ograniczania duplikacji, a kontrola danych nie wykazała powtórzeń numerów NIP. W analizowanej próbie nie zidentyfikowano więc przypadku dwukrotnego ujęcia tego samego podmiotu.

Grupa została dobrana celowo i nielosowo. Wyników nie należy uogólniać na wszystkie podmioty publiczne w Polsce.

Realizacja badania
i charakter odpowiedzi

Respondentów zapraszano do udziału mailowo lub telefonicznie. Kwestionariusz miał postać standaryzowanego formularza elektronicznego i obejmował 34 pytania. Można go było wypełnić samodzielnie albo z udziałem doradcy INEA – podczas spotkania online, rozmowy telefonicznej lub spotkania bezpośredniego. Niezależnie od trybu wykorzystywano ten sam formularz i tę samą logikę pytań.

Kto wypełnił ankietę?

Ankietę wypełniały osoby posiadające wiedzę o technologiach i procesach wykorzystywanych w organizacji, m.in.

- przedstawiciele kierownictwa
- dyrektorzy jednostek
- osoby odpowiedzialne za informatykę i cyfryzację
- informatycy

Jeżeli odpowiedź przygotowywało kilka osób, ostateczną wersję zatwierdzał główny respondent reprezentujący instytucję.

34 pytania

formularz elektroniczny

1 logika pytań niezależnie od trybu realizacji

Sposób realizacji badania



Odpowiedzi mają charakter deklaratywny

Formularz kontrolował kompletność i logiczną spójność odpowiedzi, a numer REGON ograniczał ryzyko duplikacji. Kontrole nie oznaczały jednak merytorycznego potwierdzania deklaracji. **Odpowiedzi nie były niezależnie weryfikowane i należy je traktować jako samoocenę respondentów.**

12.4 **Zakres badania**

Zakres diagnozy

Kwestionariusz obejmował trzy szerokie obszary:

01 **Technologie** wspierające procesy i tworzenie wartości;

02 **Infrastruktura** teleinformatyczną;

03 **Bezpieczeństwo** cyfrowe.

Podział pozwala rozróżnić technologie bezpośrednio zmieniające sposób realizacji procesów od infrastruktury i zabezpieczeń niezbędnych do ich stabilnego oraz bezpiecznego działania.



Technologie wspierające procesy i tworzenie wartości – rozwiązania wykorzystywane bezpośrednio w funkcjonowaniu instytucji, cyfrowej obsłudze spraw, komunikacji oraz automatyzacji.



obsługa spraw



komunikacja z interesariuszami



automatyzacja procesów



rozwiązania chmurowe



wymiana danych



analiza i wykorzystanie danych

Warunki bezpiecznego i stabilnego korzystania z technologii infrastruktura + bezpieczeństwo cyfrowe

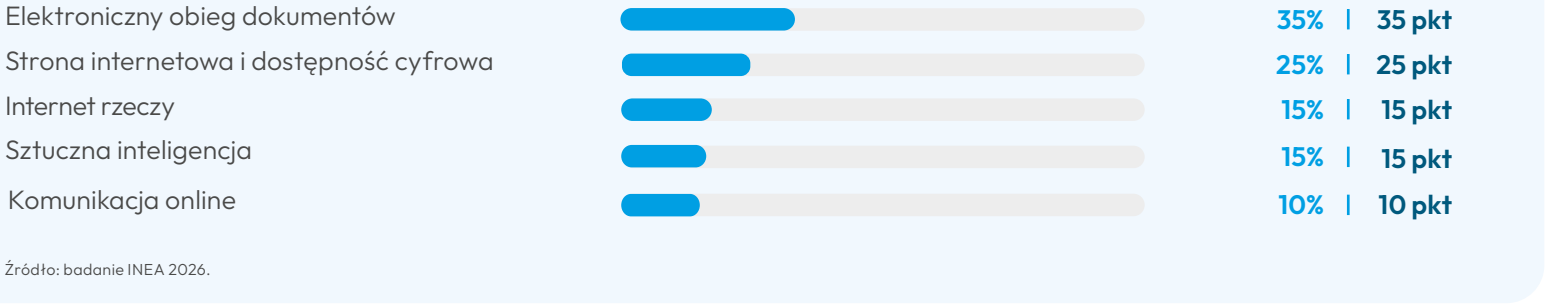
Infrastruktura teleinformatyczna – dostęp do internetu, parametry łączy, mobilność oraz korzystanie z usług chmurowych.

Bezpieczeństwo cyfrowe – stosowane zabezpieczenia, doświadczenia związane z utratą danych, kopie zapasowe i działania rozwijające kompetencje pracowników.

12.5 **Model oceny dojrzałości cyfrowej**

Model oceny dojrzałości cyfrowej

Poziom cyfryzacji został obliczony na podstawie odpowiedzi dotyczących pięciu grup technologii:



Źródło: badanie INEA 2026.

100 pkt
maksymalny wynik

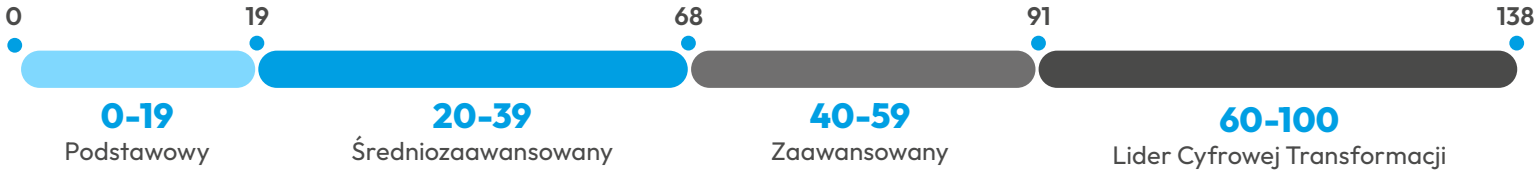
Największą wagę przypisano elektronicznemu obiegowi dokumentów, ponieważ rozwiązanie to może wpływać na organizację pracy, przepływ informacji i sposób obsługi spraw. Strona internetowa i jej dostępność odzwierciedlają możliwość korzystania z informacji i usług cyfrowych przez odbiorców instytucji. Komunikacja online pokazuje zakres wykorzystywania kanałów kontaktu, natomiast internet rzeczy i sztuczna inteligencja reprezentują bardziej zaawansowane zastosowania technologii.

Sposób przyznawania punktów zależał od charakteru danego obszaru i pytania. Uwzględniano m.in. sam fakt wykorzystania rozwiązania, zakres wykorzystania technologii, a w wybranych przypadkach także stopień integracji z innymi rozwiązaniami lub procesami oraz osiągane efekty. Wyższy wynik mógł zatem wynikać zarówno z wykorzystywania większej liczby technologii, jak i z szerszego lub bardziej zaawansowanego sposobu ich zastosowania. Dobór obszarów, punktacja oraz ich wagi zostały opracowane przez ekspertów INEA na podstawie doświadczenia we współpracy z organizacjami i wiedzy dotyczącej roli poszczególnych technologii w transformacji cyfrowej. Wagi nie wynikają z modelowania statystycznego ani z zewnętrznego standardu certyfikacyjnego. Stanowią element autorskiego modelu diagnostycznego INEA.

12.5 **Model oceny dojrzałości cyfrowej**

Poziomy dojrzałości

Na podstawie sumy uzyskanych punktów instytucje zaklasyfikowano do czterech poziomów:



Granice poziomów

Progi zostały ustalone ekspercko przez INEA i nie stanowią równomiernego podziału skali. Odzwierciedlają kolejne etapy rozwoju cyfrowego organizacji: przejście na wyższy poziom wiąże się z wykorzystaniem szerszego lub bardziej zaawansowanego zestawu rozwiązań objętych modelem.

Granice służą uporządkowaniu różnych punktów wyjścia i dopasowaniu możliwych kierunków rozwoju; nie należy ich interpretować jako uniwersalnej normy obowiązującej wszystkie instytucje publiczne.

Co pokazuje wynik?

Wynik pokazuje zakres wykorzystania technologii objętych modelem. Nie mierzy bezpośrednio jakości usług publicznych, efektywności instytucji, satysfakcji mieszkańców ani ekonomicznych efektów wdrożeń.

Dotyczy to również udziału instytucji zaklasyfikowanych jako liderzy cyfrowej transformacji. Wynik opisuje celowo dobraną grupę, obejmującą wielu wieloletnich klientów INEA, i nie powinien być przedstawiany jako udział liderów w całym sektorze publicznym.

B2P ≠B2B

Model B2P został zbudowany inaczej niż model B2B: obejmuje inne obszary, wagi i progi. Z tego względu wartości indeksu oraz rozkłady poziomów dojrzałości w obu raportach nie są bezpośrednio porównywalne. W szczególności udziału liderów w badanej grupie instytucji nie należy zestawiać z udziałem liderów wśród przedsiębiorstw.

Rola infrastruktury i bezpieczeństwa

Dostęp do internetu, parametry łączy, usługi chmurowe oraz cyberbezpieczeństwo zostały objęte badaniem, ale nie zwiększały bezpośrednio liczby punktów decydujących o poziomie dojrzałości.

Przyjęto, że są one warunkiem stabilnego, skalowalnego i bezpiecznego korzystania z technologii, lecz samo posiadanie infrastruktury lub zabezpieczeń nie przesądza jeszcze o cyfrowej transformacji procesów.



Dotyczy to także chmury:

samo miejsce przetwarzania lub przechowywania danych – lokalnie albo w chmurze – jest decyzją technologiczną i organizacyjną, zależną m.in. od potrzeb, bezpieczeństwa, kosztów i użyteczności rozwiązania.

Jak czytać wyniki?

W badaniu B2P nie pytano o wykorzystanie konkretnych systemów i aplikacji w modelu chmurowym, dlatego chmura nie mogła stanowić odrębnego elementu punktacji.

Wyniki dotyczące infrastruktury, chmury i bezpieczeństwa są analizowane w raporcie jako uzupełnienie właściwego modelu dojrzałości.

Benchmarki zewnętrzne

W wybranych miejscach wyniki badania zestawiono z danymi GUS lub Eurostatu. Porównania wykorzystano jedynie wtedy, gdy dostępne wskaźniki odnosiły się do podobnych technologii i grup podmiotów.

Benchmarki należy traktować jako kontekst, a nie bezpośrednią miarę pozycji badanej grupy. Różnice mogą wynikać m.in. z:

01
odmiennego sposobu doboru próby

02
różnych terminów realizacji badań

03
innego brzmienia pytań

04
różnic w definicjach technologii;

05
odmiennych podstaw procentowania odpowiedzi

W przypadku braku wystarczającej porównywalności dane zewnętrzne nie powinny być wykorzystywane do formułowania wniosków o przewadze lub zapóźnieniu badanych instytucji.

Zasady interpretacji

Wyniki opisują wykorzystanie technologii w momencie realizacji badania. Nie pozwalają samodzielnie ocenić jakości wdrożeń, stopnia integracji systemów ani efektów osiąganych przez konkretną instytucję.

- stan w momencie badania
- wyniki badanej grupy
- bez oceny jakości wdrożeń

Wyniki pytań wielokrotnego wyboru nie sumują się do 100%.

Odpowiedzi dotyczące kilku możliwych zastosowań technologii były pytaniami wielokrotnego wyboru, dlatego możliwe było wskazanie więcej niż jednej odpowiedzi.

Wszystkie wnioski odnoszą się do badanej grupy.

O raporcie

INEA to ogólnopolski dostawca nowoczesnych usług telekomunikacyjnych dla klientów indywidualnych, biznesowych oraz sektora publicznego. Oferuje szybki Internet światłowodowy, telefonię, telewizję, usługi data center, dedykowane łącza oraz rozwiązania chmurowe. INEA zapewnia niezawodność, elastyczność i profesjonalne wsparcie, dostosowane do potrzeb firm każdej wielkości. Dzięki innowacyjnym technologiom wspiera rozwój biznesu i cyfrową transformację przedsiębiorstw.

Redakcja i skład:

2026 INEA.
Wszystkie prawa zastrzeżone.

Koncepcja i metodologia badania:

INEA

Opracowanie redakcyjne, projekt graficzny i skład:
Open Format

Przy cytowaniu danych prosimy podawać źródło:
„Wyniki pierwszej fali badania poziomu cyfryzacji przez INEA”.
Część zdjęć użytych w raporcie została wygenerowana przez AI.

RAPORT



Biznes wymaga dobrego połączenia

biznes.inea.pl