Allegato A alla DGR ……del……

REGIONE CALABRIA

# *Piano Strategico di Cybersecurity 2024 – 2027*

# Indice

# Indice delle Tabelle

# Indice delle Figure

# 1. Introduzione

Nel corso degli ultimi anni, con l'imponente processo di digitalizzazione, la sicurezza informatica sta progressivamente assumendo un ruolo fortemente strategico, diventando una priorità per le organizzazioni pubbliche e private.

La rapida evoluzione tecnologica e i processi di digitalizzazione, seppur offrono nuove opportunità, hanno anche comportato un'evoluzione del panorama delle minacce informatiche ed una sofisticazione degli attacchi informatici, sempre più frequenti ed articolati.

In questo contesto, risulta quanto mai fondamentale un rinnovato approccio alla *cybersecurity* che includa l'adozione di misure di prevenzione, di protezione e di mitigazione del rischio *cyber*.

Le prime politiche italiane in ambito *cybersecurity* sono state sviluppate già a partire dagli anni Novanta e si focalizzavano, per lo più, sul contrasto ai crimini informatici.

Nel tempo vi sono stati numerosi sviluppi, anche a livello normativo, fino alla creazione di un'Agenzia per la *Cyber*sicurezza Nazionale, istituita dal Decreto-legge n. 82 del 14 giugno 2021, e alla recente pubblicazione della Strategia Nazionale di *Cyber*sicurezza 2022 – 2026. Quest'ultima riconosce la sicurezza informatica quale fondamento del processo di digitalizzazione del Paese.

La Strategia, inoltre, mira al potenziamento del livello di maturità delle capacità *cyber* nazionali al fine di alimentare un continuo impulso all'innovazione tecnologica e alla digitalizzazione della Pubblica Amministrazione e del tessuto produttivo del Paese, assicurando una costante rispondenza ai principi di *cyber*sicurezza.

## 1.1 Contesto

Il profondo processo di trasformazione digitale avviato dalla Regione Calabria, avente la finalità di portare innovazione nei servizi forniti ai cittadini, ha richiesto una maggior attenzione alle tematiche inerenti alla sicurezza informatica e alla protezione dei dati personali.

Da tempo la Regione Calabria ha intrapreso un percorso di crescita ed evoluzione in termini di digitalizzazione dei servizi regionali. Uno dei principali strumenti di attuazione per la crescita digitale della Regione è stato il "Programma Operativo Regionale (POR) Calabria FESR FSE 2014-2020". Successivamente, con la Deliberazione n. 532 del 10 novembre 2017, la Giunta Regionale ha approvato le "Linee Guida per la Crescita Digitale 2020", documento di rilevanza strategica che accoglie gli indirizzi del primo Piano Triennale per l'Informatica nella PA 2017-2019 pubblicato da AgID. Infine, la Regione con Deliberazione n. 413 del 01 settembre 2022, ha approvato le "Linee Guida per la Crescita Digitale della Regione Calabria 2022 – 2025", le cui attività di indirizzo strategico si innestano su un'architettura ben delineata a livello internazionale con l'Agenda 2030 per lo Sviluppo Sostenibile, a livello europeo tramite l'Agenda Digitale Europea e Politiche di Coesione 2021 – 2027, a livello nazionale attraverso, ad esempio, l'Agenda Digitale Italiana, il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2021 – 2023, il Piano Nazionale di Ripresa e Resilienza (PNRR) e a livello regionale con il PR 2021 – 2027, PAC 2021 – 2027, DISR e S3.

Le “Linee Guida per la Crescita Digitale della Regione Calabria 2022 – 2025” delineano una strategia complessiva di crescita digitale per il periodo di riferimento che si basa su 4 Linee Strategiche di intervento. Lo scopo è perseguire la crescita digitale in un’ottica di sistema, superando la visione compartimentale per adottare, piuttosto, un approccio unitario che includa anche la gestione delle tematiche legate alla *cyber*sicurezza.

In tale contesto, la Regione Calabria ha elaborato il presente Piano Strategico in ambito *cybersecurity* quale strumento essenziale per il rafforzamento della resilienza *cyber* dei servizi digitali. Il Piano Strategico di *cybersecurity* 2024 – 2027 affonda le sue radici nei seguenti elementi:

- il contesto regionale in tema di Agenda Digitale;
- i risultati raggiunti in passato e/o le azioni intraprese, che rappresentano i fondamenti sui quali è stato costruito il Piano Strategico;
- le aspirazioni future della Regione Calabria per la sicurezza e la resilienza dei sistemi e dei servizi regionali.

Il presente Piano Strategico si propone di:

- delineare la direzione strategica in ambito *cybersecurity* della Regione Calabria;
- individuare le linee di indirizzo per la definizione e l’implementazione degli interventi da attuare nel breve, medio e lungo termine per il potenziamento delle capacità *cyber* dell’Ente;
- contribuire al raggiungimento degli obiettivi delle “Linee Guida per la Crescita Digitale della Regione Calabria 2022 – 2025”, per assicurare una transizione digitale *cyber* resiliente.

## 1.2 Ruoli e Responsabilità

Una chiara definizione di ruoli e responsabilità è cruciale al fine di garantire l'attuazione ed il monitoraggio del Piano Strategico.

| Ruolo | Responsabilità |
|---|---|
| Giunta Regionale | Approvare il Piano Strategico di *cybersecurity* della Regione Calabria (Strategia di *Cybersicurezza* Regionale). |
| Responsabile per la Transizione Digitale (RTD) | • Sviluppare il Piano Strategico in ambito *cybersecurity* della Regione Calabria stabilendo obiettivi ed individuando le line di indirizzo per il medio-lungo termine per rafforzare le capacità *cyber* dell'Ente;<br>• approvare il piano di attuazione elaborato dai Settori del Dipartimento Transizione Digitale e Attività Strategiche in coerenza con il Piano Strategico<br>• svolgere una funzione di coordinamento dei Dipartimenti Regionali per la successiva attuazione del Piano Strategico favorendo collaborazione, cooperazione e coordinamento in linea con gli indirizzi del Piano Strategico;<br>• monitorare l'andamento della attuazione del Piano Strategico;<br>• eseguire una valutazione dei rischi sull'effettiva attuazione del Piano Strategico;<br>• approvare eventuali azioni correttive e/o strategie di mitigazione dei rischi identificati;<br>• revisionare ed aggiornare periodicamente il Piano Strategico in base ai risultati del processo di monitoraggio sullo stato di attuazione e ad eventuali cambiamenti del contesto interno ed esterno (ulteriori dettagli sono forniti nel paragrafo 2.5.3 "*Revisione Periodica*"). |
| *Dipartimento Transizione Digitale ed Attività Strategiche* | • Elaborare il Piano di Attuazione della Strategia di *Cybersicurezza* Regionale; |

| Ruolo | Responsabilità |
|---|---|
| Settore 1: Infrastrutture Digitali e Sicurezza<br><br>Settore 2: Coordinamento e progettazione interventi per la transizione digitale<br><br>Settore 3: Integrazioni e sviluppo sistemi informativi regionali | • disegnare e realizzare gli interventi per il rafforzamento delle capacità *cyber* in termini di organizzazione, processi e tecnologie, in linea con il Piano Strategico approvato dalla Giunta Regionale;<br>• definire i requisiti di sicurezza e supportare gli altri Dipartimenti per il loro recepimento nell'ambito delle progettualità di carattere tecnico/informatico per la transizione digitale avviate a livello regionale per il rispetto degli stessi;<br>• rilevare lo stato di attuazione degli interventi del Piano di Attuazione;<br>• identificare ed analizzare i potenziali rischi che abbiano un impatto sulla corretta attuazione degli interventi di propria competenza e di competenza degli altri Dipartimenti;<br>• elaborare e proporre all'RTD delle strategie di mitigazione dei rischi identificati per sua approvazione;<br>• supportare l'RTD nell'attività di revisione del Piano Strategico.<br>• recepire i requisiti di sicurezza nell'ambito delle progettualità connesse agli applicativi e ai sistemi informatici dell'amministrazione regionale gestiti dai Settori del Dipartimento Transizione Digitale e Attività Strategiche. |
| Responsabile della Protezione dei Dati (DPO) | • Fornire, se richiesto, un parere, informazioni o consulenza sugli interventi di attuazione del Piano Strategico in merito ai requisiti di compliance in materia di protezione dei dati personali previsti dalla normativa vigente;<br>• vigilare sull'ottemperanza dei requisiti di compliance in materia di protezione dei dati personali nell'ambito dell'attuazione del Piano Strategico;<br>• cooperare con i Settori del Dipartimento Transizione Digitale e Attività Strategiche per la realizzazione degli interventi del Piano Strategico che prevedono l'implementazione di soluzioni/misure tecniche per garantire, sin dalla fase di disegno, l'applicazione dei principi fondamentali per la protezione dei dati personali;<br>• implementare gli interventi del Piano Strategico di propria competenza, con particolare riferimento agli aspetti organizzativi e di processo per l'adeguamento alla normativa vigente in materia di protezione dei dati personali; |

| Ruolo | Responsabilità |
|---|---|
| | • partecipare quale supporto ai Settori del Dipartimento Transizione Digitale e Attività Strategiche in sede di interfaccia con le diverse Autorità di Vigilanza e Controllo;<br>• supportare i Settori del Dipartimento Transizione Digitale e Attività Strategiche nella corretta gestione dei fornitori con riferimento alle tematiche afferenti alla protezione dei dati personali;<br>• rilevare lo stato di attuazione degli interventi di propria competenza;<br>• comunicare ai Settori del Dipartimento Transizione Digitale e Attività Strategiche eventuali evoluzioni della normativa privacy vigente che possono avere potenziali impatti sul Piano Strategico al fine di valutare la necessità di rivedere ed aggiornare lo stesso. |

*Tabella 1 – Ruoli e Responsabilità*

# 2. Componenti del Piano Strategico

Il Piano Strategico si articola in 5 principali componenti che, complessivamente, contribuiscono a definire ed attuare le linee strategiche della Regione Calabria in ambito *cybersecurity*.

Tali componenti sono:

- ***Visione** e **Missione***. La Visione rappresenta l'ambizione finale che l'Ente desidera realizzare nel lungo periodo. La Missione riflette la modalità attraverso cui l'Ente intende realizzare la Visione e i propri obiettivi strategici.
- ***Driver.*** I Driver rappresentano le direttrici di sviluppo del Piano Strategico.
- ***Obiettivi.*** Gli Obiettivi riflettono le aspirazioni regionali di medio-lungo termine che si ambisce a realizzare, i quali delineano una linea d'azione ad ampio raggio sui differenti temi di *cybersecurity*.
- ***Linee di indirizzo degli Interventi.*** Le Linee di indirizzo degli Interventi delineano le indicazioni per la definizione e l'implementazione dell'insieme degli interventi che consentiranno di perseguire con successo gli obiettivi prefissati e, in ultima analisi, realizzare la Visione della Regione Calabria.
- ***Fattori critici di successo.*** I fattori critici di successo rappresentano gli elementi chiave per la corretta ed efficace attuazione del Piano Strategico.

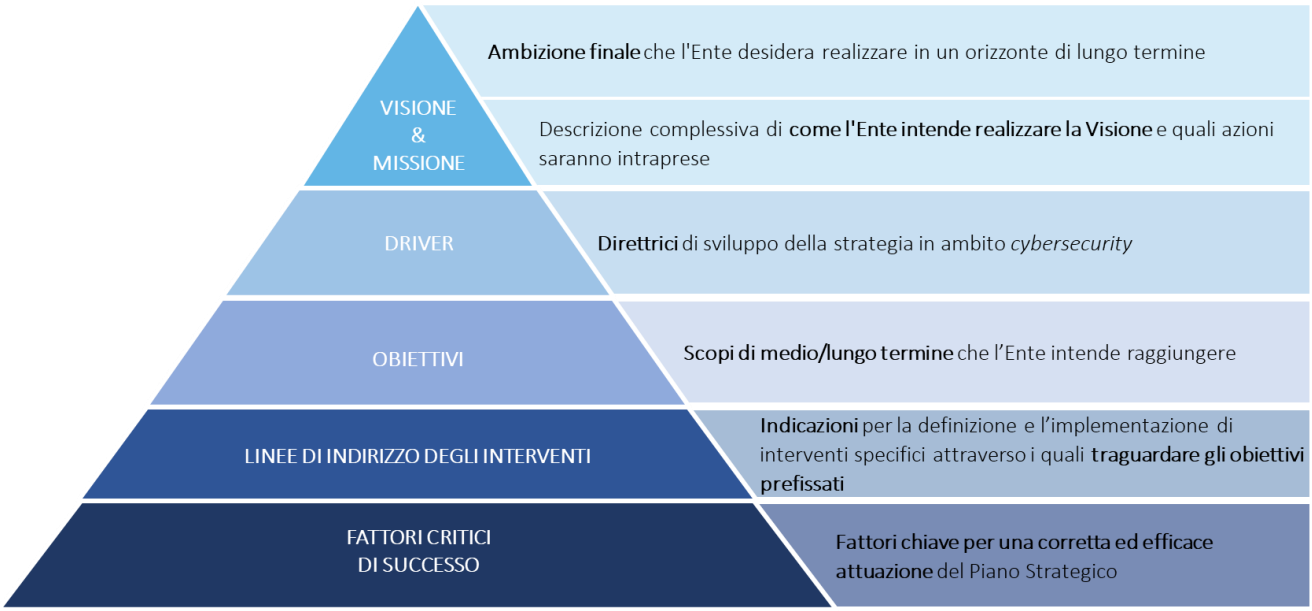


*Figura 1 – Componenti del Piano Strategico*

## 2.1 Visione e Missione

La prima componente del Piano Strategico racchiude due elementi fondamentali: la Visione e la Missione.

La Regione Calabria intende realizzare una transizione digitale *cyber* resiliente attraverso un rinnovato approccio alla *cybersecurity* per affrontare efficacemente le principali sfide attuali e future.

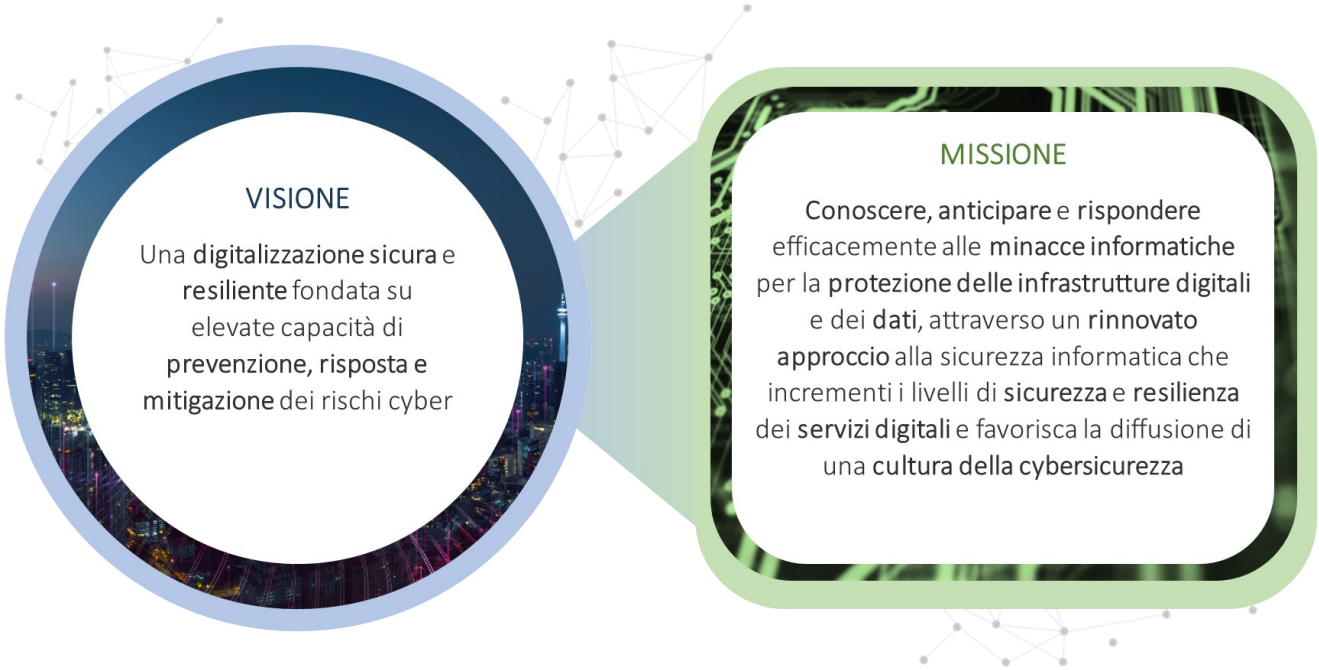


*Figura 2 – Visione e Missione del Piano Strategico*

## 2.2 Driver

La definizione degli obiettivi in ambito *cybersecurity* che la Regione Calabria intende perseguire nel periodo 2024 – 2027 segue l'orientamento offerto da 8 Driver.

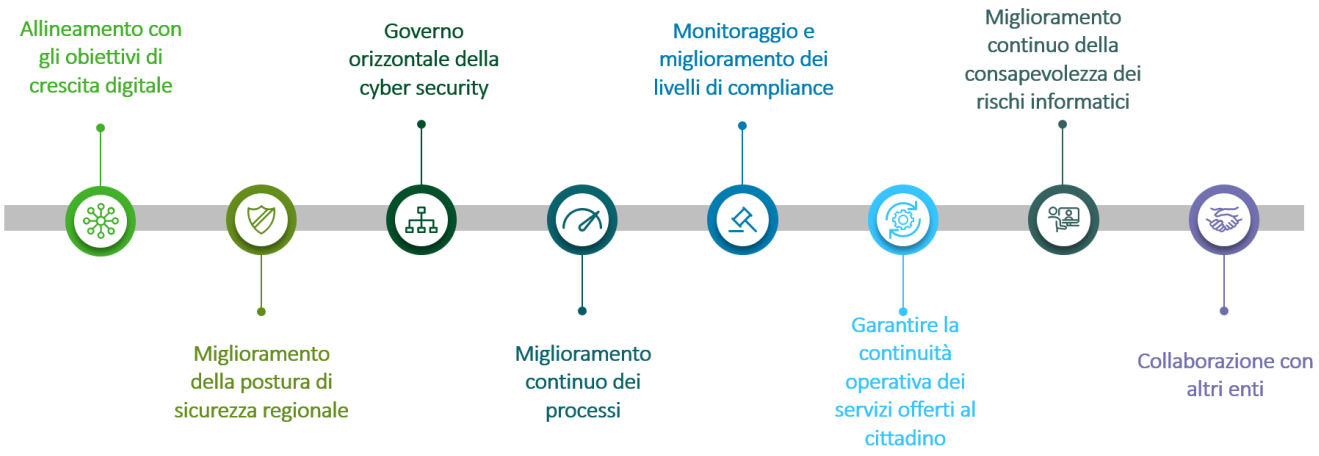


*Figura 3 – Driver del Piano Strategico*

I Driver sono stati individuati in considerazione del panorama delle minacce *cyber* e delle Linee Guida per la Crescita Digitale della Regione Calabria 2022 – 2025. Questi rappresentano le direttrici fondamentali per l'adozione di un rinnovato approccio alla *cybersecurity* e la creazione di una cultura della sicurezza cibernetica.

1. **Allineamento con gli obiettivi di crescita digitale:** Declinazione degli obiettivi strategici digitali della Regione Calabria al contesto di sicurezza informatica per supportare una digitalizzazione sicura e resiliente.

2. **Miglioramento della postura di sicurezza regionale**: Evoluzione costante dei meccanismi di difesa e risposta per mantenere un livello adeguato di sicurezza in funzione della rapida evoluzione del panorama delle minacce e delle tecnologie.

3. **Governo orizzontale della *cybersecurity*:** Centralizzazione del governo della *cybersecurity*, inclusa la definizione di requisiti tecnici, organizzativi, di processo e di monitoraggio delle performance.

4. **Miglioramento continuo dei processi:** Efficientamento dei processi ed incremento dell'efficacia per ottimizzare le risorse a disposizione e ridurre i tempi di gestione dei rischi.

5. **Monitoraggio e miglioramento dei livelli di compliance:** Adeguamento costante ai requisiti normativi applicabili per mantenere un livello di compliance adeguato nel tempo.

6. **Garantire la continuità operativa dei servizi offerti al cittadino:** Accessibilità, disponibilità e sicurezza dei servizi digitali erogati ai cittadini e agli altri enti regionali.

7. **Miglioramento continuo della consapevolezza dei rischi informatici:** Potenziamento delle competenze e della consapevolezza per i dipendenti dell'Ente sulle minacce informatiche e sulle migliori pratiche.

8. **Collaborazione con altri enti:** Coordinamento, cooperazione interregionale e nazionale per la gestione delle minacce, degli incidenti informatici e delle crisi.

## 2.3 Obiettivi

Il Piano Strategico di *cybersecurity* individua 18 Obiettivi, i quali riflettono le aspirazioni di medio-lungo termine della Regione Calabria.

| Driver | Obiettivi | Descrizione |
|---|---|---|
| Allineamento con gli obiettivi di crescita digitale | *Allineamento* | Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali. |
| | *Digitalizzazione sicura e resiliente* | Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza. |
| Miglioramento della postura di sicurezza regionale | *Gestione dei rischi cyber* | Gestire efficacemente e proattivamente i rischi informatici. |
| | *Rischi delle Terze Parti* | Incrementare la resilienza della catena di fornitura assicurando l'identificazione, la valutazione e la mitigazione dei rischi *cyber* legati ai fornitori. |
| | *Gestione dinamica degli asset* | Garantire una completa visibilità e una gestione dinamica degli asset aziendali. |
| | *Monitoraggio continuo* | Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni. |

| Driver | Obiettivi | Descrizione |
|---|---|---|
| | *Risposta rapida* | Assicurare una risposta rapida, coordinata ed efficace agli incidenti di sicurezza. |
| | *Misurazione e valutazione* | Miglioramento delle performance dei processi in ambito *cybersecurity*. |
| Governo orizzontale della *cybersecurity* | *Governo uniforme* | Adottare un modello di governo della *cybersecurity* uniforme che garantisca il corretto coordinamento di tutti gli attori. |
| | *Centralizzazione* | Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*. |
| Miglioramento continuo dei processi | *Miglioramento continuo* | Rivedere e migliorare continuamente i processi di *cybersecurity*. |
| | *Omogeneità* | Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity*. |
| Monitoraggio e miglioramento dei livelli di compliance | *Sicurezza dati e informazioni* | Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'Ente, in linea con i requisiti normativi. |
| | *Adeguamento normativo* | Analizzare le variazioni normative applicabili e mantenere un programma di adeguamento della compliance. |
| Garantire la continuità operativa dei servizi offerti al cittadino | *Resilienza operativa* | Mantenere i presidi tecnici ed organizzativi necessari a garantire l'erogazione dei servizi e pianificare la risposta e la gestione di eventuali crisi. |

| Driver | Obiettivi | Descrizione |
|---|---|---|
| Miglioramento continuo della consapevolezza dei rischi informatici | *Formazione* | Potenziare e consolidare abilità e competenze sui rischi derivanti dall'uso di strumenti informatici. |
| | *Consapevolezza* | Sensibilizzare i dipendenti a riconoscere e gestire i rischi informatici, promuovendo l'adozione di buone pratiche per proteggere sistemi, informazioni e dati. |
| Collaborazione con altri enti | *Cooperazione* | Rafforzare la collaborazione e la cooperazione con altri enti a livello nazionale e interregionale per migliorare le capacità di difesa e risposta a minacce, incidenti e crisi in ambito *cybersecurity*. |

*Tabella 2 – Driver ed Obiettivi del Piano Strategico*

### 2.3.1 Allineamento con le Linee Guida di Crescita Digitale

Gli Obiettivi definiti nel presente Piano Strategico contribuiscono alla realizzazione degli obiettivi delineati dalle "Linee Guida per la Crescita Digitale della Regione Calabria 2022-2025". Pertanto, la realizzazione del Piano Strategico è cruciale al fine di condurre la Regione Calabria verso una transizione digitale sicura e resiliente che considera la *cybersecurity* quale suo fondamento.

| Driver | Obiettivi | Obiettivi Crescita Digitale |
|---|---|---|
| Allineamento con gli obiettivi di crescita digitale | *Allineamento* | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese |
| | *Digitalizzazione sicura e resiliente* | |
| Miglioramento della postura di sicurezza regionale | *Gestione dei rischi cyber* | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 3**: Semplificazione amministrativa |
| | *Rischi delle Terze Parti* | |
| | *Gestione dinamica degli asset* | |
| | *Monitoraggio continuo* | |
| | *Risposta rapida* | |

| Driver | Obiettivi | Obiettivi Crescita Digitale |
|---|---|---|
| | *Misurazione e valutazione* | |
| Governo orizzontale della *cybersecurity* | *Governo uniforme* | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 3**: Semplificazione amministrativa |
| | *Centralizzazione* | |
| Miglioramento continuo dei processi | *Miglioramento continuo* | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 3**: Semplificazione amministrativa |
| | *Omogeneità* | |
| Monitoraggio e miglioramento dei livelli di compliance | *Sicurezza dati e informazioni* | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance |
| | *Adeguamento normativo* | |
| Garantire la continuità operativa dei servizi offerti al cittadino | *Resilienza operativa* | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance |
| Miglioramento continuo della consapevolezza dei rischi informatici | *Formazione* | ○ **Linea Strategica 3**: Semplificazione amministrativa |
| | *Consapevolezza* | |

| Driver | Obiettivi | Obiettivi Crescita Digitale |
|---|---|---|
| Collaborazione con altri enti | *Cooperazione* | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 4**: Realizzazione di Ecosistemi verticali |

*Tabella 3 – Mappatura Driver, Obiettivi e Linee Guida di Crescita Digitale*

## 2.4 Linee di Indirizzo degli Interventi

All'interno del Piano Strategico di *cybersecurity* sono delineate 51 Linee di Indirizzo degli Interventi funzionali al raggiungimento degli Obiettivi prefissati, alle quali è stato attribuito un livello di priorità (Priorità Alta, Priorità Media e Priorità Bassa).

| Priorità Alta | | | |
|---|---|---|---|
| **Linee di Indirizzo degli Interventi** | **Driver** | **Obiettivi** | **Obiettivi di Crescita Digitale** |
| **Modello di governo della *cyber*sicurezza** | • Allineamento con gli obiettivi di crescita digitale<br>• Governo orizzontale della *cybersecurity*<br>• Collaborazione con altri enti | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Governo uniforme** – Adottare un modello di governo della *cybersecurity* uniforme che garantisca il corretto coordinamento di tutti gli attori<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Cooperazione** – Rafforzare la collaborazione e la cooperazione con altri enti a livello nazionale e interregionale per migliorare le capacità di difesa e risposta a minacce, incidenti e crisi in ambito *cybersecurity* | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 3:** Semplificazione amministrativa<br>○ **Linea Strategica 4**: Realizzazione di Ecosistemi verticali |
| **Politica per la sicurezza delle informazioni** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi | ○ **Linea Strategica 1:** Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2:** Servizi digitali a cittadini, Enti locali ed imprese |

| Priorità Alta | | | |
|---|---|---|---|
| **Linee di Indirizzo degli Interventi** | **Driver** | **Obiettivi** | **Obiettivi di Crescita Digitale** |
| | • Governo orizzontale della *cybersecurity*<br>• Miglioramento continuo dei processi<br>• Monitoraggio e miglioramento dei livelli di compliance<br>• Miglioramento continuo della consapevolezza dei rischi informatici | includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Gestione dei rischi *cyber*** – Gestire efficacemente e proattivamente i rischi informatici<br>• **Governo uniforme** – Adottare un modello di governo della *cybersecurity* uniforme che garantisca il corretto coordinamento di tutti gli attori<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity*<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi<br>• **Consapevolezza** – Sensibilizzare i dipendenti a riconoscere e gestire i rischi informatici, promuovendo l'adozione di buone pratiche per proteggere sistemi, informazioni e dati | ○ **Linea Strategica 3:** Semplificazione amministrativa |
| **Processo per la gestione degli asset aziendali** | • Allineamento con gli obiettivi di crescita digitale | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | • Miglioramento della postura di sicurezza regionale<br>• Governo orizzontale della *cybersecurity*<br>• Miglioramento continuo dei processi<br>• Monitoraggio e miglioramento dei livelli di compliance | • **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Gestione dinamica degli asset** – Garantire una completa visibilità e una gestione dinamica degli asset aziendali<br>• **Monitoraggio continuo** – Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Miglioramento continuo** – Rivedere e migliorare continuamente i processi di *cybersecurity*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity*<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi | ○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3**: Semplificazione amministrativa |
| **Politica per il corretto utilizzo** | • Allineamento con gli obiettivi | • **Allineamento** – Garantire che gli interventi in materia *cyber* | ○ **Linea Strategica 1**: Sicurezza, data privacy, |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| delle risorse informatiche | di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Governo orizzontale della *cybersecurity*<br>• Miglioramento continuo dei processi<br>• Monitoraggio e miglioramento dei livelli di compliance | supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Gestione dinamica degli asset** – Garantire una completa visibilità e una gestione dinamica degli asset aziendali<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity*<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi | interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3**: Semplificazione amministrativa |
| **Processo per la gestione degli accessi logici**<br>**Processo per la gestione degli accessi fisici** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | • Governo orizzontale della *cybersecurity*<br>• Miglioramento continuo dei processi<br>• Monitoraggio e miglioramento dei livelli di compliance | includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Monitoraggio continuo** – Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Miglioramento continuo** – Rivedere e migliorare continuamente i processi di *cybersecurity*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity*<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi | ○ **Linea Strategica 3**: Semplificazione amministrativa |
| *Cyber* Risk Management Framework | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Gestione dei rischi *cyber*** – Gestire efficacemente e proattivamente i rischi informatici<br>• **Governo uniforme** – Adottare un modello di governo della *cybersecurity* uniforme che | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 3**: Semplificazione amministrativa |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | • Governo orizzontale della *cybersecurity*<br>• Miglioramento continuo dei processi<br>• Monitoraggio e miglioramento dei livelli di compliance | garantisca il corretto coordinamento di tutti gli attori<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity*<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi | |
| *Cyber* Risk Management Framework per i fornitori | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Governo orizzontale della *cybersecurity*<br>• Miglioramento continuo dei processi<br>• Monitoraggio e miglioramento | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Rischi delle Terze Parti** – Incrementare la resilienza della catena di fornitura assicurando l'identificazione, la valutazione e la mitigazione dei rischi *cyber* legati ai fornitori<br>• **Misurazione e valutazione** – Miglioramento delle performance dei processi in ambito *cybersecurity*<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 3**: Semplificazione amministrativa |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | dei livelli di compliance | supervisione dei livelli di rischio *cyber*<br>• **Governo uniforme** – Adottare un modello di governo della *cybersecurity* uniforme che garantisca il corretto coordinamento di tutti gli attori<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity*<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi | |
| **Processo per la gestione dei rischi** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Governo orizzontale della *cybersecurity*<br>• Miglioramento continuo dei processi<br>• Monitoraggio e miglioramento | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Gestione dei rischi *cyber*** – Gestire efficacemente e proattivamente i rischi informatici<br>• **Rischi delle Terze Parti** – Incrementare la resilienza della catena di fornitura assicurando l'identificazione, la valutazione e la | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3**: Semplificazione amministrativa |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | dei livelli di compliance | mitigazione dei rischi *cyber* legati ai fornitori<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Miglioramento continuo** – Rivedere e migliorare continuamente i processi di *cybersecurity*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity*<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi | |
| **Processo di gestione di sicurezza della rete** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Governo orizzontale della *cybersecurity* | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Gestione dei rischi *cyber*** – Gestire efficacemente e proattivamente i rischi informatici | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3**: Semplificazione amministrativa |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | • Miglioramento continuo dei processi<br>• Monitoraggio e miglioramento dei livelli di compliance<br>• Garantire la continuità operativa dei servizi offerti al cittadino | • **Rischi delle Terze Parti** – Incrementare la resilienza della catena di fornitura assicurando l'identificazione, la valutazione e la mitigazione dei rischi *cyber* legati ai fornitori<br>• **Monitoraggio continuo** – Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Miglioramento continuo** – Rivedere e migliorare continuamente i processi di *cybersecurity*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity*<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi<br>• **Resilienza operativa** – Mantenere i presidi tecnici ed organizzativi necessari a garantire l'erogazione dei servizi e pianificare la risposta e la gestione di eventuali crisi | |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| **Strumenti per la Business Impact Analysis (BIA)** | • Allineamento con gli obiettivi di crescita digitale<br>• Garantire la continuità operativa dei servizi offerti al cittadino | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Resilienza operativa** – Mantenere i presidi tecnici ed organizzativi necessari a garantire l'erogazione dei servizi e pianificare la risposta e la gestione di eventuali crisi | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese |
| **Esecuzione di Business Impact Analysis (BIA)** | • Allineamento con gli obiettivi di crescita digitale<br>• Garantire la continuità operativa dei servizi offerti al cittadino | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Resilienza operativa** – Mantenere i presidi tecnici ed organizzativi necessari a garantire l'erogazione dei servizi e pianificare la risposta e la gestione di eventuali crisi | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3**: Semplificazione amministrativa |
| **Creazione di un CSIRT** | • Allineamento con gli obiettivi di crescita digitale | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | • Miglioramento della postura di sicurezza regionale<br>• Governo orizzontale della *cybersecurity*<br>• Garantire la continuità operativa dei servizi offerti al cittadino<br>• Monitoraggio e miglioramento dei livelli di compliance<br>• Collaborazione con altri enti | • **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Gestione dei rischi *cyber*** – Gestire efficacemente e proattivamente i rischi informatici<br>• **Rischi delle Terze Parti** – Incrementare la resilienza della catena di fornitura assicurando l'identificazione, la valutazione e la mitigazione dei rischi *cyber* legati ai fornitori<br>• **Monitoraggio continuo** – Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni<br>• **Risposta rapida** – Assicurare una risposta rapida, coordinata ed efficace agli incidenti di sicurezza<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi<br>• **Resilienza operativa** – Mantenere i presidi tecnici ed organizzativi necessari a garantire l'erogazione | ○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3**: Semplificazione amministrativa<br>○ **Linea Strategica 4:** Realizzazione di Ecosistemi verticali |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | | dei servizi e pianificare la risposta e la gestione di eventuali crisi<br>• **Cooperazione** – Rafforzare la collaborazione e la cooperazione con altri enti a livello nazionale e interregionale per migliorare le capacità di difesa e risposta a minacce, incidenti e crisi in ambito *cybersecurity* | |
| **Processo per la gestione dei log** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Governo orizzontale della *cybersecurity*<br>• Miglioramento continuo dei processi | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Monitoraggio continuo** – Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Miglioramento continuo** – Rivedere e migliorare continuamente i processi di *cybersecurity*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3**: Semplificazione amministrativa |

| Priorità Alta | | | |
|---|---|---|---|
| **Linee di Indirizzo degli Interventi** | **Driver** | **Obiettivi** | **Obiettivi di Crescita Digitale** |
| | | processi standard per la gestione della *cybersecurity* | |
| **Processo per la gestione degli incidenti** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Governo orizzontale della *cybersecurity*<br>• Miglioramento continuo dei processi<br>• Monitoraggio e miglioramento dei livelli di compliance | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Risposta rapida** – Assicurare una risposta rapida, coordinata ed efficace agli incidenti di sicurezza<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Miglioramento continuo** – Rivedere e migliorare continuamente i processi di *cybersecurity*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity*<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi | ○ **Linea Strategica 1:** Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2:** Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3:** Semplificazione amministrativa |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| Piani di Business Continuity e Disaster Recovery | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Governo orizzontale della *cybersecurity*<br>• Miglioramento continuo dei processi<br>• Monitoraggio e miglioramento dei livelli di compliance<br>• Garantire la continuità operativa dei servizi offerti al cittadino | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Risposta rapida** – Assicurare una risposta rapida, coordinata ed efficace agli incidenti di sicurezza<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Miglioramento continuo** – Rivedere e migliorare continuamente i processi di *cybersecurity*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity*<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi<br>• **Resilienza operativa** – Mantenere i presidi tecnici ed organizzativi necessari a garantire l'erogazione | ○ **Linea Strategica 1:** Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2:** Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3:** Semplificazione amministrativa |

| Priorità Alta | | | |
|---|---|---|---|
| **Linee di Indirizzo degli Interventi** | **Driver** | **Obiettivi** | **Obiettivi di Crescita Digitale** |
| | | dei servizi e pianificare la risposta e la gestione di eventuali crisi | |
| **Processo di Patch e Vulnerability Management** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Governo orizzontale della *cybersecurity*<br>• Miglioramento continuo dei processi | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Monitoraggio continuo** – Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Miglioramento continuo** – Rivedere e migliorare continuamente i processi di *cybersecurity* | ○ **Linea Strategica 1:** Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2:** Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3:** Semplificazione amministrativa |
| **Processo per la gestione del ciclo di vita dei dati** | • Allineamento con gli obiettivi di crescita digitale<br>• Governo orizzontale della *cybersecurity* | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi | ○ **Linea Strategica 1:** Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2:** Servizi digitali a cittadini, Enti locali ed imprese |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | • Miglioramento continuo dei processi<br>• Monitoraggio e miglioramento dei livelli di compliance | includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Miglioramento continuo** – Rivedere e migliorare continuamente i processi di *cybersecurity*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity*<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi<br>• **Adeguamento normativo** – Analizzare le variazioni normative applicabili e mantenere un programma di adeguamento della compliance | ○ **Linea Strategica 3:** Semplificazione amministrativa |
| **Security by design** | • Allineamento con gli obiettivi di crescita digitale<br>• Governo orizzontale della *cybersecurity* | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi | ○ **Linea Strategica 1:** Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2:** Servizi digitali a cittadini, Enti locali ed imprese |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | • Miglioramento continuo dei processi<br>• Monitoraggio e miglioramento dei livelli di compliance | includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Miglioramento continuo** – Rivedere e migliorare continuamente i processi di *cybersecurity*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity*<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi<br>• **Adeguamento normativo** – Analizzare le variazioni normative applicabili e mantenere un programma di adeguamento della compliance | ○ **Linea Strategica 3:** Semplificazione amministrativa |
| **Soluzione di *Cyber* Governance, Risk & Compliance** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi | ○ **Linea Strategica 1:** Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2:** Servizi digitali a cittadini, Enti locali ed imprese |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | • Governo orizzontale della *cybersecurity*<br>• Miglioramento continuo dei processi<br>• Monitoraggio e miglioramento dei livelli di compliance | includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Gestione dei rischi *cyber*** – Gestire efficacemente e proattivamente i rischi informatici<br>• **Rischi delle Terze Parti** – Incrementare la resilienza della catena di fornitura assicurando l'identificazione, la valutazione e la mitigazione dei rischi *cyber* legati ai fornitori<br>• **Gestione dinamica degli asset** – Garantire una completa visibilità e una gestione dinamica degli asset aziendali<br>• **Risposta rapida** – Assicurare una risposta rapida, coordinata ed efficace agli incidenti di sicurezza<br>• **Governo uniforme** – Adottare un modello di governo della *cybersecurity* uniforme che garantisca il corretto coordinamento di tutti gli attori<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Miglioramento continuo** – Rivedere e migliorare continuamente i processi di *cybersecurity*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei | ○ **Linea Strategica 3:** Semplificazione amministrativa |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | | processi standard per la gestione della *cybersecurity*<br>• **Adeguamento normativo** – Analizzare le variazioni normative applicabili e mantenere un programma di adeguamento della compliance | |
| **Servizi CSIRT per la rilevazione degli eventi** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Governo orizzontale della *cybersecurity*<br>• Collaborazione con altri enti | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Monitoraggio continuo** – Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni<br>• **Risposta rapida** – Assicurare una risposta rapida, coordinata ed efficace agli incidenti di sicurezza<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Cooperazione** – Rafforzare la collaborazione e la cooperazione con altri enti a livello nazionale e interregionale per migliorare le capacità di difesa e risposta a | ○ **Linea Strategica 1:** Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2:** Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3:** Semplificazione amministrativa<br>○ **Linea Strategica 4:** Realizzazione di Ecosistemi verticali |

| Priorità Alta | | | |
|---|---|---|---|
| **Linee di Indirizzo degli Interventi** | **Driver** | **Obiettivi** | **Obiettivi di Crescita Digitale** |
| | | minacce, incidenti e crisi in ambito *cybersecurity* | |
| **Processo di analisi forense** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento continuo dei processi | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Miglioramento continuo** – Rivedere e migliorare continuamente i processi di *cybersecurity* | ○ **Linea Strategica 1:** Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 3:** Semplificazione amministrativa |
| **Servizi CSIRT per la risposta agli incidenti** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Governo orizzontale della *cybersecurity*<br>• Monitoraggio e miglioramento dei livelli di compliance | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Risposta rapida** – Assicurare una risposta rapida, coordinata ed efficace agli incidenti di sicurezza<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante | ○ **Linea Strategica 1:** Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2:** Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3:** Semplificazione amministrativa<br>○ **Linea Strategica 4:** Realizzazione di Ecosistemi verticali |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | • Garantire la continuità operativa dei servizi offerti al cittadino<br>• Collaborazione con altri enti | supervisione dei livelli di rischio *cyber*<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi<br>• **Adeguamento normativo** – Analizzare le variazioni normative applicabili e mantenere un programma di adeguamento della compliance<br>• **Resilienza operativa** – Mantenere i presidi tecnici ed organizzativi necessari a garantire l'erogazione dei servizi e pianificare la risposta e la gestione di eventuali crisi<br>• **Cooperazione** – Rafforzare la collaborazione e la cooperazione con altri enti a livello nazionale e interregionale per migliorare le capacità di difesa e risposta a minacce, incidenti e crisi in ambito *cybersecurity* | |
| **Tecnologie Web Application Firewall (WAF)** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Monitoraggio e miglioramento | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza | ○ **Linea Strategica 1:** Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2:** Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3:** Semplificazione amministrativa |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | dei livelli di compliance | • **Gestione dei rischi *cyber*** – Gestire efficacemente e proattivamente i rischi informatici<br>• **Monitoraggio continuo** – Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi | |
| **Aautenticazione multi-fattore (MFA)** | • Allineamento con gli obiettivi di crescita digitale<br>• Monitoraggio e miglioramento dei livelli di compliance | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi | ○ **Linea Strategica 1:** Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2:** Servizi digitali a cittadini, Enti locali ed imprese |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| **Identity Governance** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Monitoraggio e miglioramento dei livelli di compliance | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Monitoraggio continuo** – Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi | ○ **Linea Strategica 1:** Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2:** Servizi digitali a cittadini, Enti locali ed imprese |
| **Privileged Account Management (PAM)** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Monitoraggio e miglioramento dei livelli di compliance | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Monitoraggio continuo** – Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | | • **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi<br>• **Adeguamento normativo** – Analizzare le variazioni normative applicabili e mantenere un programma di adeguamento della compliance | |
| Network Access Control (NAC) | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Monitoraggio e miglioramento dei livelli di compliance | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Monitoraggio continuo** – Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese |
| Processo di *Cyber* Threat Intelligence | • Allineamento con gli obiettivi di crescita digitale | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance |

| Priorità Alta | | | |
|---|---|---|---|
| **Linee di Indirizzo degli Interventi** | **Driver** | **Obiettivi** | **Obiettivi di Crescita Digitale** |
| | • Miglioramento della postura di sicurezza regionale<br>• Governo orizzontale della *cybersecurity*<br>• Collaborazione con altri enti | • **Gestione dei rischi *cyber*** – Gestire efficacemente e proattivamente i rischi informatici<br>• **Rischi delle Terze Parti** – Incrementare la resilienza della catena di fornitura assicurando l'identificazione, la valutazione e la mitigazione dei rischi *cyber* legati ai fornitori<br>• **Monitoraggio continuo** – Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Cooperazione** – Rafforzare la collaborazione e la cooperazione con altri enti a livello nazionale e interregionale per migliorare le capacità di difesa e risposta a minacce, incidenti e crisi in ambito *cybersecurity* | ○ **Linea Strategica 3**: Semplificazione amministrativa<br>○ **Linea Strategica 4:** Realizzazione di Ecosistemi verticali |
| **Aggiornamento dei trattamenti** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Monitoraggio e miglioramento | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Gestione dinamica degli asset** – Garantire una completa visibilità e una gestione dinamica degli asset aziendali<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | dei livelli di compliance | integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi<br>• **Adeguamento normativo** – Analizzare le variazioni normative applicabili e mantenere un programma di adeguamento della compliance | |
| **Svolgimento di DPIA** | • Allineamento con gli obiettivi di crescita digitale<br>• Monitoraggio e miglioramento dei livelli di compliance | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi<br>• **Adeguamento normativo** – Analizzare le variazioni normative applicabili e mantenere un programma di adeguamento della compliance | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance |
| **Classificazione delle informazioni** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento continuo dei processi<br>• Monitoraggio e miglioramento | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity*<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 3**: Semplificazione amministrativa |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | dei livelli di compliance | patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi | |
| Data Classification & Labelling | • Allineamento con gli obiettivi di crescita digitale<br>• Monitoraggio e miglioramento dei livelli di compliance | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi<br>• **Adeguamento normativo** – Analizzare le variazioni normative applicabili e mantenere un programma di adeguamento della compliance | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese |
| Data Encryption | • Allineamento con gli obiettivi di crescita digitale<br>• Monitoraggio e miglioramento | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | dei livelli di compliance | strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi<br>• **Adeguamento normativo** – Analizzare le variazioni normative applicabili e mantenere un programma di adeguamento della compliance | ○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese |
| Mobile Security | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Monitoraggio e miglioramento dei livelli di compliance | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Monitoraggio continuo** – Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3**: Semplificazione amministrativa |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| Sistema documentale privacy | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Governo orizzontale della *cybersecurity*<br>• Miglioramento continuo dei processi<br>• Monitoraggio e miglioramento dei livelli di compliance<br>• Miglioramento continuo della consapevolezza dei rischi informatici | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Rischi delle Terze Parti** – Incrementare la resilienza della catena di fornitura assicurando l'identificazione, la valutazione e la mitigazione dei rischi *cyber* legati ai fornitori<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Miglioramento continuo** – Rivedere e migliorare continuamente i processi di *cybersecurity*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity*<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi<br>• **Adeguamento normativo** – Analizzare le variazioni normative applicabili e mantenere un programma di adeguamento della compliance | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 3**: Semplificazione amministrativa |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | | • **Formazione** – Potenziare e consolidare abilità e competenze sui rischi derivanti dall'uso di strumenti informatici<br>• **Consapevolezza** – Sensibilizzare i dipendenti a riconoscere e gestire i rischi informatici, promuovendo l'adozione di buone pratiche per proteggere sistemi, informazioni e dati | |
| **Data Discovery Audit & Protection** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Monitoraggio e miglioramento dei livelli di compliance | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Gestione dinamica degli asset** – Garantire una completa visibilità e una gestione dinamica degli asset aziendali<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi<br>• **Adeguamento normativo** – Analizzare le variazioni normative applicabili e mantenere un programma di adeguamento della compliance | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance |
| **Data Loss Prevention** | • Allineamento con gli obiettivi di crescita digitale<br>• Monitoraggio e miglioramento | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | dei livelli di compliance | conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi<br>• **Adeguamento normativo** – Analizzare le variazioni normative applicabili e mantenere un programma di adeguamento della compliance | ○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese |
| **Posta elettronica** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Monitoraggio e miglioramento dei livelli di compliance | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Monitoraggio continuo** – Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| Patch Management | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Gestione dei rischi *cyber*** – Gestire efficacemente e proattivamente i rischi informatici<br>• **Gestione dinamica degli asset** – Garantire una completa visibilità e una gestione dinamica degli asset aziendali<br>• **Monitoraggio continuo** – Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese |
| Servizio di *Cyber* Threat Intelligence | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Governo orizzontale della *cybersecurity*<br>• Collaborazione con altri enti | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Gestione dei rischi *cyber*** – Gestire efficacemente e proattivamente i rischi informatici<br>• **Rischi delle Terze Parti** – Incrementare la resilienza della catena di fornitura assicurando l'identificazione, la valutazione e la mitigazione dei rischi *cyber* legati ai fornitori | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 3**: Semplificazione amministrativa<br>○ **Linea Strategica 4**: Realizzazione di Ecosistemi verticali |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | | • **Monitoraggio continuo** – Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Cooperazione** – Rafforzare la collaborazione e la cooperazione con altri enti a livello nazionale e interregionale per migliorare le capacità di difesa e risposta a minacce, incidenti e crisi in ambito *cybersecurity* | |
| **Formazione sulla sicurezza informatica** | • Allineamento con gli obiettivi di crescita digitale<br>• Governo orizzontale della *cybersecurity*<br>• Miglioramento continuo dei processi<br>• Monitoraggio e miglioramento dei livelli di compliance<br>• Miglioramento continuo della consapevolezza dei rischi informatici | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity* | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3**: Semplificazione amministrativa |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | | • **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi<br>• **Formazione** – Potenziare e consolidare abilità e competenze sui rischi derivanti dall'uso di strumenti informatici<br>• **Consapevolezza** – Sensibilizzare i dipendenti a riconoscere e gestire i rischi informatici, promuovendo l'adozione di buone pratiche per proteggere sistemi, informazioni e dati | |
| **Sensibilizzazione sulla sicurezza informatica** | • Allineamento con gli obiettivi di crescita digitale<br>• Governo orizzontale della *cybersecurity*<br>• Miglioramento continuo dei processi<br>• Monitoraggio e miglioramento dei livelli di compliance<br>• Miglioramento continuo della consapevolezza dei rischi informatici | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity* | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3**: Semplificazione amministrativa |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | | • **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi<br>• **Formazione** – Potenziare e consolidare abilità e competenze sui rischi derivanti dall'uso di strumenti informatici<br>• **Consapevolezza** – Sensibilizzare i dipendenti a riconoscere e gestire i rischi informatici, promuovendo l'adozione di buone pratiche per proteggere sistemi, informazioni e dati | |
| **Strumento di Asset Management** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Gestione dinamica degli asset** – Garantire una completa visibilità e una gestione dinamica degli asset aziendali<br>• **Monitoraggio continuo** – Incrementare le capacità di monitoraggio continuo e analisi di rete, sistemi e applicazioni | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese |

| Priorità Alta | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| **Classificazione degli incidenti di sicurezza** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Miglioramento continuo dei processi | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Risposta rapida** – Assicurare una risposta rapida, coordinata ed efficace agli incidenti di sicurezza<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity* | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 3:** Semplificazione amministrativa |
| **Infrastruttura di Disaster Recovery** | • Allineamento con gli obiettivi di crescita digitale<br>• Monitoraggio e miglioramento dei livelli di compliance<br>• Garantire la continuità operativa dei servizi al cittadino | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Resilienza operativa –** Mantenere i presidi tecnici ed organizzativi necessari a garantire l'erogazione dei servizi e pianificare la risposta e la gestione di eventuali crisi<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese |

*Tabella 4 – Linee di Indirizzo degli Interventi Priorità Alta*

| Priorità Media | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| **Processo di Performance Management** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Miglioramento continuo dei processi | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente –** Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Gestione dei rischi *cyber*** – Gestire efficacemente e proattivamente i rischi informatici<br>• **Misurazione e valutazione** – Miglioramento delle performance dei processi in ambito *cybersecurity*<br>• **Miglioramento continuo** – Rivedere e migliorare continuamente i processi di *cybersecurity*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity* | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese |
| **Password Policy** | • Allineamento con gli obiettivi di crescita digitale<br>• Governo orizzontale della *cybersecurity*<br>• Miglioramento continuo dei processi | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3**: Semplificazione amministrativa |

| Priorità Media | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | • Monitoraggio e miglioramento dei livelli di compliance | • **Centralizzazione** – Centralizzare i meccanismi processuali e tecnici per una corretta e costante supervisione dei livelli di rischio *cyber*<br>• **Omogeneità** – Ridurre la frammentazione e adottare dei processi standard per la gestione della *cybersecurity*<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'ente, in linea con i requisiti normativi | |
| **Test/verifica dei piani IT Business Continuity e Disaster Recovery** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Garantire la continuità operativa dei servizi offerti al cittadino | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Risposta rapida** – Assicurare una risposta rapida, coordinata ed efficace agli incidenti di sicurezza<br>• **Resilienza operativa** – Mantenere i presidi tecnici ed organizzativi necessari a garantire l'erogazione dei servizi e pianificare la risposta e la gestione di eventuali crisi | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3**: Semplificazione amministrativa |

| Priorità Media | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| **Security Ratings** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Gestione dei rischi *cyber*** – Gestire efficacemente e proattivamente i rischi informatici<br>• **Misurazione e valutazione** – Miglioramento delle performance dei processi in ambito *cybersecurity* | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3**: Semplificazione amministrativa |

*Tabella 5 – Linee di Indirizzo degli Interventi Priorità Media*

| Priorità Bassa | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| **Crisis Management** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Monitoraggio e miglioramento | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese |

| Priorità Bassa | | | |
|---|---|---|---|
| Linee di Indirizzo degli Interventi | Driver | Obiettivi | Obiettivi di Crescita Digitale |
| | dei livelli di compliance<br>• Garantire la continuità operativa dei servizi al cittadino | • **Risposta rapida –** Assicurare una risposta rapida, coordinata ed efficace agli incidenti di sicurezza<br>• **Sicurezza dati e informazioni** – Salvaguardare riservatezza, integrità e disponibilità del patrimonio dati personali e informazioni dell'Ente, in linea con i requisiti normativi<br>• **Resilienza operativa –** Mantenere i presidi tecnici ed organizzativi necessari a garantire l'erogazione dei servizi e pianificare la risposta e la gestione di eventuali crisi | |
| **Soluzioni di Performance Management** | • Allineamento con gli obiettivi di crescita digitale<br>• Miglioramento della postura di sicurezza regionale<br>• Miglioramento continuo dei processi | • **Allineamento** – Garantire che gli interventi in materia *cyber* supportino gli obiettivi strategici regionali<br>• **Digitalizzazione sicura e resiliente** – Verificare che per il conseguimento degli obiettivi strategici regionali gli interventi includano gli adeguati presidi per garantire sicurezza e resilienza<br>• **Gestione dei rischi *cyber*** – Gestire efficacemente e proattivamente i rischi informatici<br>• **Misurazione e valutazione** – Miglioramento delle performance dei processi in ambito *cybersecurity*<br>• **Miglioramento continuo** – Rivedere e migliorare continuamente i processi di *cybersecurity* | ○ **Linea Strategica 1**: Sicurezza, data privacy, interoperabilità e data governance<br>○ **Linea Strategica 2**: Servizi digitali a cittadini, Enti locali ed imprese<br>○ **Linea Strategica 3**: Semplificazione amministrativa |

*Tabella 6 – Linee di Indirizzo degli Interventi Priorità Bassa*

## 2.5 Fattori Critici di Successo

Il Piano Strategico rappresenta uno strumento essenziale per la Regione Calabria nel suo percorso verso un rinnovato approccio alla *cybersecurity*. Per tale ragione, sono stati identificati 4 fattori chiave per una corretta ed efficace attuazione dello stesso.


*Figura 4 – Fattori critici di successo*

### 2.5.1 Modello di Governance

Al fine di favorire, coordinare e monitorare l'implementazione del Piano Strategico, è stato costruito un modello di governo in accordo con i ruoli e le responsabilità definiti nel presente documento (paragrafo 1.2 *"Ruoli e Responsabilità"*).

### 2.5.2 Monitoraggio e Valutazione dei Progressi

Si prevede l'implementazione di un processo di monitoraggio e valutazione dei progressi, che comprende la definizione e la misurazione degli indicatori chiave di prestazione, quale strumento per monitorare lo stato di attuazione del Piano Strategico, valutare i risultati ottenuti, individuare eventuali scostamenti tra gli obiettivi inizialmente pianificati e quelli raggiunti, mettere in atto tempestive azioni correttive.

### 2.5.3 Revisione Periodica

Al fine di verificare ed assicurare che il Piano Strategico sia, nel corso del tempo, coerente con le priorità e le esigenze della Regione Calabria, è previsto un processo di revisione periodica, su base annua o ogniqualvolta necessario, in funzione dei seguenti elementi:

- *Panorama delle minacce cyber globali*. Il panorama delle minacce *cyber* è in continua evoluzione e risulta essenziale rivolgere costantemente lo sguardo alle tendenze emergenti per identificare gli adeguati strumenti di prevenzione e contrasto ai rischi informatici.
- *Evoluzione delle tecnologie e delle soluzioni di cybersecurity*. Le tecnologie emergenti offrono molteplici e nuove opportunità ma allo stesso tempo comportano nuovi rischi. È fondamentale elaborare una strategia che consenta di sfruttare i vantaggi offerti dalle nuove tecnologie sia per

avanzare nel processo di digitalizzazione dei servizi sia per rafforzare la capacità di prevenire e contrastare i rischi *cyber*.

- *Evoluzione normativa*. Gli organismi normativi nazionali, sovranazionali ed internazionali stanno sviluppando e raffinando le leggi e le regolamentazioni in ambito sicurezza informatica e protezione dei dati personali. L'adeguamento alle normative è un aspetto fondamentale che la Regione Calabria terrà in considerazione nell'ambito della definizione e dell'attuazione del proprio approccio alla *cybersecurity*, al fine di assicurare la conformità alle disposizioni vigenti e, al contempo, allineare il proprio sistema di gestione della sicurezza informatica ai più recenti sviluppi normativi.
- *Modello organizzativo.* Eventuali revisioni del modello organizzativo della Regione Calabria possono avere impatti sull'assegnazione di ruoli e responsabilità nella gestione della sicurezza informatica. Contestualmente, cambiamenti nell'architettura *cyber* nazionale possono richiedere adeguamenti che comportano significative modifiche del modello organizzativo regionale e/o l'attuazione di ulteriori interventi inizialmente non pianificati.
- *Esiti delle attività di monitoraggio sull'attuazione del Piano Strategico.* I risultati delle attività di monitoraggio svolte contribuiscono alla valutazione sull'eventuale necessità di rivedere ed aggiornare alcune delle componenti del Piano Strategico, in funzione dei potenziali rischi identificati e delle relative strategie di mitigazione e/o azioni correttive definite.

### 2.5.4 Modalità di attuazione

Il presente piano non comporta oneri in quanto di natura programmatica. Le linee strategiche di indirizzo in esso indicate saranno oggetto di un successivo piano di attuazione in cui verranno definiti gli interventi e le loro tempistiche nonché le risorse finanziarie ad essi attribuite. Le risorse finanziarie per gli interventi di cybersicurezza sono già disponibili nei programmi sostenuti da fondi del PR 2021-2027, FSC e PNRR.