Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Beschluss der Landesregierung

Deliberazione della Giunta Provinciale

Nr. 151
Sitzung vom 11/03/2025 Seduta del

ANWESEND SIND		SONO PRESENTI
Landeshauptmann	Arno Kompatscher	Presidente
Landeshauptmannstellvertr.	Rosmarie Pamer	Vicepresidente
Landeshauptmannstellvertr.	Marco Galateo	Vicepresidente
Landeshauptmannstellvertr.	Daniel Alfreider	Vicepresidente
Landesräte	Peter Brunner	Assessori
	Ulli Mair	
	Hubert Messner	
	Luis Walcher	
Generalsekretär	Eros Magnago	Segretario Generale

Betreff:

Cyber-Sicherheits-Governance und CSIRT der Autonome Provinz Bozen Südtirol

Oggetto:

Cyber Security Governance e CSIRT della Provincia Autonoma di Bolzano Alto Adige

Vorschlag vorbereitet von Abteilung / Amt Nr. 9 Proposta elaborata dalla Ripartizione / Ufficio n.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Die Landesregierung

hat in folgende Rechtsvorschriften und Unterlagen Einsicht genommen:

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (sog. Datenschutz-Grundverordnung);

Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie);

Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG;

Verordnung (EU) 2019/881 des Europäischen Parlamentes und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit)

Durchführungsverordnung (EU)

La Giunta Provinciale

ha preso visione delle seguenti norme giuridiche e documenti:

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche in materia di trattamento dei dati personali e alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati, cosidetto GDPR);

Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2);

Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento die dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2022/CE;

Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENSIA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (regolamento sulla cibersicurezza);

Regolamento di esecuzione (UE)

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

2024/482 der Kommission vom 31. Januar 2024 mit Durchführungsbestimmungen zur Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates hinsichtlich der Annahme des auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die Cybersicherheitszertifizierung (EUCC);

2024/482 della Commissione del 31 gennaio 2024 recante modalità per l'applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC);

Gesetzesvertretendes Dekret vom 4. September 2024, Nr. 138 zur Umsetzung der Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148;

Decreto Legislativo 4 settembre 2024, n. 138 riguardante il recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148;

Gesetz vom 28. Juni 2024, Nr. 90 betreffend Bestimmungen zur Stärkung der nationalen Cybersicherheit und zur Cyberkriminalität. Das Gesetz zielt darauf ab, die nationale Cybersicherheit zu stärken sowie die Cyberkriminalität durch innovative Maßnahmen zu bekämpfen und sieht zu diesem Zweck unter anderem vor, dass alle in Artikel 1 Absatz 1 des Gesetzes Nr. 90/2024 genannten Subjekte die Agentur für nationale Cybersicherheit (in der Folge „ACN") über die Ernennung einer Ansprechperson für Cybersicherheit unterrichten müssen;

Legge 28 giugno 2024, n. 90 riguardante Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici. La legge mira a rafforzare la cybersicurezza nazionale nonché a contrastare i reati informatici attraverso misure innovative e a tal fine prevede, tra l'altro, che tutti i soggetti di cui all'articolo 1, comma 1 della Legge n. 90/2024 comunicano all'Agenzia per la cybersicurezza nazionale (di seguito "ACN") la nomina del Referente per la Cybersicurezza;

Leitlinien der ACN zur Stärkung der Resilienz der in Artikel 1, Absatz 1 des Gesetzes Nr. 90 vom 28. Juni 2024 genannten Subjekte;

Linee guida di ACN per il rafforzamento della resilienza dei soggetti di cui all'articolo 1, comma 1, della Legge 28 giugno 2024, n. 90;

Gesetzesvertretendes Dekret 7. März 2005, Nr. 82 i.g.F. betreffend den Kodex der digitalen Verwaltung (in der Folge „CAD") und insbesondere den Artikel 14-bis zur Umsetzung der Agenda digitales Italien, den Artikel 71 zu den Regeln und technischen Richtlinien für die Verwaltung von digitalen Dokumenten und Daten sowie den

Decreto legislativo 7 marzo 2005, n. 82 e ss. modifiche recante il Codice dell'amministrazione digitale (di seguito "CAD"), in particolare l'articolo 14-bis relativo all'attuazione dell'Agenda per l'Italia Digitale, l'articolo 71 sulle regole e indirizzi tecnici per la gestione dei documenti e dei dati digitali e l'articolo 17 sul ruolo e compiti del Responsabile

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Artikel 17 über die Rolle und Aufgaben des Verantwortlichen für den Digitalen Wandel (RTD);

della Trasformazione Digitale (RTD);

Landesgesetz vom 8. November 1982, Nr. 33 in geltender Fassung zur Regelung der Maßnahmen im Zusammenhang mit der Datenverarbeitung der Autonomen Provinz Bozen - Südtirol;

Legge provinciale dell'8 novembre 1982, n. 33 e successive modifiche, che regola i provvedimenti in materia di informatica della Provincia autonoma di Bolzano - Alto Adige;

Beschluss der Landesregierung vom 30. Jänner 2018, Nr. 85 mit Betreff „Ernennung des Direktors der Abteilung Informatik als Verantwortlichen für den digitalen Wandel (RTD) laut Art. 17 des Kodex für die digitale Verwaltung (CAD)“; laut AgID-Richtlinien muss der RTD u.a. Maßnahmen setzten, die zur Digitalisierung der Verwaltungen führen, um der gesamten Bevölkerung die Nutzung der digitalen Dienste zu ermöglichen;

Delibera della Giunta provinciale del 30 gennaio 2018, n. 85 avente ad oggetto “Nomina del Direttore della Ripartizione Informatica quale responsabile della trasformazione digitale (RTD) ai sensi dell'art.17 del Codice dell'Amministrazione Digitale (CAD)”; secondo le linee guida di AgID, il RTD deve adottare misure necessarie per la digitalizzazione delle amministrazioni, per consentire a tutta la popolazione di fruire dei servizi digitali;

Beschluss der Landesregierung vom 20. April 2021, Nr. 342, mit Betreff „Erweiterung des Wirkungsbereichs des Verantwortlichen für den digitalen Wandel (RTD) auf die kontrollierten Körperschaften“;

Delibera della Giunta provinciale del 20 aprile 2021, n. 342, avente ad oggetto “Estensione dell'ambito di azione del responsabile della transizione digitale (RTD) agli enti strumentali”;

Beschluss der Landesregierung vom 29. März 2022, Nr. 202, mit welchem die Digitale Agenda Südtirol Digital 2022-2026 genehmigt wurde, welche unter anderem das strategische Ziel „IKT-Infrastruktur“ und insbesondere das IKT-Ziel „Cybersecurity“ vorsieht;

Delibera della Giunta provinciale 29 marzo 2022, n. 202, con la quale è stata approvata l’Agenda Digitale dell’Alto Adige 2022-2026, che prevede, tra l’altro, l’obiettivo strategico “Infrastrutture ICT” e l’obiettivo ICT “cybersecurity”;

Beschluss der Landesregierung vom 5. Juli 2022, Nr. 470, über den Strategischen IKT-Plan 2022-2026, womit u.a. transversale Vorhaben zugunsten der Cybersecurity (PICT 1.3) genehmigt wurden;

Delibera della Giunta provinciale del 5 luglio 2022, n. 470 riguardante il Piano strategico ICT 2022-2026, che approva interventi a favore della Cybersecurity (PICT 1.3);

Beschluss der Landesregierung vom 1. August 2023, Nr. 647, u.a. betreffend die Definition der Kompetenzzentren, die sich auf die AgID-Vorgaben (Agentur für das digitale Italien, CAP7.PA.LA21)

Delibera della Giunta provinciale 1°agosto 2023, n. 647, che riguarda tra l’altro la definizione dei centri di competenza, sulla base delle linee guida AgID (Agenzia per l'Italia Digitale,

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

stützt, wonach ab Januar 2023 Provinzen und Großstädte Zentren für Innovation einrichten sollen, um den digitalen Transformationsprozess der lokalen Behörden in ihrem Gebiet zu fördern;

CAP7.PA.LA21), secondo la quale, a partire da gennaio 2023, le province e le grandi città dovrebbero creare centri per l'innovazione per sostenere il processo di trasformazione digitale degli enti locali del proprio territorio;

Beschluss der Landesregierung vom 26. Oktober 2021, Nr. 899, mit welchem die Innovationsstrategie 2030 (RIS3-Strategie) der Provinz Bozen, die u.a. auch das Thema Digitalisierung und Nachhaltigkeit, sowie die Cybersecurity aufgreift, genehmigt wurde;

Delibera della Giunta provinciale 26 ottobre 2021, n. 899, con la quale è stata approvata la Strategia di Innovazione 2030 (Strategia RIS3) della Provincia di Bolzano, che, tra le altre cose, affronta anche il tema della digitalizzazione e della sostenibilità, nonché la cybersicurezza;

Beschluss der Landesregierung vom 9. Mai 2023, Nr. 370 zur Genehmigung des PNRR-Projektes CERT für Südtirol (CUP B59E22000110006) mit dem Ziel innerhalb 2024 eine Analyse des aktuellen Stands der Cybersicherheit und Ausarbeitung eines mittel- bis langfristigen Plans zur Verbesserung der Cybersicherheit durchzuführen. Das Projekt wurde auf Grundlage der öffentlichen Bekanntmachung Nr. 3/2022, die am 2. August 2022 von der ACN zur Einreichung von Vorschlägen für Maßnahmen zur Verbesserung der Cybersicherheit im Rahmen des PNRR, Mission 1, Komponente 1, Investition 1.5 „Cybersicherheit“ veröffentlicht wurde, finanziert;

Delibera della Giunta provinciale 9 maggio 2023, n. 370 con la quale è stato approvato il progetto PNRR CERT territoriale dell'Alto Adige (CUP B59E22000110006) con l'obiettivo di elaborare un'analisi della postura di cybersicurezza attuale e di un piano di potenziamento in cybersicurezza a medio lungo termine. Il progetto è stato finanziato in base alla proposta presentata nell'ambito dell'Avviso Pubblico n. 3/2022 pubblicato in data 2 agosto 2022 da parte di ACN per la presentazione di proposte di interventi di potenziamento della resilienza cyber a valere sul PNRR, Missione 1, Componente 1, Investimento 1.5 “Cybersecurity”;

Beschluss der Landesregierung vom 27. Februar 2024, Nr. 83, mit welchem die Realisierung des PNRR-Projektes CERT-II genehmigt wurde, mit dem Ziel bis Ende 2025 das Computer Emergency Response Team Südtirol zu stärken, damit alle öffentlichen Verwaltungen im Land, bei einer Reihe von Cybersicherheitsdiensten unterstützt werden können. Das Projekt wurde auf der Grundlage des im Rahmen der am 11. August 2023 von ACN veröffentlichten öffentlichen Bekanntmachung Nr. 6/2023, eingereichten Projektes finanziert, für die Durchführung von Investitionen, die

Delibera della Giunta provinciale 27 febbraio 2024, n. 83, con la quale è stata approvata la realizzazione del progetto PNRR CERT-II con l'obiettivo di rafforzare il Computer Emergency Response Team dell'Alto Adige affinché possa supportare tutte le pubbliche amministrazioni del territorio in una serie di servizi di cyber sicurezza, entro la fine del 2025. Il progetto è stato finanziato in base alla proposta presentata nell'ambito dell'Avviso Pubblico n. 6/2023 pubblicato in data 11 Agosto 2023 da parte di ACN per l'attuazione di investimenti finalizzati al rafforzamento delle capacità tecniche nazionali in

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

auf die Stärkung der nationalen technischen Kapazitäten bei der Verhinderung und Behebung von Cybervorfällen abzielen und zwar durch die Aktivierung von Cyber-Notfallteams, die sich mit der Bewältigung von Cybervorfällen und Angriffen auf ihre Informationssysteme befassen, im Rahmen der Mission 1, Komponente 1, Investition 1.5 „Cybersicherheit“;

materia di prevenzione e risoluzione di incidenti cyber, mediante l’attivazione di squadre di pronto intervento informatico deputate alla gestione degli incidenti e degli attacchi informatici sui propri sistemi informativi, investimenti a valere sul PNRR, Missione 1, Componente 1, Investimento 1.5 “Cybersecurity;

stellt fest, dass

constata che,

die strategische IKT-Planung und Steuerung der digitalen Transformation für das Land in den Zuständigkeitsbereich des Verantwortlichen für den digitalen Wandel (RTD) gemäß Artikel 17 des CAD und der Beschlüsse der Landesregierung Nr. 85/2018 und Nr. 342/2021 fallen;

la pianificazione strategica ICT e la gestione della trasformazione digitale per la Provincia rientrano nelle competenze del Responsabile della Trasformazione Digitale (RTD) ai sensi dell'articolo 17 del CAD e delle delibere della Giunta provinciale n. 85/2018 e n. 342/ 2021;

die Cybersicherheit für öffentliche Verwaltungen in Südtirol sowohl auf strategischer als auch auf operativer Ebene eine Gesamtvision erfordert;

la sicurezza informatica per le pubbliche amministrazioni in Alto Adige necessità di una visione d’insieme sia a livello strategico che operativo;

zu diesem Zweck zwei Organisationsmodelle entwickelt wurden, die im Anhang ‘Cyber-Sicherheits-Governance’ zusammengefasst sind, welcher wesentlicher Bestandteil des vorliegenden Beschlusses ist;

per tale scopo sono stati sviluppati due modelli organizzativi sintetizzati nell’allegato “Cyber Sicurezza Governance” costituente parte integrante della presente deliberazione;

das strategische Organisationsmodell für die Cyber-Sicherheits-Governance in Südtirol, die Organisationsstruktur beschreibt und folgende Organe vorsieht:

- Strategischer Ausschuss für Cyber-Sicherheit
- Kompetenzzentrum für die Cyber-Sicherheit
- Öffentliche Körperschaften des Landes und deren Referent für Cybersicherheit und technischer Referent für Informationssicherheit;
- Anbieter von zentralisierten Cybersicherheitsdiensten;

il modello organizzativo strategico per la governance della cyber sicurezza in Alto Adige descrive la struttura organizzativa e prevede i seguenti organi:

- Comitato Strategico Cybersecurity
- Competence Center per la Cybersicurezza
- Enti Pubblici Provinciali e il loro Referente per la Cybersicurezza e Referente tecnico di Sicurezza Informatica
- Fornitori di Servizi Centralizzati di Cybersicurezza;

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

das operative Organisationsmodell des landesweiten CSIRT (Computer Security Incident Response Team) Südtirol, das in der landeseigenen Gesellschaft Südtiroler Informatik (SIAG) angesiedelt ist, folgende Organe vorsieht:
- CSIRT-AA Kernteam
- CSIRT-AA Manager
- Technisches CSIRT-AA Team

das strategische Organisationsmodell für die Cyber-Sicherheit-Governance des Landes und jenes des landesweiten CSIRT Südtirol sorgfältig aufeinander abgestimmt sind, sodass eine ständige Integration und Zusammenarbeit gewährleistet ist. Diese Abstimmung ermöglicht eine klare Verteilung der Verantwortlichkeiten und eine effiziente Kommunikation zwischen den verschiedenen Akteuren.

All dies vorausgeschickt wird weiters festgestellt, dass

durch den vorliegenden Beschluss keine direkten Kosten zu Lasten des Landeshaushaltes entstehen, da er ausschließlich auf die Genehmigung des Organisationsmodells für die Cybersicherheit in der Autonomen Provinz Bozen abzielt, während die Umsetzung desselben mit nachträglichen Akten durch den Direktor der Abteilung Informatik erfolgt;

die zuständige Organisationsstruktur bescheinigt, dass mit dieser Verwaltungsmaßnahme kein öffentliches Investitionsprojekt finanziert wird;

Dies vorausgeschickt,

b e s c h l i e ß t

DIE LANDESREGIERUNG

il modello organizzativo operativo del CSIRT (Computer Security Incident Response Team) provinciale dell'Alto Adige, istituito nella società in-house Informatica Alto Adige (SIAG), prevede i seguenti organi:
- Core Team del CSIRT-AA
- CSIRT-AA Manager
- Team Tecnico del CSIRT-AA

il modello strategico per la governance della sicurezza informatica del territorio e quello operativo del CSIRT-AA sono attentamente coordinati, sicché è garantita un'integrazione e una collaborazione continua. Questo coordinamento consente una chiara distribuzione delle responsabilità e una comunicazione efficiente tra i vari attori.

Tutto ciò premesso, si considera inoltre che

la presente deliberazione non comporta oneri diretti a carico del bilancio provinciale, in quanto è finalizzata esclusivamente all'approvazione del modello organizzativo per la Cybersicurezza nella Provincia autonoma di Bolzano, mentre l'attuazione dello stesso avverrà con successivi atti a cura del Direttore della Ripartizione Informatica;

la competente struttura organizzativa attesta che con il presente provvedimento non si finanzia un progetto d'investimento pubblico;

Ciò premesso,

LA GIUNTA PROVINCIALE

d e l i b e r a

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

einstimmig in gesetzmäßiger Weise

1. das diesem Beschluss als integrierende Bestandteile beigelegte Organisationsmodell für die Cybersicherheit in der Autonomen Provinz Bozen zu genehmigen,

2. den Direktor der Abteilung Informatik in seiner Eigenschaft als Verantwortlicher für den Digitalen Wandel (RTD) mit der Umsetzung des Organisationsmodells laut Punkt 1 sowie insbesondere mit folgenden Aufgaben zu betrauen:
   a. Aufbau des Kompetenzzentrums für Cybersicherheit;
   b. Beauftragung der In-House Gesellschaft mit der Umsetzung der organisatorischen Maßnahme CSIRT-Südtirol;
   c. Unterstützung der Zusammenarbeit zwischen den beteiligten Stakeholdern;

3. den Direktor der Abteilung Informatik in seiner Eigenschaft als Verantwortlicher für den Digitalen Wandel (RTD) im Sinne von Art. 8 Abs. 2 und 3 des Gesetzes Nr. 90/2024 als Referenten für die Cybersicherheit der Autonomen Provinz Bozen zu bestimmen und diesem gleichzeitig die mittels eigenem Dekret vorzunehmende Möglichkeit der Delegierung dieser Funktion einzuräumen;

4. die Abteilung Informatik anzuweisen, der Nationalen Agentur für Cybersicherheit den

a voti unanimi legalmente espressi

1. di approvare il modello organizzativo per la Cybersicurezza nella Provincia autonoma di Bolzano, come da allegati costituenti parte integrante della presente deliberazione;

2. di incaricare il Direttore della Ripartizione Informatica, nella sua qualità di Responsabile della transizione digitale (RTD), con l'attuazione del modello organizzativo di cui al punto 1 e di affidargli in particolare i seguenti compiti:
   a. istituire il Centro di competenza per la Cybersicurezza;
   b. incaricare la società in-house SIAG con l'attuazione dell'atto organizzativo per il CSIRT-Alto Adige;
   c. facilitare la collaborazione tra gli stakeholder coinvolti;

3. di individuare, ai sensi dell'art. 8 co. 2 e 3 della Legge n. 90/2024, il Direttore della Ripartizione Informatica, nella sua qualità di Responsabile della transizione digitale (RTD), quale referente per la cybersicurezza della Provincia autonoma di Bolzano ed al contempo conferirgli la facoltà di delegare tale funzione con proprio decreto;

4. di incaricare la Ripartizione Informatica a comunicare il nominativo del referente per la

Namen des Referenten für Cybersicherheit der Autonomen Provinz Bozen mitzuteilen.

cybersicurezza della Provincia autonoma di Bolzano all'Agenzia per la cybersicurezza nazionale.

DER LANDESHAUPTMANN

IL PRESIDENTE DELLA PROVINCIA

DER GENERALSEKRETÄR DER L.R.

IL SEGRETARIO GENERALE DELLA G.P.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Cyber-Sicherheits-Governance Autonome Provinz Bozen-Südtirol

1. Einführung

Das vorliegende Dokument ist wesentlicher Bestandteil des Beschlusses der Landesregierung Nr. X vom XX.XX.2025 und stellt einen grundlegenden Schritt zur Stärkung der digitalen Resilienz der Autonomen Provinz Bozen dar. Es gewährleistet eine effektive Verwaltung der IT-Systeme und der Cyber-Sicherheits-Risiken durch eine neue, bereichsübergreifende IKT-Governance, die alle öffentlichen Einrichtungen Südtirols einbezieht.

Das Ziel ist es, einen umfassenden Überblick über das Thema der IT-Sicherheit für die öffentlichen Verwaltungen in Südtirol zu entwickeln. Zu diesem Zweck wurden folgende zwei miteinander verbundene und integrierte Organisationsmodelle entwickelt:

1. Organisationsmodell des Competence Center für die Cyber-Sicherheits-Governance in Südtirol, welches die Organisationsstruktur für die Governance der Cyber-Sicherheit der Autonomen Provinz Bozen-Südtirol und der beitretenden / beigetretenen öffentlichen Einrichtungen im Allgemeinen beschreibt;

2. Organisationsmodell des landesweiten CSIRT Südtirol (CSIRT-AA), das die operative Organisationsstruktur des Teams für die Reaktion auf Sicherheitsvorfälle (Computer Security Incident Response Team), das von der Autonomen Provinz Bozen mit der operativen Unterstützung der landeseigenen Gesellschaft Südtiroler Informatik (SIAG) eingerichtet wurde, beschreibt.

2. Zusammenfassung des rechtlichen Rahmens

Richtlinie NIS 2, erlassen von der Europäischen Union am 17. Januar 2023 und muss von allen EU-Mitgliedstaaten bis zum 17. Oktober umgesetzt werden. Führt strenge Anforderungen an das Risikomanagement ein und erweitert den Anwendungsbereich auf eine größere Anzahl von Sektoren.

Cyber Security Governance Provincia Autonoma di Bolzano Alto Adige

1. Introduzione

Il presente documento costituisce parte integrante della delibera di Giunta n. X del XX.XX.2025 e rappresenta un passo fondamentale per rafforzare la resilienza digitale della Provincia Autonoma di Bolzano, garantendo una gestione efficace dei sistemi informatici e dei rischi di cybersecurity attraverso una nuova governance ICT trasversale che vedrà coinvolti tutti gli enti pubblici altoatesini.

L'obiettivo è sviluppare una visione d'insieme sul tema della sicurezza informatica per le pubbliche amministrazioni in Alto Adige. A tal fine, sono stati sviluppati i seguenti due modelli organizzativi interconnessi e integrati:

1. Modello organizzativo del Competence Center per la Cyber Security Governance in Alto Adige che descrive in generale la struttura organizzativa per la governance della cybersecurity della Provincia Autonoma di Bolzano Alto Adige e degli enti pubblici provinciali aderenti;

2. Modello organizzativo del CSIRT Territoriale Alto Adige (CSIRT-AA), che descrive la struttura organizzativa operativa del Team di Risposta agli Incidenti di Sicurezza (Computer Security Incident Response Team) istituito dalla Provincia Autonoma di Bolzano con il supporto operativo della società in-house provinciale Informatica Alto Adige (SIAG).

2. Sintesi del contesto normativo

Direttiva NIS 2, emessa dall'Unione Europea, approvata il 17 gennaio 2023 con data di recepimento per tutti gli Stati membri dell'UE per il 17 ottobre 2024: Introduce requisiti stringenti per la gestione del rischio e amplia il campo di applicazione a un maggior numero di settori.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Gesetz Nr. 90/2024: Erfordert die Ernennung eines Referenten für Cybersicherheit mit spezifischen Kompetenzen. Es ist möglich, einen Referenten für Cybersicherheit zu benennen, der auch die Funktion eines Aggregators übernimmt.

Die Verpflichtung aus dem PNRR-Projekt ACN 1.5 CERT (Computer Emergency Respons Team) sieht die Implementierung eines landesweiten CSIRT (Computer Security Incident Response Team) für Südtirol vor. Dies beinhaltet die Schaffung eines Teams für die Reaktion auf IT-Sicherheitsvorfälle, das speziell für die Provinz zuständig ist, und zielt darauf ab, das Management und die Reaktion auf Cyber-Sicherheit-Vorfälle auf territorialer Ebene zu verbessern.

Legge n. 90/2024: Richiede la nomina di un referente per la cybersicurezza con competenze specifiche. È possibile designare un Referente per la Cybersicurezza che svolga anche la funzione di aggregatore.

L'obbligo derivante dal progetto PNRR/ACN 1.5 CERT (Computer Emergency Respons Team) prevede l'implementazione del CSIRT (Computer Security Incident Response Team) in Alto Adige. Questo implica la creazione di un Team di risposta agli incidenti di sicurezza informatica specifico per la Provincia, con l'obiettivo di migliorare la gestione e la risposta agli incidenti di cybersecurity a livello territoriale.

3.
Referenzrahmen

Das Modell basiert auf dem NIST Cyber-Sicherheit Framework 2.0, das sechs Hauptfunktionen umfasst: Identify, Protect, Detect, Respond, Recover und Governance.

3.
Framework di Riferimento

Il modello si basa sul NIST Cybersecurity Framework 2.0, che comprende sei funzioni principali: Identify, Protect, Detect, Respond, Recover e Governance.

4.
Neue Digitale Governance

Für die Koordinierung der bereichsübergreifenden Governance wird eine eigene öffentliche Einrichtung gegründet. Die Interventionsbereiche der neuen digitalen Governance sind: Digital Strategy and Innovation, ICT Stewardship, Shared Services und Kompetenzzentren, wie im Beschluss der Landesregierung Nr. 647/2023 beschrieben.

4.
Nuova Governance Digitale

Per il coordinamento della governance trasversale sarà istituito un'apposito ente pubblico. Gli ambiti di intervento della nuova Governance digitale sono: Digital Strategy and Innovation, ICT Stewardship, Shared Services e Competence Centers come descritto nella delibera di Giunta n. 647/2023.

5.
Organisationsmodell für die Cybersicherheit

Das Organisationsmodell für die neue bereichsübergreifende IKT-Governance der Provinz sieht die Einrichtung eines Kompetenzzentrums für Cybersicherheit in Südtirol vor. Dieses Kompetenzzentrum wird im einfachen Anhang des vorliegenden Beschlusses der Landesregierung beschrieben.

Es wird vorausgeschickt, dass eine detaillierte Regelung zur Disziplinierung des Betriebs des Kompetenzzentrums entwickelt wird, welches in die neue Governance-Struktur integriert wird.

Nachfolgend sind die für den Betrieb zuständigen Organe aufgeführt:

5.
Modello Organizzativo per la Cybersecurity

Il modello organizzativo per la nuova governance ICT trasversale provinciale prevede l'istituzione di un competence center per la cybersicurezza in Alto Adige. Tale competence center viene descritto nell'allegato semplice della presente delibera della Giunta provinciale.

Si specifica che verrà sviluppato un regolamento dettagliato per disciplinare il funzionamento del Centro di Competenza, che sarà integrato nella nuova struttura di governance.

Di seguito sono elencati gli organi preposti al funzionamento:

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

5.1
Strategischer Ausschuss für Cybersicherheit

Der strategische Ausschuss definiert die Gesamtstrategie für die Cybersicherheit in der Autonomen Provinz Bozen Südtirol und steuert die notwendigen Initiativen für deren Umsetzung.

Mitglieder:
- Landeshauptmann/-Frau
- Landesrat-/Landesrätin für die Digitalisierung
- Verantwortlicher/Verantwortliche für den digitalen Wandel (RTD)
- Generaldirektor/in der Landesverwaltung
- Direktor/in des Ressorts für Bevölkerungsschutz/Zivilschutz
- Generaldirektor/in des Südtiroler Sanitätsbetriebes (SABES)
- Präsident/in des Gemeindenverbandes (GVCC)
- Generaldirektor/in des Südtiroler Wohnbauinstitutes (IPES)
- Generaldirektor/in der Südtiroler Informatik AG (SIAG)
- Generaldirektor/in der Infranet AG
- IT-Vertretung der Region Trentino Südtirol
- CSIRT-Manager/in
- sowie alle öffentlichen Körperschaften, die ausdrücklich darum ansuchen.

5.1
Comitato Strategico Cybersecurity

Il Comitato strategico definisce la strategia complessiva per la cybersecurity nella Provincia Autonoma di Bolzano Alto Adige e governa le iniziative necessarie per la sua implementazione.

Componenti:
- Presidente della Provincia
- Assessore competente in materia di digitalizzazione
- Responsabile per la Transizione Digitale (RTD)
- Direttore Generale dell'Amministrazione Provinciale
- Direttore del Dipartimento per la Protezione Civile
- Direttore Generale dell'Azienda Sanitaria Alto Adige (SABES)
- Presidente del Consorzio dei Comuni (GVCC)
- Direttore Generale dell'Istituto provinciale per l'Edilizia Sociale (IPES)
- Direttore Generale della Società Informatica Alto Adige (SIAG)
- Direttore Generale di Infranet s.p.a.
- Rappresentante IT della Regione Trentino-Alto Adige
- CSIRT Manager
- nonché tutti gli enti pubblici che ne fanno esplicita richiesta.

5.2
Kompetenzzentrum für Cybersicherheit

Das Kompetenzzentrum überwacht die Strategie zur Verwaltung von Cyber-Sicherheit-Risiken, indem es die Richtlinien, Modelle, Werkzeuge und Programme des Strategischen Ausschusses für die Cybersicherheit umsetzt.
Es steuert, koordiniert und überwacht die organisatorischen und technischen Maßnahmen zur Cybersicherheit sowie die Bereitstellung zentralisierter Cybersicherheitsdienste für die öffentlichen Einrichtungen des Landes.

Die Leitung des Kompetenzzentrums für Cybersicherheit wird vom Strategischen Ausschuss für Cybersicherheit ernannt.

Im Kompetenzzentrum für Cybersicherheit arbeiten der CSIRT-AA Manager, der Referent für Cybersicherheit und die technischen Referenten der öffentlichen Körperschaften mit.

5.2
Competence Center per la Cybersicurezza

Il Competence Center presidia la strategia per la gestione dei rischi di cybersecurity, attuando politiche, modelli, strumenti e programmi predisposti dal Comitato Strategico per la Cybersicurezza.
Esso governa, coordina e controlla i presidi organizzativi e tecnici di cybersecurity nonché le forniture di servizi centralizzati di cybersecurity agli Enti pubblici della Provincia.

La direzione del Centro di Competenza per la Cybersicurezza è nominata dal Comitato Strategico per la Cybersicurezza.

Nel Centro di Competenza per la Cybersicurezza collaborano il Manager del CSIRT-AA, il Referente per la Cybersicurezza e i referenti tecnici degli enti pubblici.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

5.3
Öffentliche Körperschaften des Landes

Die öffentlichen Körperschaften des Landes implementieren die Richtlinien und Prozesse der Cybersicherheit, passen die Vorgaben des Kompetenzzentrums für Cybersicherheit an ihren eigenen Kontext an und arbeiten im Kompetenzzentrum für Cybersicherheit zusammen.

Alle öffentlichen Körperschaften benennen:
- einen Referenten für Cybersicherheit (gemäß Gesetz Nr. 90/2024); diese Rolle kann an eine aggregierende Stelle delegiert werden;
- einen technischen Referenten für Informationssicherheit; dieser arbeitet mit dem technischen Team des CSIRT-AA zusammen.

5.3
Enti Pubblici Provinciali

Gli Enti pubblici provinciali implementano le politiche e i processi di cybersecurity, adattano le indicazioni del Competence Center per la Cybersicurezza al proprio contesto e collaborano nel Competence Center per la Cybersicurezza.

Tutti gli Enti pubblici nominano:
- un Referente per la cybersicurezza (ex Legge n. 90/2024); questo ruolo può essere delegato ad un soggetto aggregatore;
- un Referente Tecnico di Sicurezza Informatica; esso collabora al Team tecnico del CSIRT-AA.

5.4
Anbieter von zentralisierten Cybersicherheitsdiensten

Diese haben eine operative Rolle. Sie unterstützen und erbringen Cybersicherheits-dienste für alle öffentlichen Einrichtungen des Landes.

5.4
Fornitori di Servizi Centralizzati di Cybersecurity

Essi hanno un ruolo operativo, supportano ed erogano servizi di cybersecurity a tutti gli enti pubblici della Provincia.

6.
Organisationsmodell
Landesweites CSIRT Südtirol (CSIRT-AA)

Das CSIRT-AA (Computer Security Incident Response Team Südtirol) ist ein operatives Organ, das für alle beigetretenen öffentlichen Einrichtungen technische Dienstleistungen erbringt und zeitnahe Reaktionen auf Sicherheitsvorfälle gewährleistet. Die angebotenen technischen Dienstleistungen werden in die Grund-, Mittel- und Fortgeschrittene Stufe unterteilt. Für die Mittel- und Fortgeschritten Stufen fallen Gebühren an.

Das CSIRT-AA ist bei der Südtiroler Informatik AG (SIAG) angesiedelt und analysiert Cyberbedrohungen, löst Cyber-Sicherheit-Vorfälle, verbreitet Sicherheitsinformationen, fördert das Bewusstsein sowie best practice und arbeitet mit nationalen und internationalen Einrichtungen zusammen.

Nachfolgend sind die für den Betrieb zuständigen Organe aufgeführt:

6.
Modello Organizzativo
CSIRT Territoriale dell'Alto Adige (CSIRT-AA)

Il CSIRT-AA (Computer Security Incident Response Team Alto Adige) è un organo operativo che fornisce servizi tecnici e risposte tempestive agli incidenti per tutti gli enti pubblici aderenti. I servizi offerti sono suddivisi in tre livelli (base, intermedio e avanzato). Per il livello intermedio e avanzato si prevedono delle commissioni.

Inoltre, il CSIRT-AA, istituito presso la Società in-house provinciale Informatica Alto Adige, (SIAG) analizza minacce informatiche, risolve incidenti di cybersecurity, diffonde informazioni sulla sicurezza, promuove consapevolezza e best practice, e collabora con enti nazionali e internazionali.

Di seguito sono elencati gli organi preposti al funzionamento:

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

6.1
CSIRT-AA Kernteam

Das Kernteam besteht aus dem CSIRT-AA-Manager, dem Cybersicherheitsbeauftragten gemäß Gesetz Nr. 90/2024 und/oder einem Referenten bzw. Sprecher der dem CSIRT-AA angeschlossenen öffentlichen Einrichtung.

6.1
Core Team del CSIRT-AA

Il Core Team è composto dal CSIRT-AA Manager, dal Referente Cybersicurezza ex L. n. 90/2024 e/o comunque da un referente ovvero portavoce dell'ente pubblico aderente al CSIRT-AA.

6.2
CSIRT-AA Manager

Der CSIRT-AA Manager ist dafür verantwortlich, das territoriale Core Team zu koordinieren, um schnelle Reaktionen auf Vorfälle zu gewährleisten. Diese Person arbeitet mit den Mitgliedern des Kompetenzzentrums für Cybersicherheit zusammen und berichtet direkt an den strategischen Ausschuss für Cybersicherheit.

Der CSIRT-AA Manager wird vom Strategischen Ausschuss für Cybersicherheit ernannt und bei der landeseigenen Gesellschaft Südtiroler Informatica (SIAG) angesiedelt.

6.2
CSIRT-AA Manager

Il CSIRT-AA Manager è incaricato di coordinare il Core Team territoriale per assicurare risposte tempestive agli incidenti. Questa figura collabora con i membri del Competence Center per la Cybersicurezza e riferisce direttamente al Comitato strategico per la Cybersicurezza.

Il CSIRT-AA Manager sarà nominato dal Comitato strategico per la Cybersicurezza e collocato presso la Società in-house provinciale Informatica Alto Adige, (SIAG).

6.3
Technisches CSIRT-AA Team

Das technische Team, bestehend aus IT-Sicherheitsspezialisten der teilnehmenden öffentlichen Einrichtungen, ist für die operative Verwaltung von Vorfällen und die Bereitstellung der Dienste des CSIRT-AA zuständig. Es berichtet an den CSIRT-AA-Manager.

6.3
Team Tecnico del CSIRT-AA

Il Team Tecnico, composto da specialisti di sicurezza informatica degli enti pubblici aderenti, ha il compito di gestire operativamente gli incidenti e fornire i servizi del CSIRT-AA. Risponde al CSIRT-AA Manager.

7.
Schlussfolgerung

Das strategische Organisationsmodell für die Cyber-Sicherheit-Governance des Landes und jenes des landesweiten CSIRT Südtirol sind sorgfältig aufeinander abgestimmt, sodass eine ständige Integration und Zusammenarbeit gewährleistet ist. Diese Abstimmung ermöglicht eine klare Verteilung der Verantwortlichkeiten und eine effiziente Kommunikation zwischen den verschiedenen Akteuren.

Details zur Abstimmung und Koordination

Strategische und operative Ebenen:

- Die zukünftige neue transversale Governance-Struktur für den digitalen Wandel in Südtirol legt die strategischen Leitlinien und Ziele fest, die vom

7.
Conclusione

Il modello strategico per la governance della sicurezza informatica del territorio e quello operativo del CSIRT-AA sono attentamente coordinati per garantire un'integrazione e una collaborazione di continuità. Questo coordinamento consente una chiara distribuzione delle responsabilità e una comunicazione efficiente tra i vari attori.

Dettagli sul coordinamento e la collaborazione

Livelli strategici e operativi:

- La futura nuova struttura di governance trasversale per la trasformazione digitale in Alto Adige stabilisce le linee guida strategiche e gli obiettivi, che sono

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Strategischen Ausschuss für Cybersicherheit überwacht und vom Kompetenzzentrum für Cybersicherheit koordiniert werden;
- Das CSIRT-AA setzt diese strategischen Vorgaben operativ um, indem es konkrete Maßnahmen zur Bedrohungsanalyse und Incident-Management durchführt.

Rollen und Verantwortlichkeiten:
- Das Kompetenzzentrum für Cybersicherheit übernimmt die zentrale Rolle in der Definition und Überwachung der Cyber-Sicherheit-Strategie, während das CSIRT-AA als operatives Team fungiert, das direkt auf Sicherheitsvorfälle reagiert und technische Unterstützung bietet.
- Die öffentlichen Körperschaften und Anbieter von zentralisierten Cybersicherheitsdiensten arbeiten unter der Leitung des Kompetenzzentrum für Cybersicherheit und in enger Zusammenarbeit mit dem CSIRT-AA.

Kommunikation und Zusammenarbeit:
- Regelmäßige Treffen und Informationsaustausch zwischen dem Kernteam des CSIRT-AA und dem Kompetenzzentrum für Cybersicherheit stellen sicher, dass strategische Entscheidungen schnell und effektiv in operative Maßnahmen umgesetzt werden.
- Die technischen IKT-Referenten der verschiedenen öffentlichen Körperschaften fungieren als Bindeglied zwischen den zentralen und lokalen Einheiten, was eine reibungslose Implementierung der Cyber-Sicherheit-Politiken und -Prozesse gewährleistet.

Gemeinsame Ziele und Synergien:
- Beide Modelle verfolgen das gemeinsame Ziel, die Cyber-Sicherheit in der Provinz Bozen zu stärken und die Resilienz gegen Cyber-Bedrohungen zu erhöhen.
- Durch die abgestimmte Vorgehensweise werden Synergien geschaffen, die die Effektivität und Effizienz der Cyber-Sicherheit-Maßnahmen maximieren.

Diese enge Abstimmung und Koordination zwischen den beiden Modellen sorgt dafür, dass die Verwaltung der Cyber-Sicherheit in der Provinz Bozen nicht nur effektiv ist, sondern auch flexibel und anpassungsfähig auf neue Bedrohungen reagieren kann.

monitorati dal Comitato Strategico per la Sicurezza Informatica e coordinati dal Centro di Competenza per la Sicurezza Informatica;
- Il CSIRT-AA attua queste linee guida strategiche operativamente, implementando misure concrete per l'analisi delle minacce e la gestione degli incidenti.

Ruoli e responsabilità:
- Il Competence Center per la Cyber sicurezza assume il ruolo centrale nella definizione e nel monitoraggio della strategia di cybersecurity, mentre il CSIRT-AA funge da team operativo che risponde direttamente agli incidenti di sicurezza e fornisce supporto tecnico.
- Gli enti pubblici e i fornitori di servizi centralizzati di cybersecurity operano sotto la direzione del Competence Center per la Cybersicurezza e in stretta collaborazione con il CSIRT-AA.

Comunicazione e collaborazione:
- Incontri regolari e scambi di informazioni tra il Core Team del CSIRT-AA e il Competence Center per la Cybersicurezza garantiscono che le decisioni strategiche vengano rapidamente ed efficacemente trasformate in azioni operative.
- I referenti tecnici ICT delle varie amministrazioni pubbliche fungono da collegamento tra le unità centrali e locali, garantendo un'implementazione senza intoppi delle politiche e dei processi di cybersecurity.

Obiettivi comuni e sinergie:
- Entrambi i modelli perseguono l'obiettivo comune di rafforzare la cybersecurity nella Provincia di Bolzano e aumentare la resilienza contro le minacce informatiche.
- Grazie all'approccio coordinato, si creano sinergie che massimizzano l'efficacia e l'efficienza delle misure di cybersicurezza.

Questa stretta coordinazione e collaborazione tra i due modelli garantisce che la gestione della cybersecurity nella Provincia di Bolzano non sia solo efficace, ma anche flessibile e adattabile alle nuove minacce.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

CYBERSECURITY
IN DER AUTONOMEN PROVINZ BOZEN

Organisationsmodell

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Zusammenfassung

1. Einführung ... 3
1.1 Zielsetzung ... 3
1.2 Rechtlicher Rahmen ... 3
1.2.1 NIS-2-Richtlinie ... 3
1.2.2 Gesetz Nr. 90/2024 ... 3
1.3 Aufbau des Dokuments ... 4
2. Bezugsrahmen ... 5
3. Die neue digitale Governance ... 8
3.1 Organisationsmodell ... 8
3.2 Die Kompetenzzentren der Agentur ... 9
4. Organisationsmodell für die Cybersicherheit der APB und der Körperschaften des Landes ... 11
4.1 Akteure und Kategorien ... 11
4.1.1 Der Strategische Ausschuss für Cybersicherheit ... 11
4.1.2 Das Kompetenzzentrum für Cybersicherheit ... 12
4.1.3 Die Körperschaften des Landes ... 13
4.1.4 Zentralisierte Anbieter von Cybersicherheitsdiensten ... 13
4.2 Übersicht der wichtigsten Fachgebiete ... 14
4.3 Aufgaben in Bezug auf die NIS-2-Richtlinie und das Gesetz 90/2024 ... 15
4.4 Cyber-Modell Südtirol – Überblick ... 15
5. Kompetenzzentrum für Cybersicherheit ... 17
5.1 Die Rolle des Kompetenzzentrums im Allgemeinen ... 17
5.2 Die Rolle des Kompetenzzentrum innerhalb der künftigen Agentur ... 17
5.3 Zuständigkeiten ... 17
5.4 Aktivitäten ... 18
5.5 Die Kontaktperson des Kompetenzzentrums ... 19
6. Körperschaften des Landes ... 19
7. CSIRT-AA ... 20

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

1. Einführung

1.1 Zielsetzung

Ziel dieses Dokuments ist es, u.a. im Zusammenhang mit der Agentur Südtirol Digital und einer einheitlichen Strategie für den digitalen Wandel auf Landesebene, einen **Überblick** und die **Beschreibung des Organisationsmodells für Cybersicherheit** (im Folgenden auch „**Cyber-Modell Südtirol**“) der Autonomen Provinz Bozen und der öffentlichen Verwaltung und gleichgestellten öffentlichen Einrichtungen, die auf dem Gebiet der Provinz ansässig oder tätig sind (im Folgenden auch „**Einrichtungen**“), zu entwickeln.

1.2 Rechtlicher Rahmen

1.2.1 NIS-2-Richtlinie

Mit der Richtlinie (EU) 2022/2555 („NIS-2-Richtlinie“) des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes **gemeinsames Cybersicherheitsniveau** in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972, wird die Richtlinie (EU) 2016/1148 („NIS-Richtlinie“) aufgehoben.

Die NIS-Richtlinien wurden geschaffen, um die Sicherheit von Netzen und Informationssystemen in der Europäischen Union zu verbessern, indem die **Betreiber wesentlicher Dienste** verpflichtet werden, **die digitale Resilienz** ihrer Infrastrukturen zu **gewährleisten.**

Die NIS-2-Richtlinie erweitert die Bestimmungen der **NIS-Richtlinie, indem sie strengere Anforderungen** an das Risikomanagement **einführt, den Anwendungsbereich auf weitere Sektoren ausweitet** und die Verantwortlichkeiten der Leiter:innen der Einrichtungen, für die sie gilt, erhöht. Die NIS-2-Richtlinie gilt insbesondere für die **zentrale und lokale öffentliche Verwaltung** und führt **Verpflichtungen für die öffentlichen Verwaltungen** und die **Behörden des Landes in Bezug auf Cybersicherheit** ein.

1.2.2 Gesetz Nr. 90/2024

Das Gesetz Nr. 90 vom 28. Juni 2024 („Gesetz Nr. 90/2024“) ist ein wichtiger italienischer Rechtsakt, in dem der rechtliche Rahmen für **Cybersicherheit und digitale Widerstandsfähigkeit in der öffentlichen Verwaltung** aktualisiert wurde.

Insbesondere schreibt das Gesetz Nr. 90/2024 vor, dass öffentliche Einrichtungen eine **Struktur für Cybersicherheit festlegen** und eine **„Kontaktperson für Cybersicherheit“ benennen** müssen, die nachweislich über eine besondere Fachkompetenz und Sachkenntnis in Fragen der Cybersicherheit verfügt und die der italienischen Agentur für Cybersicherheit („ACN“) namentlich bekannt sein muss.

Der Vollständigkeit halber sei angemerkt:

- Die öffentlichen Einrichtungen können *„das Amt der Kontaktperson für Cybersicherheit einer:m Bediensteten der öffentlichen Verwaltung übertragen, vorbehaltlich einer zuvor erteilten Genehmigung*

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

gemäß Artikel 53 des gesetzesvertretenden Dekrets Nr. 165 vom 30. März 2001 und im Rahmen der nach den geltenden Rechtsvorschriften verfügbaren Mittel". [Gesetz 90/2024 Art. 8.2]

- *„Die Struktur und die Kontaktperson [...] können in der Geschäftsstelle bzw. bei der:m Verantwortlichen für den digitalen Wandel gemäß Artikel 17 der Gesetzesvorschriften zur digitalen Verwaltung, auf die im gesetzesvertretenden Dekret Nr. 82 vom 7. März 2005 Bezug genommen wird, bestimmt werden.*" [Gesetz 90/2024 Art. 8.2]
- *„Die unter 1 und 2 genannten Aufgaben können gemäß den Bestimmungen von Artikel 17, Absatz 1 -sexies und 1 -septies des im gesetzesvertretenden Dekret Nr. 82 vom 7. März 2005 genannten Regelwerks **im Verbund miteinander** ausgeübt werden.*" [Gesetz 90/2024 Art. 8.4].

Gesetzesvertretendes Dekret Nr. 82 vom 7. März 2005, Absatz 1 -sexies: Im Einklang mit ihrer organisatorischen Autonomie bestimmen die öffentlichen Verwaltungen, die keine staatlichen Verwaltungen sind, die in Absatz 1 genannte digitale Geschäftsstelle aus den Reihen der Führungsebene oder benennen, falls sie über keine solche verfügen, eine:n Verantwortliche:n für digitale Angelegenheiten aus den Reihen der leitenden Angestellten. Sofern keine politische Führung vorliegt, ist die:der Verantwortliche der in Absatz 1 genannten digitalen Geschäftsstelle direkt der Verwaltungsleitung der Einrichtung unterstellt.

Gesetzesvertretendes Dekret Nr. 821 vom 7. März 2005, Absatz -septies: Die in Absatz 1 -sexies genannten Einrichtungen können die im selben Absatz genannten Funktionen auch im Verbund miteinander ausüben. Dies gilt unbeschadet des Rechts, die Unterstützung interner Unternehmen durch entsprechende Vereinbarungen und ohne neue oder größere Belastungen für die öffentlichen Finanzen in Anspruch zu nehmen.

Am 26. November 2024 wurden auf dem ACN-Portal auch die „**Leitlinien zur Stärkung der Resilienz der in Artikel 1, Absatz 1 des Gesetzes Nr. 90 vom 28. Juni 2024 genannten Einrichtungen**" („ACN-Leitlinien") veröffentlicht. Sie stellen den ersten operativen Schritt dar, um die zusätzlichen neuen Anforderungen an Einrichtungen der öffentlichen Verwaltung im Bereich der Cybersicherheit zu erfüllen. In den ACN-Leitlinien werden 26 Sicherheitsmaßnahmen genannt, die in etwa 100 Durchführungskontrollen unterteilt sind, die die Anforderungen an **das Land und den Körperschaften des Landes** weiter erhöhen werden.

1.3 Aufbau des Dokuments

In diesem Dokument werden die Konzepte, Kriterien und Leitlinien vorgestellt, nach denen das **Cyber-Modell Südtirol** entwickelt wurde:

- der Bezugsrahmen,
- die neue digitale Governance,
- das Organisationsmodell für die Cybersicherheit des Landes und ihrer Körperschaften („**Cyber-Modell Südtirol**"),
- das Kompetenzzentrum für Cybersicherheit,
- das CSIRT-AA

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

2. Bezugsrahmen

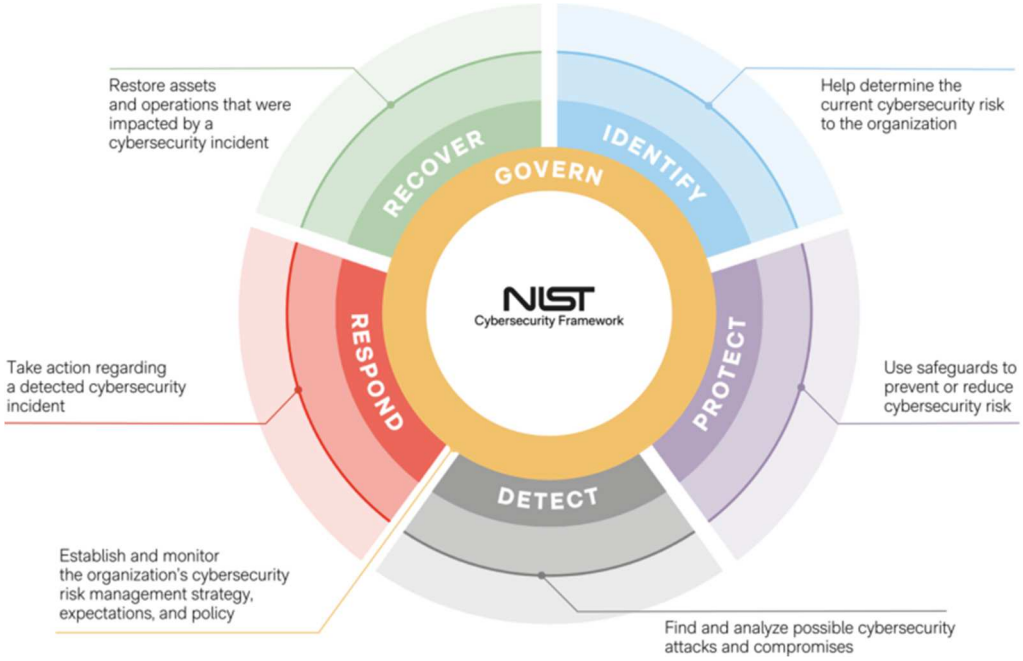
Um die Beschreibung des Cyber-Modell Südtirol solide und systematisch zu strukturieren, wurde das **NIST Cybersecurity Framework 2.0**[1] **(„CSF 2.0“)** als methodischer Bezugsrahmen verwendet, der eine Auflistung und Zuordnung der Funktionen und Prozesskategorien ermöglicht, die erforderlich sind, um eine angemessene Steuerung, Kontrolle und Verwaltung von Cybersicherheitsrisiken zu gewährleisten. Der CFS-2.0-Rahmen ermöglicht die Erstellung einer klaren Übersicht der Zuständigkeiten und erleichtert die Zusammenarbeit zwischen den Akteur:innen und eine strategische Koordinierung der Cybersicherheit. Zu den Vorteilen dieses methodischen Rahmens gehören:

- die Verringerung von Überschneidungen oder Lücken in den Zuständigkeiten,
- die Abstimmung der Sicherheitsziele mit den Zielen der öffentlichen Verwaltung,
- die Weiterentwicklung hin zu einem widerstandsfähigen und proaktiven Organisationsmodell.

Der Rahmen bietet:

- **Hauptfunktionen:** sechs Funktionen (Identifizieren, Schützen, Erkennen, Reagieren, Wiederherstellen und Governance), die den gesamten Zyklus des Cybersicherheitsmanagements abbilden,
- **Kategorien und Unterkategorien:** Jede Funktion ist in Kategorien und Unterkategorien unterteilt, für die bestimmte Aktivitäten identifiziert werden.

[1] Das CSF 2.0 ist eine Aktualisierung des bewährten, vom US National Institute of Standards and Technology (NIST) entwickelten Cybersicherheits-Rahmenwerks. Die im Jahr 2024 veröffentlichte Version 2.0 stellt eine erhebliche Verbesserung gegenüber der ursprünglichen Version von 2014 (und dem nachfolgenden Update 1.1 aus dem Jahr 2018) dar und passt sich den neuen Anforderungen der globalen digitalen Landschaft und den aufkommenden Cybersicherheitsherausforderungen an.



Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Im Folgenden werden die Funktionen des CFS 2.0 zusammengefasst, um einen Anhaltspunkt für die Elemente zu geben, die bei der **Erstellung eines Betriebsmodells für die Cybersicherheit** zu berücksichtigen sind, das durch das entsprechende Organisationsmodell mit der Bezeichnung „**Cyber-Modell Südtirol**“ (s. oben) umgesetzt werden soll.

GOVERN (GV)	Organizational Context (GV.OC)
	Risk Management Strategy (GV.RM)
	Roles, Responsibilities, and Authorities (GV.RR)
	Policy (GV.PO)
	Oversight (GV.OV)
	Cybersecurity Supply Chain Risk Management (GV.SC)
IDENTIFY (ID)	Asset Management (ID.AM)
	Risk Assessment (ID.RA)
	Improvement (ID.IM)
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AA)
	Awareness and Training (PR.AT)
	Data Security (PR.DS)
	Platform Security (PR.PS)
	Technology Infrastructure Resilience (PR.IR)
DETECT (DE)	Continuous Monitoring (DE.CM)
	Adverse Event Analysis (DE.AE)
RESPOND (RS)	Incident Management (RS.MA)
	Incident Analysis (RS.AN)
	Incident Response Reporting and Communication (RS.CO)
	Incident Mitigation (RS.MI)
RECOVER (RC)	Incident Recovery Plan Execution (RC.RP)
	Incident Recovery Communication (RC.CO)

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

- **Governance** – stellt die strategische Rolle der Cybersicherheit in der Unternehmensführung dar, um sicherzustellen, dass die Cybersicherheit in die Entscheidungsprozesse integriert wird und das Risikomanagement auf Führungsebene unterstützt wird.
- **Identify** – konzentriert sich auf das Verständnis des Kontexts, der kritischen Ressourcen und der damit verbundenen Risiken, um ein Bild davon zu erstellen, was geschützt werden muss und welche Schwachstellen vorliegen.
- **Protect** – betrifft die Umsetzung von Maßnahmen zum Schutz von IKT-Informationen, -Systemen und -Diensten und zur Verbesserung der digitalen Widerstandsfähigkeit.
- **Detect** – konzentriert sich auf die Fähigkeit, Sicherheitsvorfälle sofort zu erkennen, um Anomalien und potenzielle Gefährdungen rechtzeitig zu entdecken und effektiv darauf zu reagieren.
- **Respond** – definiert die Maßnahmen, die im Umgang mit einem IT-Vorfall nach seiner Entdeckung erforderlich sind, um Schäden zu begrenzen und die Sicherheit wiederherzustellen, Vorfälle einzudämmen und ihre Auswirkungen zu minimieren.
- **Recover** – konzentriert sich auf die Wiederherstellung der Betriebsabläufe und der Widerstandsfähigkeit nach einem Vorfall, um gefährdete Ressourcen und den normalen Betrieb schnell wiederherzustellen und die langfristigen Auswirkungen zu minimieren.

3. Die neue digitale Governance

3.1 Organisationsmodell

Die Autonome Provinz Bozen hat **ein neues Modell der digitalen Governance („New Digital Governance“)** eingeführt, das die Schaffung der**Agentur Südtirol Digital** („Agentur“) umfasst.

Diese Agentur wird eingerichtet, um eine einheitliche Strategie für den digitalen Wandel auf Landesebene zu formulieren und umzusetzen. Dabei werden die Ziele der Effektivität, Effizienz, Unparteilichkeit und Vereinfachung verfolgt und auf der Grundlage der Prinzipien der Subsidiarität, Transparenz und Kosteneffizienz gearbeitet.

Auch im Bereich der Cybersicherheit ist die Agentur Südtirol Digital für die politische Entscheidungsfindung, die Festlegung der entsprechenden Ziele auf Landesebene, die Definition und Steuerung der Strategie und deren Umsetzung durch die Koordinierung von Initiativen, Aktionen und Synergien zuständig, um deren Umsetzung zu ermöglichen.

Die künftige neue Agentur agiert daher im Governance-Bereich, indem sie einerseits mit dem Land und den Körperschaften des Landes (*Business Domain*) und andererseits mit den IKT-Dienstleistern (*ICT Service Provider Domain*) zusammenarbeitet.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

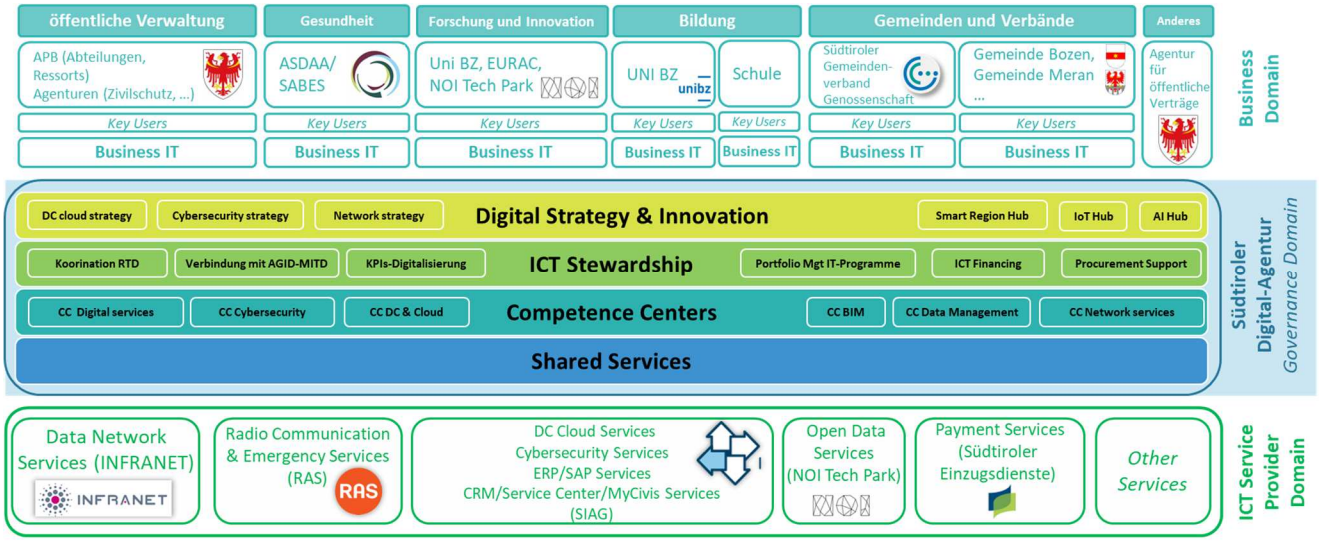


ABBILDUNG1 – DIE NEUE DIGITALE VERWALTUNG UND DIE AGENTUR SÜDTIROL DIGITAL

3.2 Die Kompetenzzentren der Agentur

Die Agentur ist in vier Hauptbereiche unterteilt:

- Digital Strategy and Innovation
- ICT Stewardship
- Shared Services
- Competence Centers

Das Funktionsmodell der Fachkompetenzzentren (im Folgenden auch „Kompetenzzentren“) kann als „graue Box“ angesehen werden, die die verschiedenen Dienste umfasst, die das Kompetenzzentrum benötigt, um operative Richtlinien für die Service Provider zu formulieren, die es ihnen ermöglichen, technologische Dienste anzubieten, die mit der Strategie und den Bedürfnissen der Stakeholder übereinstimmen.

Die Einrichtung eines Kompetenzzentrums beginnt mit der Ermittlung der angebotenen Dienstleistungen, der Kontaktstellen mit den Organisationen (Input), des Interventionsbereichs/der Kompetenzen (Beschränkung) und der Produkte der angebotenen Dienstleistungen (Output), die die Variablen des Modells darstellen.

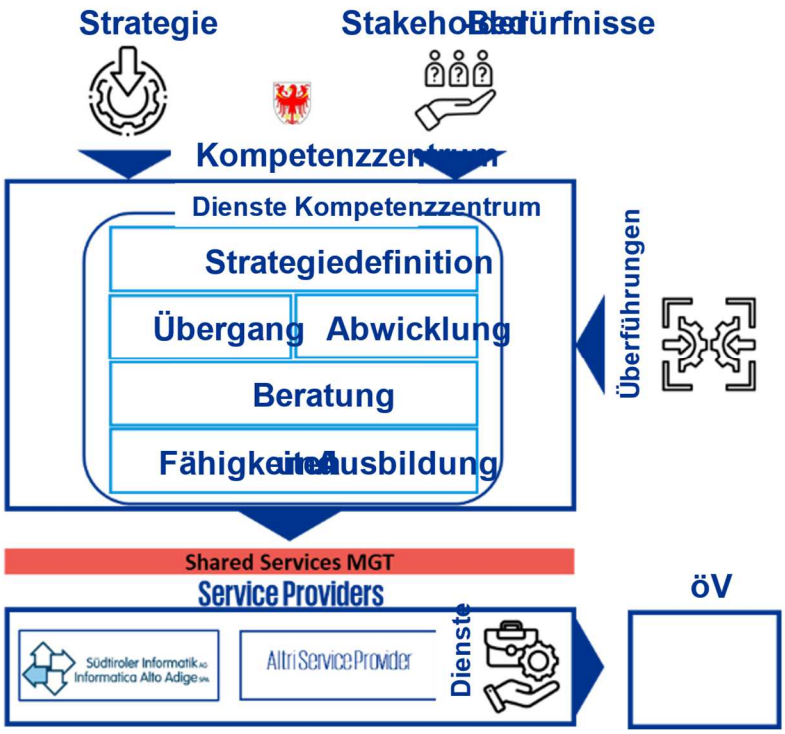


ABBILDUNG2 – SYSTEM DER KOMPETENZZENTREN

Im Zuge der Schaffung der neuen digitalen Governance hat das Land der Organisation eines trasversalen **Kompetenzzentrums für die Cybersicherheit in Südtirol („Kompetenzzentrum“)** eine hohe Priorität eingeräumt. Im Folgenden wird erläutert, wie das Kompetenzzentrum im Rahmen der Agentur Südtirol Digital eine zentrale Rolle im **Cyber-Modell Südtirol** spielt.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

4. Organisationsmodell für die Cybersicherheit der APB und der Körperschaften des Landes

4.1 Akteure und Kategorien

Das Cyber-Modell Südtirol sieht die folgenden Rollen-Kategorien vor, die den verschiedenen Akteuren zugeordnet sind:

- **Strategische Ebene – neue Governance:**
  - **Strategischer Ausschuss für Cybersicherheit**
  - **Kompetenzzentrum für Cybersicherheit**
  - **beteiligte öffentliche Einrichtungen des Landes**
  - **Anbieter von zentralisierten Cybersicherheitsdiensten**
- **Operative Ebene: CSIRT-AA**

4.1.1 Der Strategische Ausschuss für Cybersicherheit

Im Rahmen der Cyberstrategie der Autonomen Provinz Bozen ist der **Strategische Ausschuss für Cybersicherheit** innerhalb der **Agentur Südtirol Digital** angesiedelt. Er ist für die **Definition der Gesamtstrategie für Cybersicherheit** in der APB und die **trasversale Steuerung der für ihre Umsetzung erforderlichen Cyberinitiativen** verantwortlich („**Accountable**“).

Der Strategische Ausschuss für Cybersicherheit:

- **gibt die strategischen Leitlinien vor** und **genehmigt die Cybersicherheitsziele** der APB und der Körperschaften des Landes,
- teilt und bewertet **endogene oder exogene Elemente (z. B. organisatorische Strukturen, regulatorische Entwicklungen, lokale gesetzliche Beschränkungen...) in Bezug auf die IT-Sicherheit,** die sich maßgeblich auf die Erreichung der festgelegten Ziele auswirken,
- genehmigt die **Analysen der Cybersicherheitsrisiken** des Kompetenzzentrums,
- definiert das **Akzeptanzlevel von Cybersicherheitsrisiken**,
- genehmigt den vom Kompetenzzentrum vorgeschlagenen **Jahresplan für Aktivitäten** zur Risikominderung,
- genehmigt den **Plan für Cybersicherheit** und die **Programme für die zentralen Dienste.**

Der Strategische Ausschuss für Cybersicherheit setzt sich aus den folgenden Teilnehmer:innen zusammen:

- Landeshauptmann,
- Generaldirektor der Autonomen Provinz Bozen,

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

- der Verantwortliche für den digitalen Wandel (auch als Kontaktperson für das Kompetenzzentrum),
- für die Digitalisierung zuständige Landesrat der Autonomen Provinz Bozen,
- Generaldirektor:in ASDAA/SABES,
- Präsident:in des Gemeindenverbands,
- IPES-Geschäftsführer:in,
- Generaldirektor:in SIAG,
- Generaldirektor:in Infranet AG,
- IT-Beauftragte:r der Region Trentino-Südtirol,
- CSIRT Manager,
- zukünftige Teilnehmer:innen.

4.1.2 Das Kompetenzzentrum für Cybersicherheit

Die Cybersecurity-Governance-Zentrale ist verantwortlich für die Festlegung und Überwachung der Strategie für das Cybersicherheits-Risikomanagement unter Berücksichtigung der verbindlichen gesetzlichen Auflagen, der Erwartungen der Interessengruppen und der im Kontext der Provinz ermittelten, weiter gefassten Ziele sowie für die Festlegung, Umsetzung und Koordinierung von Strategien, Modellen, Instrumenten und Programmen zu deren Umsetzung.

Diese Rolle wird dem **Kompetenzzentrum für Cybersicherheit** der Agentur Südtirol Digital übertragen**,** das für die Entwicklung von Cybersicherheitsstrategien, die Verwaltung und Kontrolle der entsprechenden Prozesse, die Messung ihrer Wirksamkeit, die angemessene Minderung von Cybersicherheitsrisiken und die kontinuierliche Verbesserung zuständig ist.

Das Kompetenzzentrum ist das Steuerungsinstrument („Responsible"), mit dessen Hilfe das, was auf der Ebene des Strategischen Ausschusses für Cybersicherheit („Accountable") beschlossen wurde, aufgegriffen, umgesetzt und in seiner Durchführung überwacht wird.

Das Kompetenzzentrum übernimmt **Governance-, Koordinations- und Kontrolltätigkeiten und Verantwortlichkeiten** in Bezug auf:

- die **organisatorischen und technischen Cybersicherheitsstrukturen,**
- **die Bereitstellung zentralisierter Cybersicherheitsdienste für die Körperschaften des Landes** (durch Shared Service Management).

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

4.1.3 Die Körperschaften des Landes

Die Körperschaften des Landes sind Einrichtungen, die vor Cybersicherheitsrisiken geschützt werden müssen und für die interne Einführung/Umsetzung von Richtlinien, Prozessen, Rollen und Verantwortlichkeiten zum Schutz vor Cybersicherheitsrisiken verantwortlich sind. In diesem Zusammenhang gilt:

- Sie müssen intern geeignete Rollen (mit den entsprechenden Verantwortlichkeiten) festlegen:
  - o **eine Kontaktperson für Cybersicherheit** (Ref.1.2.2) – diese Rolle kann delegiert werden,
  - o **eine Kontaktperson für IKT-Technik und/oder ein:e Sprecher:in der betreffenden öffentlichen Einrichtung,**
- **Sie werden vom Kompetenzzentrum koordiniert,** das als Cybersicherheits-Governance-Zentrale fungiert.
- **Sie erhalten vom Kompetenzzentrum Anweisungen zu den anzuwendenden Cybersicherheitsstrategien, -prozessen, organisatorischen Aufgaben, Programmen und Diensten.**
- **Sie passen die vom Kompetenzzentrum erhaltenen Anweisungen bei Bedarf oder in Abstimmung mit dem Kompetenzzentrum an ihren eigenen Kontext an.**
- Sie erhalten **zentralisierte Cybersicherheitsdienste.**

In diesem Zusammenhang sei noch einmal darauf hingewiesen, dass die Körperschaften des Landes eine **Kontaktperson für Cybersicherheit** benennen müssen, ggf. auch im Verbund miteinander (Ref.1.2.2). Wenn die Kontaktperson für Cybersicherheit innerhalb der Behörde selbst tätig ist, ist er/sie mit der **technischen Kontaktperson** identisch und Teil des CSIRT-AA-Kernteams. Wird die Kontaktperson für Cybersicherheit außerhalb der Behörde benannt, so muss die Behörde auch eine **technische Kontaktperson** benennen, die innerhalb der Organisation tätig werden kann.

4.1.4 Zentralisierte Anbieter von Cybersicherheitsdiensten

Dies sind **Akteure, die den Körperschaften des Landes zentral gesteuerte und durch das Kompetenzzentrum geregelte Cybersicherheitsdienste zur Verfügung stellen**. Diese Anbieter können dem APB-Kontext angehören, was jedoch nicht zwingend erforderlich ist.

Eine strategische Rolle wird in diesem Kontext der Südtiroler Informatik AG (SIAG) zuteil, dem inhouse IKT-Service Provider der Autonomen Provinz Bozen.

In diesem Zusammenhang wurde bei der Autonomen Provinz Bozen das **Computer Security Incident Response Team Südtirol (CSIRT-AA)** eingerichtet, das mit operativer Unterstützung der SIAG arbeitet, einen Cybersicherheitsdienst von höchster Bedeutung darstellt und im Strategischen Ausschuss für Cybersicherheit vertreten ist.

Die folgende Beschreibung des Cyber-Modells Südtirol sieht nicht die zeitnahe Identifizierung aller zentralisierten Cybersicherheitsdienstleister vor, mit Ausnahme – aufgrund seiner Bedeutung – des CSIRT-AA.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

4.2 Übersicht der wichtigsten Fachgebiete

FUNKTIONEN UND BEREICHE		KOMPETENZZENTRUM	LOKALE BEHÖRDEN	DIENSTLEISTER	CSIRT-AA
GV	Organizational Context (GV.OC)	A/R	C	C	C
	Risk Management Strategy (GV.RM)	A/R	C	C	C
	Roles, Responsibilities, and Authorities (GV.RR)	A/R	C	C	C
	Policy (GV.PO)	A/R	R	C	C
	Oversight (GV.OV)	A/R	R	C	C
	Cybersecurity Supply Chain Risk Management (GV.SC)	A/R	R	C	C
ID	Asset Management (ID.AM)	A/R	R	C	C
	Risk Assessment (ID.RA)	A/R	R	C	C
	Improvement (ID.IM)	A/R	R	C	C
PR	Identity MGMT, Authentication, and Access Control (PR.AA)	A	R/C	R	R
	Awareness and Training (PR.AT)	A	R/C	R	R
	Data Security (PR.DS)	A	R/C	R	R
	Platform Security (PR.PS)	A	R/C	R	R
	Technology Infrastructure Resilience (PR.IR)	A	R/C	R	R
DE	Continuous Monitoring (DE.CM)	I	R	C	A/R
	Adverse Event Analysis (DE.AE)	I	R	C	A/R
RS	Incident Management (RS.MA)	I	R	C	A/R
	Incident Analysis (RS.AN)	I	R	C	A/R
	Incident Response Reporting and Communication (RS.CO)	I	R	C	A/R
	Incident Mitigation (RS.MI)	I	R	C	A/R
RC	Incident Recovery Plan Execution (RC.RP)	I	R	C	A/R
	Incident Recovery Communication (RC.CO)	I	R	C	A/R

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

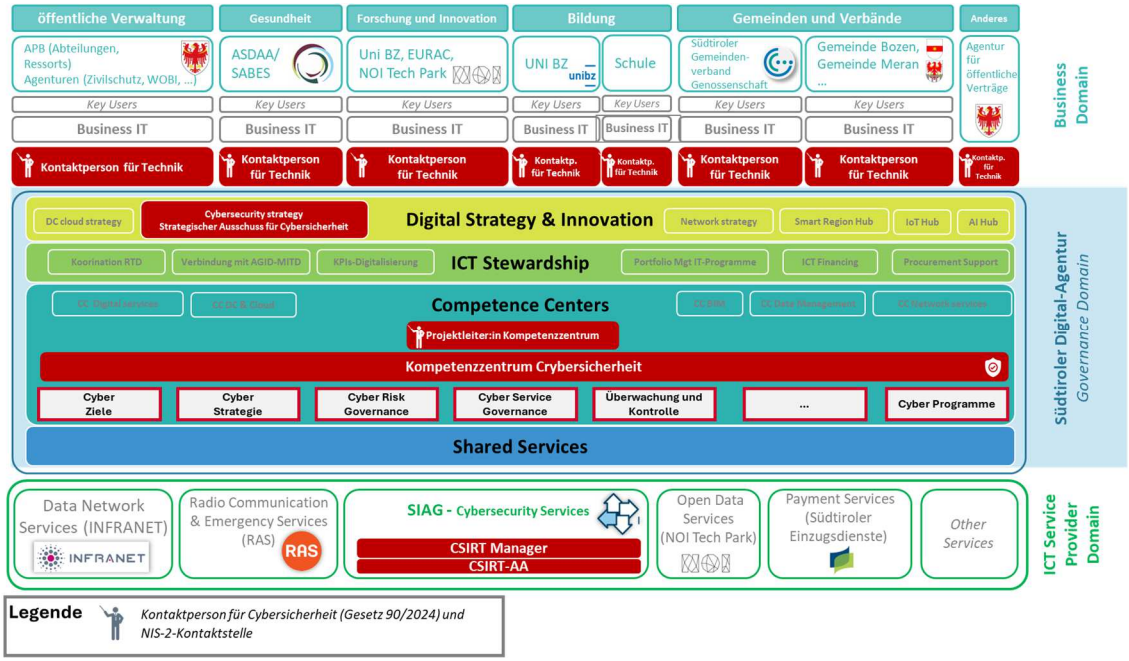
4.3 Aufgaben in Bezug auf die NIS-2-Richtlinie und das Gesetz 90/2024

Aus regulatorischer Sicht verlangt die NIS-2-Richtlinie die Benennung eines:r Ansprechpartners:in als Kontaktperson für Cybersicherheitsaspekte, während Artikel 8, Absatz1 des Gesetzes Nr. 90/2024 die Benennung einer Cybersicherheitsstruktur und innerhalb dieser einer *„Ansprechperson für Cybersicherheit, die auf der Grundlage spezifischer und nachgewiesener Fachkompetenz und Sachkenntnis in Cybersicherheitsfragen benannt wird*“, vorschreibt, die mit der NIS-2-Kontaktstelle übereinstimmen kann.

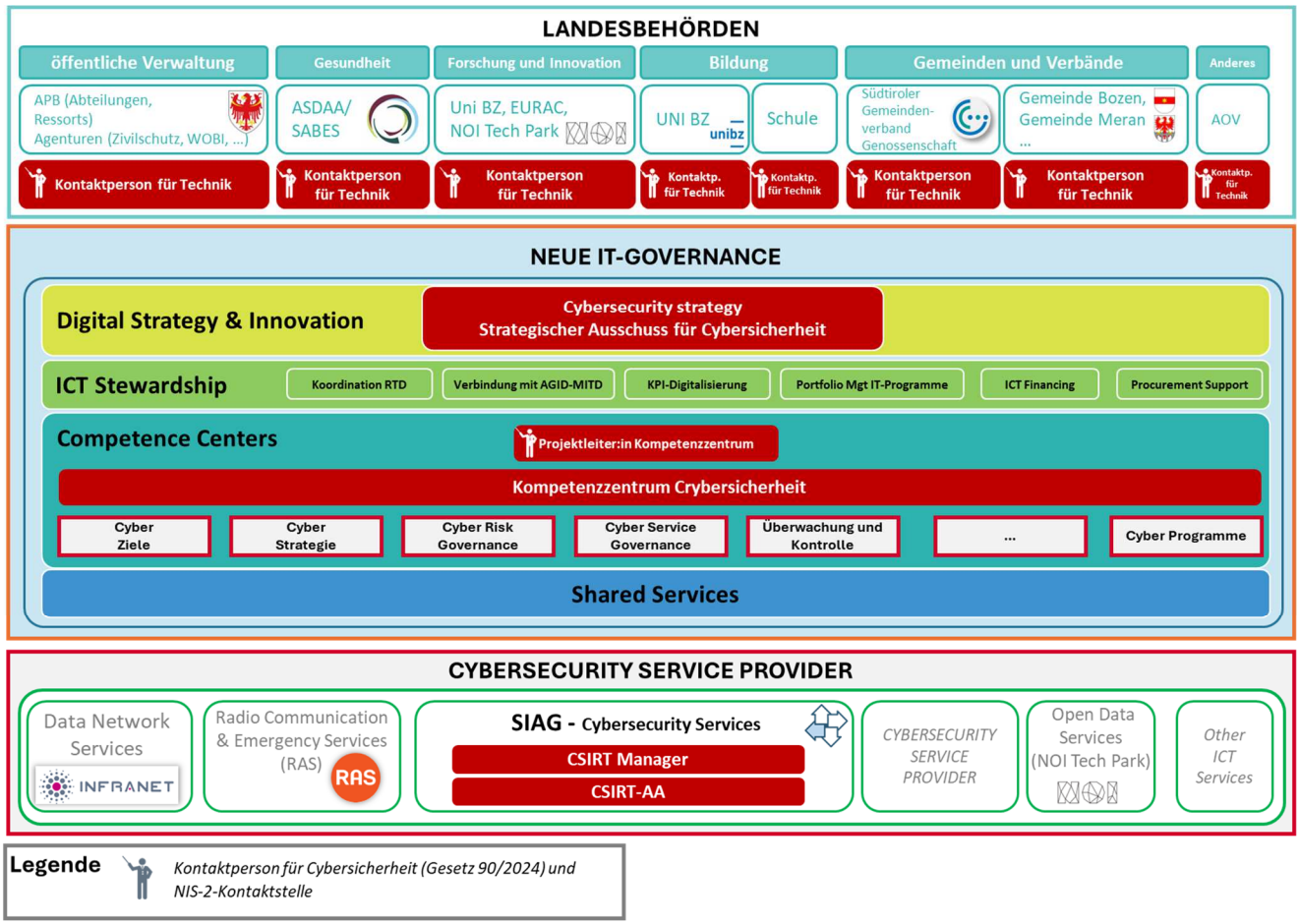
Im Rahmen des Cyber-Modell Südtirols wird festgelegt, dass **jede Körperschaft des Landes auch im Verbund (Ref.1.2.2) eine Kontaktperson für Cybersicherheit benennen muss, um die vollständige Einhaltung der Vorschriften zu gewährleisten.** Falls die Kontaktperson für Cybersicherheit im Verbund außerhalb der Einrichtung benannt wird, muss in jedem Fall eine technische Kontaktperson f und/oder ein:e Sprecher:in der öffentlichen Einrichtung benannt werden.

4.4 Cyber-Modell Südtirol – Überblick

Im Folgenden werden die Akteure des Cyber-Modell Südtirols im Rahmen des konzeptionellen Schemas der neuen digitalen Governance dargestellt.



Diese Darstellung unterstreicht die Übereinstimmung des Cyber-Modell Südtirols und des Kompetenzzentrums mit dem allgemeinen Ansatz der neuen digitalen Governance. Eine stärker auf die Cybersicherheit zugeschnittene Darstellung sieht wie folgt aus:



Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

5. Kompetenzzentrum für Cybersicherheit

5.1 Die Rolle des Kompetenzzentrums im Allgemeinen

Das Kompetenzzentrum hat eine Führungs- und Kontrollfunktion im Bereich der Cybersicherheit innerhalb der Autonomen Provinz Bozen und der damit verbundenen Körperschaften des Landes. In dieser Rolle **analysiert** es **Cyber-Risiken** und legt eine **Cybersicherheitsstrategie** fest, steuert **Projektinitiativen und Cybersicherheitsdienste** und überwacht deren **Fortschritt und Wirksamkeit.**

5.2 Die Rolle des Kompetenzzentrum innerhalb der künftigen Agentur

Innerhalb der Agentur spielt das Kompetenzzentrum die Rolle der Cybersicherheitsstruktur (gemäß Gesetz 90/2024, Artikel 8, Absatz 1). Dazu gehört:

- die **Entwicklung von Informationssicherheitsstrategien und -verfahren,**
- die **Erstellung und Aktualisierung von Systemen zur präventiven Erkennungsanalyse** und eines **IT-Risikomanagementplans,**
- die **Erstellung und Aktualisierung eines Dokuments**, in dem **die Aufgaben und die Organisation des Informationssicherheitssystems festgelegt** sind,
- die **Erstellung und Aktualisierung eines Strategieplans für die Sicherheit von Daten, Systemen und Infrastrukturen,**
- die **Planung und Durchführung von Maßnahmen zum Aufbau von Kapazitäten für das Cyber-Risikomanagement,**
- die **Planung und Umsetzung der Maßnahmen in den von der Nationalen Agentur für Cybersicherheit herausgegebenen Cybersicherheitsrichtlinien,**
- die **kontinuierliche Überwachung und Bewertung von Sicherheitsbedrohungen und Schwachstellen** von Systemen, um diese umgehend zu aktualisieren.

Ein Schlüsselelement des Umsetzungsplans der Cyber-Strategie der Autonomen Provinz Bozen ist die **Einrichtung des CSIRT-AA, das auf operativer Ebene Dienstleistungen zur Analyse neu auftretender Cyber-Bedrohungen und zur Lösung von Cyber-Sicherheitsvorfällen bietet**.

5.3 Zuständigkeiten

Das Kompetenzzentrum ist dafür verantwortlich, die **Strategie, Erwartungen und Politik der Autonomen Provinz Bozen im Bereich des Cybersicherheits-Risikomanagements** auf der Grundlage der gesetzlichen Vorgaben und der allgemeinen Ziele des Landes auszuarbeiten und deren **Vermittlung, die Übertragung in**

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Aktionspläne und die ganzheitliche Überprüfung der Initiativen und des Cyber-Risikoprofils insgesamt sicherzustellen.

Zu diesem Zweck **analysiert und berücksichtigt** das Kompetenzzentrum die **Erwartungen der Stakeholder**, die **regulatorischen Bedingungen und Anforderungen, die Prioritäten und die Einschränkungen bei der Entwicklung eines Rahmenwerks für das Cyber-Risikomanagement**. Dazu gehört auch die Umsetzung spezifischer Schutzmaßnahmen wie z. B. der operativen Dienste, die von der CSIRT-AA im Bereich der Analyse neu auftretender Cyber-Bedrohungen und der Lösung von Cyber-Sicherheitsvorfällen bereitgestellt werden.

Das Kompetenzzentrum sorgt für eine adäquate **Definition der Rollen und Verantwortlichkeiten im Bereich Cybersicherheit** im organisatorischen Kontext der Autonomen Provinz Bozen und ihrer Dienstleister. Zu seinen Aufgaben gehört es, eine **möglichst breit angelegte Cybersicherheitspolitik festzulegen**, die eine **gemeinsame Grundlage für die von den verschiedenen Stellen anzuwendenden spezifischen Ableitungen bilden kann**, um die Besonderheiten des jeweils eigenen Kontexts zu erfassen. Besonderes Augenmerk ist dabei auf die Definition von Maßnahmen und Leitlinien für Risikomanagementprozesse in der IT-Lieferkette zu richten.

Um die Risikomanagementstrategie zu untermauern, zu verbessern und abzustimmen, muss das Kompetenzzentrum eine adäquate **Überwachung und Beaufsichtigung der Ergebnisse der Aktivitäten und Leistungen im Bereich des Cybersicherheits-Risikomanagements** gewährleisten.

5.4 Aktivitäten

In diesem Sinne leitet das Kompetenzzentrum die Verantwortung für die folgenden Aktivitäten ab, die hauptsächlich mit der **CSF-2.0-Funktion** der **Governance** zusammenhängen und darauf abzielen, den organisatorischen Kontext zu analysieren, eine Cybersicherheitsstrategie festzulegen, Cybersicherheitsrisiken und die Cybersicherheitslieferkette zu verwalten sowie Rollen, Verantwortlichkeiten und Vorgehensweisen zu definieren und die wirksame Umsetzung der Cybersicherheitsstrategie zu überwachen:

- Erfassung und Analyse des Kontexts der Autonomen Provinz Bozen und der dazugehörigen Einrichtungen,
- Ermittlung und Analyse der Ziele und Strategien des Landes, insbesondere im Hinblick auf die Digitalisierung der öffentlichen Verwaltung und die damit verbundenen Bedürfnisse im Landesgebiet,
- Identifizierung, Austausch und Konsolidierung der Ziele des Landes im Bereich der Cybersicherheit,
- Definition der zur Erreichung dieser Ziele erforderlichen Strategie,
- Definition und Einrichtung eines Cybersicherheits-Managementsystems, das aus Rollen, Zuständigkeiten, Prozessen und Instrumenten besteht, um die ermittelte Strategie umzusetzen,
- Definition und Einführung eines umfassenden organisatorischen und operativen Modells für das Management von Cybersicherheitsrisiken,

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

- Ermittlung der von Cybersicherheitsdienstleistern (z. B. CSIRT-AA) angebotenen Dienste, die in die Strategien und das Betriebsmodell integriert und darauf abgestimmt werden können,
- Koordinierung eines Plans für Projektinitiativen zur Umsetzung der Maßnahmen, die für die Anwendung des Cybersicherheitsrahmens erforderlich sind,
- Steuerung und Lenkung der Erbringung gemeinsamer Cybersicherheitsdienste für die Autonome Provinz Bozen und die dazugehörigen Einrichtungen,
- laufende Überwachung und Analyse der Leistung der eingesetzten Cybersicherheitssysteme,
- kontinuierliche Überwachung des gesamten Cybersicherheits-Risikoprofils der Autonomen Provinz Bozen und der dazugehörigen Einrichtungen.

5.5 Die Kontaktperson des Kompetenzzentrums

Innerhalb des Kompetenzzentrums für Cybersicherheit ist eine Kontaktperson angesiedelt. Sie leitet und gewährleistet die Ausarbeitung und ständige Aktualisierung der folgenden Aspekte:

- Richtlinien und Verfahren bezüglich der Informationssicherheit,
- präventive Erkennungsanalysen, Cyber-Risikomanagement- Plan,
- Organisation des Informationssicherheitssystems,
- Programmplan für die Sicherheit von Daten, Systemen und IKT-Infrastruktur,
- Planung und Durchführung von Maßnahmen zum Aufbau von Kapazitäten für das Cyber-Risikomanagement,
- Planung und Umsetzung der Maßnahmen in den von der Nationalen Agentur für Cybersicherheit herausgegebenen Cybersicherheitsrichtlinien,
- kontinuierliche Überwachung und Bewertung von Sicherheitsbedrohungen und Schwachstellen von Systemen, um diese umgehend zu aktualisieren.

Die Kontaktperson des Kompetenzzentrums kann mit der Kontaktperson für Cybersicherheit für die Agentur übereinstimmen (Ref.1.2.2).

6. Körperschaften des Landes

Wie bereits erwähnt müssen die Körperschaften des Landes geeignete Rollen mit den entsprechenden Zuständigkeiten im Bereich der Cybersicherheit festlegen (**Kontaktperson für Cybersicherheit** und **technische Kontaktperson**).

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Die in jeder Körperschaft benannte technische Kontaktperson ist dafür verantwortlich, als Bindeglied zwischen ihrer Organisation und den zentralen Cybersicherheitsstrukturen (Kompetenzzentrum und zentralisierte Cybersicherheitsdienstleister) zu fungieren. In diesem Zusammenhang ist die technische Kontaktperson dafür verantwortlich, dass die von den zentralen Strukturen bereitgestellten Maßnahmen und Dienste wirksam sind, indem sie sie im Rahmen der Spezifikation entsprechend dekliniert. Innerhalb der Rolle der technischen Kontaktperson sind folgende Aufgaben vorgesehen:

- Verwaltung der Umsetzung zentral festgelegter Strategien innerhalb ihres technologischen und organisatorischen Zuständigkeitsbereichs,
- Überwachung der Wirksamkeit der in ihrem Zuständigkeitsbereich durchgeführten Sicherheitsmaßnahmen,
- Sicherstellung der Ressourcen und Bedingungen für die Erbringung zentralisierter Cybersicherheitsdienste (z. B. Gewährleistung einer adäquaten Konfiguration von Firewalls im Falle zentral erbrachter VA/PT, Ermittlung des Personals, das an der von den zentralen Strukturen durchgeführten Cyberrisikobewertung teilnehmen muss usw.),
- Versorgung des Kompetenzzentrums mit Informationen über die Wirksamkeit von Sicherheitsmaßnahmen (z. B. KRI, KPI) sowie lokal ermittelte Bedürfnisse und Ziele,
- Beitrag zum Monitoring von Sicherheitsereignissen, um mögliche Angriffe ganzheitlich zu adressieren und gemeinsame bewährte Verfahren auszutauschen,
- operatives Management der Prozesse im Umgang mit Cybersicherheits-Vorfällen während des gesamten Lebenszyklus der Ressourcen.

Dabei ist zu beachten, dass die **technische Kontaktperson** auch die **Kontaktperson für Cybersicherheit** ist, wenn letztere innerhalb der Körperschaft und nicht im Verbund bei einer anderen Behörde bestimmt wurde.

7. CSIRT-AA

Als Teil der umfassenderen Steuerung und Kontrolle von Cybersicherheitsfragen durch das Kompetenzzentrum wird das **Mandat der CSIRT-AA** im Einklang mit den ENISA-Leitlinien für den Aufbau von CSIRT darin bestehen, **seiner Constituency (den Körperschaften des Landes, die dem Dienst beitreten werden) fachliche Unterstützung und Hilfe bei der Analyse von Daten im Zusammenhang mit aufkommenden Cyberbedrohungen und der Lösung von Cybersicherheitsvorfällen zu bieten.** Dazu gehört auch, dass das CSIRT in der Lage ist, zeitnah technische Beratung, Unterstützung bei Nachforschungen und Lösungen zur Bekämpfung und Eindämmung von Cyberangriffen zu bieten.

Die Aufgabe des CSIRT-AA wird darin bestehen, die frühzeitige Verbreitung unmittelbar verwertbarer Informationen zur Cybersicherheit zu erleichtern, indem es Warnungen und Hinweise auf neue

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Risikoszenarien, aktuelle Angriffe und Tendenzen bei Cyberphänomenen herausgibt, die auf bestimmte Sektoren, Organisationen oder Gebiete abzielen. Dies wird dazu beitragen, das Bewusstsein und die Vorbereitung lokaler Organisationen im Umgang mit Cyberrisiken zu verbessern.

Das CSIRT-AA wird darüber hinaus die Aufgabe haben, die Anwendung von Sicherheitsmanagementprozessen und Evaluierungsmethoden für die Governance im Bereich der Cybersicherheit zu fördern. Dazu gehört auch die Förderung der Übernahme bewährter Verfahren und Leitlinien, um den Schutz digitaler Güter zu gewährleisten und eine Kultur der Cybersicherheit in seiner Constituency zu fördern (s. Anhang Organisationsmodell CSIRT-AA). Das CSIRT-AA ist also die von der Autonomen Provinz Bozen geförderte und bei Südtiroler Informatik AG angesiedelte Task Force für IT-Sicherheit. Sie wird auf dem gesamten Landesgebiet tätig sein und alle öffentlichen Einrichtungen unterstützen, die dies ausdrücklich beantragen.

Die CSIRT-AA wird Dienstleistungen und Leitlinien für eine lückenlose Handhabung von Cyber-Bedrohungen und -Vorfällen sowie aktive Unterstützung für die Mitglieder der Constituency bereitstellen, die dadurch ihrerseits in der Lage sein werden, die Leitlinien eigenständig auf ihren eigenen Kontext anzupassen, um sie so effektiv wie möglich zu gestalten.

Die hybride Organisation des CSIRT-AA mit ihren eingebetteten Campus-Merkmalen wird die Elemente einer zentralisierten Organisation mit einem dezentralen Ansatz kombinieren. Im Detail wird das CSIRT-AA über eine zentralisierte Struktur in der Südtiroler Informatik AG verfügen, die mit eigens dafür vorgesehenen Ressourcen ausgestattet sein wird und als Koordinationszentrum und Bezugspunkt für alle operativen CSIRT-Aktivitäten dienen wird.

Gleichzeitig wird das CSIRT-AA dank der Bereitstellung von Personal aus jeder Behörde (mindestens eine Kontaktperson für Technik pro Constituency) virtuell vor Ort präsent sein, um die verschiedenen Verwaltungen bei den angebotenen Diensten besser zu unterstützen und anzuleiten.

Weitere Einzelheiten entnehmen Sie bitte dem Dokument „Organisationsmodell CSIRT-AA“.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

LA CYBERSECURITY NELLA PROVINCIA AUTONOMA DI BOLZANO

Il Modello Organizzativo

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Sommario

1. Introduzione 3
1.1 Obiettivo 3
1.2 Contesto Normativo 3
1.2.1 Direttiva NIS 2 3
1.2.2 Legge 90/2024 3
1.3 La struttura del documento 4
2. Il framework di riferimento 5
3. La Nuova Governance Digitale 7
3.1 Il modello organizzativo 7
3.2 I Competence Center dell'Agenzia 7
4. Il modello organizzativo per la cybersecurity di PAB ed Enti Provinciali 9
4.1 Gli attori e le loro macrocategorie 9
4.1.1 Il Comitato Strategico Cybersecurity 9
4.1.2 Il Competence Center per la Cybersecurity 10
4.1.3 Gli Enti Provinciali 10
4.1.4 I Fornitori di servizi centralizzati di cybersecurity 11
4.2 Mappa dei principali ambiti di competenza 12
4.3 I ruoli rispetto alla NIS2 e alla Legge 90/2024 13
4.4 Modello Cyber PAB – Una rappresentazione complessiva 13
5. Cybersecurity Governance Centrale 15
5.1 Il Ruolo di governo complessivo 15
5.2 Il Ruolo all'interno dell'Agenzia 15
5.3 Le Responsabilità 15
5.4 Le Attività 16
5.5 Il Referente del CdC-CY 17
6. Enti Provinciali 17
7. CSIRT-AA 18

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

1. Introduzione

1.1 Obiettivo

Il presente documento ha lo scopo di sviluppare, anche nell'ambito della Agenzia Alto Adige Digitale e della strategia unica per la trasformazione digitale a livello provinciale, una **visione d'insieme** e una **descrizione di alto livello del modello organizzativo per la cybersecurity** (di seguito anche "**Modello Cyber PAB**") della Provincia Autonoma di Bolzano e delle amministrazioni pubbliche e degli organismi pubblici assimilati che abbiano sede od operino nel territorio provinciale (di seguito anche "**PAB ed Enti Provinciali**" o anche solo "**enti**").

1.2 Contesto Normativo

1.2.1 Direttiva NIS 2

La Direttiva (UE) 2022/2555 ("Direttiva NIS2") del parlamento europeo e del consiglio del 14 dicembre 2022, relativa a misure per un **livello di maturità comune di cibersicurezza** nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972, abroga la direttiva (UE) 2016/1148 ("Direttiva NIS").

Le direttive NIS nascono per migliorare la sicurezza delle reti e dei sistemi informativi all'interno dell'Unione Europea, imponendo agli **operatori di servizi essenziali di garantire la resilienza digitale** delle proprie infrastrutture.

La **Direttiva NIS2** amplia le disposizioni della **Direttiva NIS**, **introducendo requisiti più stringenti** per la gestione del rischio, **estendendo il campo di applicazione a un maggior numero di settori** e aumentando le responsabilità per i dirigenti dei soggetti a cui si applica. In particolare, la NIS2 si applica alla **Pubblica Amministrazione Centrale e Locale e introduce obblighi per PAB ed Enti Provinciali in tema di cybersecurity.**

1.2.2 Legge 90/2024

Legge 28 giugno 2024, n. 90 ("Legge 90/2024") è un importante provvedimento legislativo italiano che ha aggiornato il quadro normativo in materia di **cybersecurity e resilienza digitale nel contesto della Pubblica Amministrazione**.

In particolare, la Legge 90/2024 richiede al soggetto (l'Ente Pubblico) **l'individuazione di una struttura preposta alla cybersicurezza e la nomina di un "referente per la cybersicurezza"**, con specifiche e comprovate professionalità e competenze in materia di cybersicurezza, il cui nominativo deve essere comunicato all'Agenzia per la cybersecurity (di seguito "ACN").

Si noti per completezza che:

- l'Ente Pubblico può conferire "*l'incarico di referente per la cybersicurezza a un dipendente di una pubblica amministrazione, previa autorizzazione di quest'ultima ai sensi dell'articolo 53 del decreto legislativo 30 marzo 2001, n. 165, nell'ambito delle risorse disponibili a legislazione vigente.*" [Legge 90/2024 Art.8.2]

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

- "*La struttura e il referente […] possono essere individuati, rispettivamente, nell'ufficio e nel responsabile per la transizione al digitale previsti dall'articolo 17 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82*." [Legge 90/2024 Art.8.2]
- *"I compiti di cui ai commi 1 e 2 possono essere esercitati in **forma associata** secondo quanto previsto dall'articolo 17, commi 1 -sexies e 1 -septies, del codice di cui al decreto legislativo 7 marzo 2005, n. 82"*. [Legge 90/2024 Art.8.4]

Decreto legislativo 7 marzo 2005, n. 82 - 1 -sexies. *Nel rispetto della propria autonomia organizzativa, le pubbliche amministrazioni diverse dalle amministrazioni dello Stato individuano l'ufficio per il digitale di cui al comma 1 tra quelli di livello dirigenziale oppure, ove ne siano privi, individuano un responsabile per il digitale tra le proprie posizioni apicali. In assenza del vertice politico, il responsabile dell'ufficio per il digitale di cui al comma 1 risponde direttamente a quello amministrativo dell'ente*.

*Decreto legislativo 7 marzo 2005, n. 82*1 -septies*. I soggetti di cui al comma 1 -sexies possono esercitare le funzioni di cui al medesimo comma anche in forma associata. È fatta salva la facoltà di avvalersi, mediante apposite convenzioni e senza nuovi o maggiori oneri a carico della finanza pubblica, del supporto di società in house.*

Il 26 novembre 2024 sono state inoltre pubblicate, sul portale dell'ACN, le "**Linee Guida per il rafforzamento della resilienza dei soggetti di cui all'articolo 1, comma 1, della Legge 28 giugno 2024, n. 90**" ("Linee Guida ACN") che rappresentano il primo passo operativo per indirizzare gli ulteriori nuovi adempimenti richiesti, ai soggetti della Pubblica Amministrazione in tema di cybersecurity. Le Linee Guida ACN identificano 26 misure di sicurezza declinate in circa 100 controlli implementativi che andranno a rafforzare ulteriormente i requisiti che la **PAB e gli Enti Provinciali** dovranno soddisfare.

1.3 La struttura del documento

Al fine di introdurre i concetti, i criteri e le linee guida con cui è sviluppato il **Modello Cyber PAB**, il presente documento introduce:

- Il framework di riferimento;
- La Nuova Governance Digitale;
- Il modello organizzativo per la cybersecurity di PAB ed Enti Provinciali ("**Modello Cyber PAB"**);
- Il Competence Center per la Cybersecurity;
- Il CSIRT-AA.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

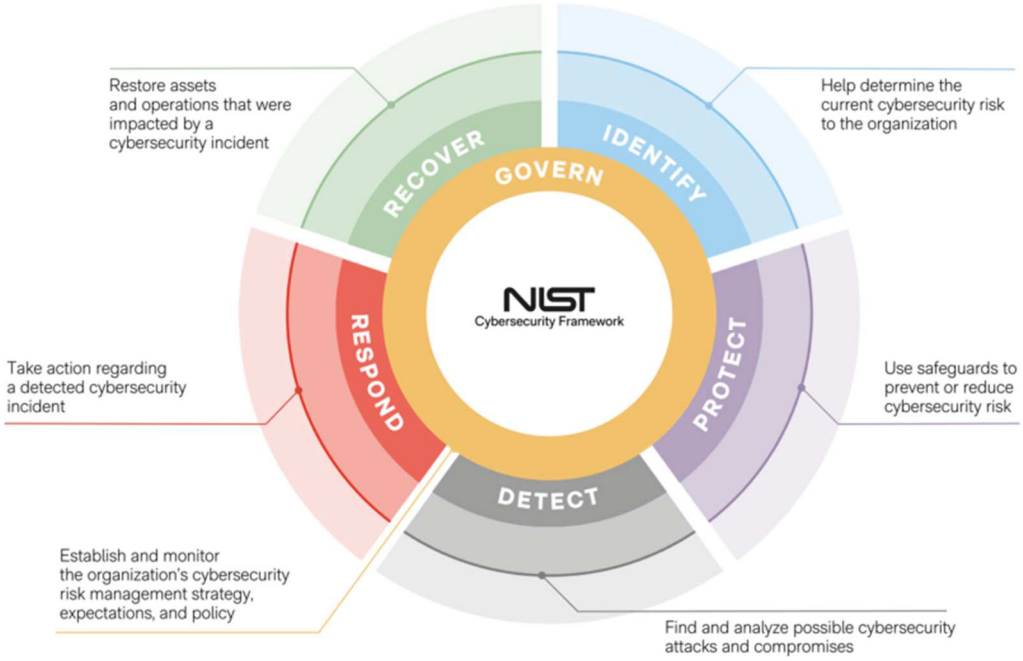
2. Il framework di riferimento

Al fine di strutturare in modo solido e sistematico la descrizione del Modello Cyber PAB, è stato utilizzato il **NIST Cybersecurity Framework 2.0**[1] **("CSF 2.0")** come framework metodologico di riferimento che permette di elencare e mappare le funzioni e le categorie dei processi necessari per assicurare un adeguato governo, controllo e gestione dei rischi di cybersecurity. Il framework CFS 2.0 consente di creare una **mappa chiara delle responsabilità**, facilitando la collaborazione tra gli attori e il coordinamento strategico per la sicurezza informatica. Tale framework metodologico di riferimento aiuta quindi a:

- Ridurre sovrapposizioni o lacune nelle responsabilità;
- Allineare gli obiettivi di sicurezza agli obiettivi della Pubblica Amministrazione;
- Evolvere verso un modello organizzativo resiliente e proattivo.

Il framework prevede:

- **Funzioni principali** - Sei funzioni (Identify, Protect, Detect, Respond, Recover, Governance) che rappresentano il ciclo completo di gestione della cybersecurity.
- **Categorie e sottocategorie** - Ogni funzione è suddivisa in categorie e sottocategorie che identificano attività specifiche.



[1] Il CSF 2.0 è un aggiornamento del noto framework di cybersecurity sviluppato dal National Institute of Standards and Technology (NIST). Pubblicato nel 2024, la versione 2.0 rappresenta un miglioramento significativo rispetto alla versione originale del 2014 (e il successivo aggiornamento 1.1 del 2018), adattandosi a nuove esigenze del panorama digitale globale e alle sfide emergenti in ambito di sicurezza informatica.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Di seguito sono introdotte, in estrema sintesi, le funzioni del CFS 2.0 al fine di fornire il riferimento per gli elementi da considerare nell'ambito della **costruzione di un modello operativo di cybersecurity** che dovrà essere attuato dal relativo modello organizzativo denominato, come già introdotto, "**Modello Cyber PAB"**.

GOVERN (GV)	Organizational Context (GV.OC)
	Risk Management Strategy (GV.RM)
	Roles, Responsibilities, and Authorities (GV.RR)
	Policy (GV.PO)
	Oversight (GV.OV)
	Cybersecurity Supply Chain Risk Management (GV.SC)
IDENTIFY (ID)	Asset Management (ID.AM)
	Risk Assessment (ID.RA)
	Improvement (ID.IM)
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AA)
	Awareness and Training (PR.AT)
	Data Security (PR.DS)
	Platform Security (PR.PS)
	Technology Infrastructure Resilience (PR.IR)
DETECT (DE)	Continuous Monitoring (DE.CM)
	Adverse Event Analysis (DE.AE)
RESPOND (RS)	Incident Management (RS.MA)
	Incident Analysis (RS.AN)
	Incident Response Reporting and Communication (RS.CO)
	Incident Mitigation (RS.MI)
RECOVER (RC)	Incident Recovery Plan Execution (RC.RP)
	Incident Recovery Communication (RC.CO)

- **Governance (Governare)** – Rappresenta il ruolo strategico della sicurezza informatica nella governance aziendale al fine di garantire che la cybersecurity sia integrata nei processi decisionali e che la gestione dei rischi sia supportata a livello di leadership.
- **Identify (Identificare)** - Si concentra sulla comprensione del contesto, delle risorse critiche e dei rischi associati, con l'obiettivo di creare un quadro di ciò che deve essere protetto e delle vulnerabilità presenti.
- **Protect (Proteggere)** - Riguarda l'implementazione di misure per salvaguardare le informazioni, i sistemi e i servizi ICT e migliorare la resilienza digitale.
- **Detect (Rilevare)** - Si focalizza sulla capacità di identificare tempestivamente incidenti di sicurezza al fine di rilevare anomalie e potenziali compromissioni in tempo utile per rispondere efficacemente.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

- **Respond (Rispondere)** - Definisce le azioni necessarie per gestire un incidente informatico una volta rilevato, limitando i danni e ripristinando la sicurezza al fine di contenere l'incidente e ridurre al minimo l'impatto.
- **Recover (Ripristinare)** - Si concentra sul recupero delle operazioni aziendali e sulla resilienza a seguito di un incidente informatico per ripristinare rapidamente le risorse compromesse, la normale operatività e ridurre al minimo l'impatto a lungo termine.

3. La Nuova Governance Digitale

3.1 Il modello organizzativo

La Provincia Autonoma di Bolzano ha introdotto un **nuovo modello di governance digitale ("Nuova Governance Digitale")** che prevede l'introduzione della "***Agenzia Alto Adige Digitale***" (di seguito anche "Agenzia").

Tale Agenzia è costituita per formulare e attuare la strategia unica per la trasformazione digitale a livello provinciale, perseguendo gli obiettivi di efficacia, efficienza, imparzialità, semplificazione e operando sulla base dei principi di sussidiarietà, trasparenza e di economicità.

L'Agenzia Alto Adige Digitale, anche nell'ambito della cybersecurity, svolge attività di indirizzo, individuando i relativi obiettivi a livello provinciale, definendo e governando la strategia e la sua messa in atto attraverso il coordinamento di iniziative, azioni e sinergie abilitanti alla sua implementazione.

La futura nuova Agenzia agisce quindi nel *Governance Domain* interfacciandosi, da una parte, con PAB ed Enti Provinciali (*Business Domain*) e dall'altra con i fornitori di servizi ICT (*ICT Service Provider Domain*).

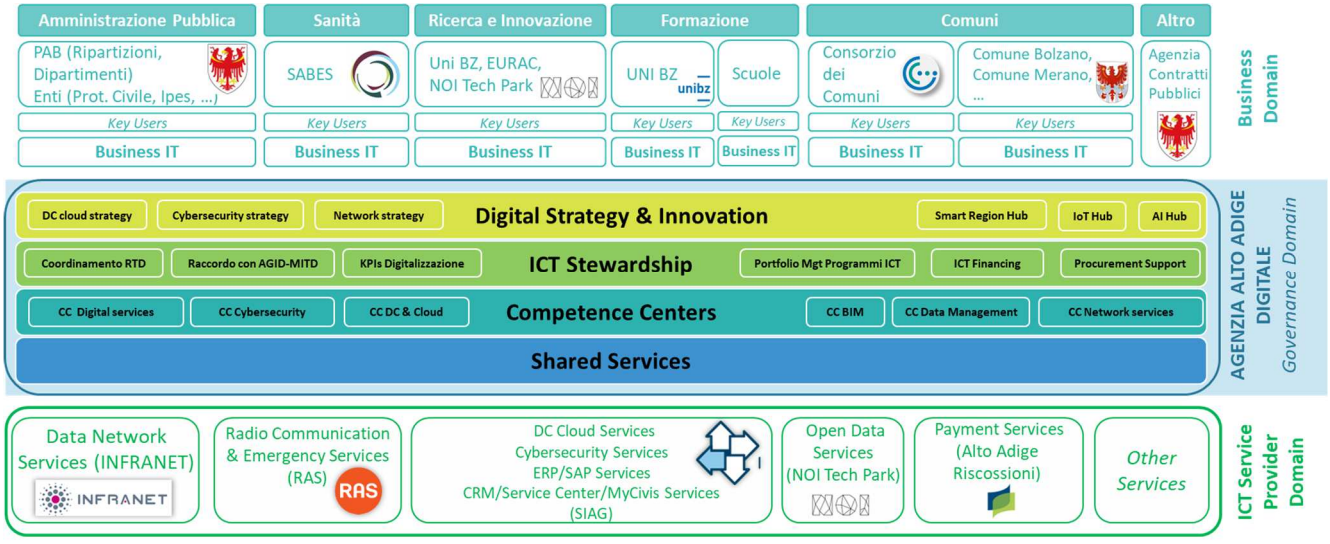


FIGURA 1 - RAPPRESENTAZIONE DELLA NUOVA GOVERNANCE DIGITALE E DELLA AGENZIA ALTO ADIGE DIGITALE

3.2 I Competence Center dell'Agenzia

L'Agenzia si articola logicamente in quattro ambiti principali:

- Digital Strategy and Innovation;
- ICT Stewardship;

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

- Shared Services;
- Competence Centers.

Il modello funzionale dei Competence Centers (di seguito anche “Centri di Competenza” o “CdC”) di Indirizzo può essere rappresentato come una 'scatola grigia' che racchiude i vari servizi necessari affinché il CdC possa formulare direttive operative per i Service Provider permettendo loro di offrire servizi tecnologici che siano in linea con la strategia e le esigenze degli Stakeholder.

La fase di istituzione di un CdC si avvia con l'identificazione dei servizi offerti, dei punti di contatto con le organizzazioni (input), il perimetro di intervento/competenza (vincoli) e prodotti dei servizi offerti (output), che rappresentano le variabili del modello.

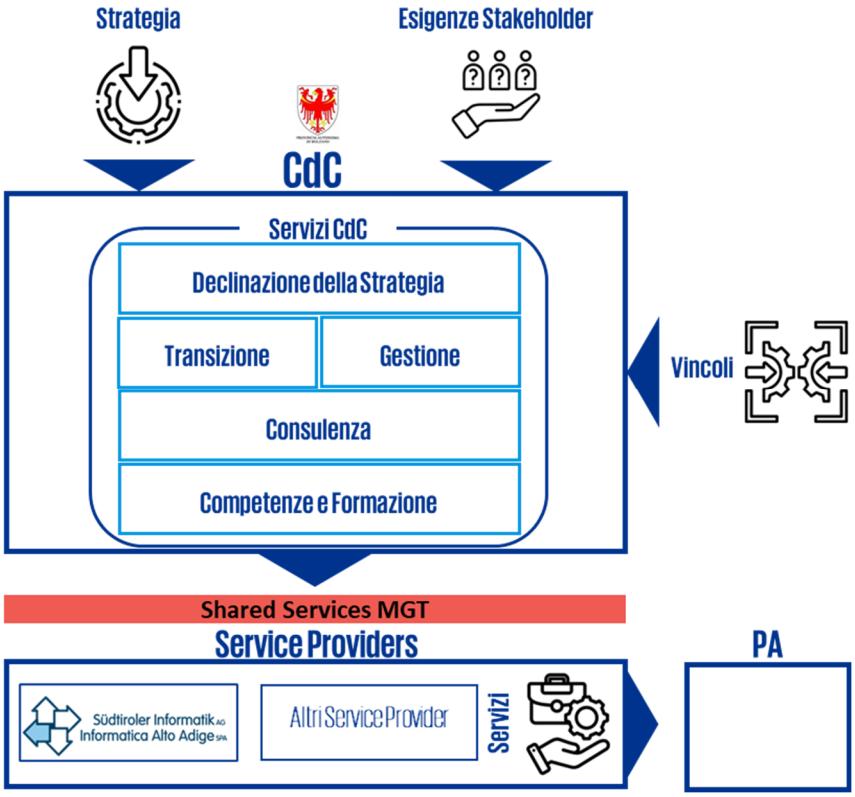


FIGURA 2 - RAPPRESENTAZIONE DELLA LOGICA DEI CENTRI DI COMPETENZA

Nel processo di creazione della Nuova Governance Digitale, la Provincia ha attribuito all'organizzazione del **Centro di Competenza trasversale per la Cybersecurity dell’Alto Adige (CdC-CY)** un'elevata priorità. Di seguito si dettaglia come, nel contesto dell’Agenzia Alto Adige Digitale, il CdC-CY ricopre un ruolo centrale nel **Modello Cyber PAB.**

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

4. Il modello organizzativo per la cybersecurity di PAB ed Enti Provinciali

4.1 Gli attori e le loro macrocategorie

Il Modello Cyber PAB prevede le seguenti categorie di ruoli associati ai differenti attori:

- **Livello strategico - nuova Governance:**
  - **Comitato Strategico Cybersecurity**;
  - **Competence Center per la cybersicurezza;**
  - **Enti Pubblici Provinciali aderenti**
  - **Fornitori di servizi centralizzati di cybersecurity**.
- **Livello operativo: CSIRT-AA**

4.1.1 Il Comitato Strategico Cybersecurity

Nell'ambito della più ampia prospettiva della strategia cyber della Provincia autonoma di Bolzano, il **Comitato Strategico Cybersecurity è posizionato all'interno dell'Agenzia Alto Adige Digitale assicurando (è "Accountable") la definizione della strategia complessiva per la cybersecurity nella Provincia autonoma di Bolzano** e la **governance trasversale delle iniziative cyber necessarie per la sua implementazione.**

Il Comitato Strategico Cybersecurity:

- **Indirizza le linee strategiche** e **approva gli obiettivi per la Cybersecurity** della PAB e degli Enti Provinciali;
- Condivide e valuta gli **elementi endogeni o esogeni (es. assetti organizzativi, evoluzioni normative, vincoli di leggi locali, …) relativi alla sicurezza informatica** che hanno impatti rilevanti sul raggiungimento degli obiettivi identificati;
- **Approva le analisi dei rischi di Cybersecurity** governate dal CdC-CY;
- Definisce il **livello di accettabilità dei rischi di Cybersecurity**;
- **Approva il piano annuale di attività per la mitigazione dei rischi** proposti dal CdC-CY;
- **Approva il piano e i programmi per la Cybersecurity legato ai servizi centralizzati**.

Il Comitato Strategico Cybersecurity è composto dai seguenti partecipanti:

- Presidente della Provincia autonoma di Bolzano;
- Direttore Generale della Provincia autonoma di Bolzano;
- Responsabile per la transizione digitale (anche in qualità di referente del CdC-CY);
- Assessore competente in materia di digitalizzazione della Provincia autonoma di Bolzano;
- Direttore Generale ASDAA/SABES;
- Presidente del Consorzio dei Comuni;
- Direttore Generale IPES;
- Direttore Generale SIAG;
- Direttore Generale Infranet;

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

- Rappresentante IT della Regione Trentino-Alto Adige
- CSIRT Manager.
- Futuri

4.1.2 Il Competence Center per la Cybersecurity

Il Ruolo di "**Cybersecurity Governance Centrale" ha la responsabilità di definire e presidiare la strategia per la gestione dei rischi di cybersecurity considerando i vincoli normativi cogenti, le aspettative dei portatori di interesse (stakeholder), i più ampi obiettivi identificati nel contesto provinciale, definendo, attuando e coordinando politiche, modelli, strumenti e programmi per la sua realizzazione**.

Tale ruolo è **attribuito al Center of Competence Cybersecurity (di seguito anche CdC-CY) dell'Agenzia Alto Adige Digitale** che ha quindi il compito di definire le strategie di Cybersecurity assicurando la gestione e il controllo dei relativi processi, misurandone l'efficacia, mitigando opportunamente i rischi di sicurezza informatica e perseguendo il miglioramento continuo.

Il CdC-CY è lo strumento di governo ("Responsible") con cui, quanto approvato a livello di Comitato Strategico Cybersecurity ("Accountable"), è indirizzato, attuato e controllato nella sua implementazione.

Al CdC-CY competono attività e responsabilità di **governo, coordinamento e controllo** in merito:

- Ai **presidi organizzativi e tecnici di cybersecurity**;
- Alle **forniture di servizi di cybersecurity centralizzati rivolti agli Enti Provinciali** (attraverso la funzione di Shared Service Management).

4.1.3 Gli Enti Provinciali

Gli enti Provinciali sono le entità che devono essere protette dai rischi di cybersecurity e che sono, al loro interno, responsabili di attuare/implementare le politiche, i processi, i ruoli e le responsabilità a presidio dei rischi di cybersecurity. In questo contesto gli Enti Provinciali:

- Devono **identificare al loro interno opportuni ruoli (con le relative responsabilità) in ambito cybersecurity**
  - **Un "Referente per la cybersicurezza"** *(Rif. 1.2.2)* **- questo ruolo può essere delegato**
  - **Un "Referente Tecnico ICT" e/o portavoce dell'Ente pubblico aderente**
- **Sono coordinati dal CdC-CY** che funge il ruolo di Cybersecurity Governance Centrale;
- **Ricevono dal CdC-CY indicazioni rispetto a politiche, processi, ruoli organizzativi, programmi e servizi di cybersecurity** che devono essere adottati;
- **Adattano, ove necessario o opportuno e sempre in coordinamento con il CdC-CY, al proprio contesto le indicazioni ricevute dal CdC-CY**;
- Ricevono i **servizi centralizzati di cybersecurity.**

Si ribadisce che gli Enti Provinciali devono nominare, anche in forma associata (*Rif. 1.2.2*) il loro "**Referente per la cybersicurezza**". Nel caso in cui il Referente per la cybersicurezza è interno all'ente stesso, questi coincide con il "Referente Tecnico" e partecipa al Core Team del CSIRT-AA. In caso in cui invece il Referente per la cybersicurezza sia identificato in forma associata fuori dall'ente, l'ente deve identificare anche un "**Referente Tecnico**" che possa agire all'interno dell'ente.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

4.1.4 I Fornitori di servizi centralizzati di cybersecurity

Sono gli **attori che erogano, indirizzati e governati in modo centralizzato dal CdC-CY servizi di cybersecurity agli Enti Provinciali.** Tali fornitori possono essere appartenenti al contesto della PAB o meno.

Un ruolo strategico in questo contesto è attribuito a Informatica Alto Adige (Südtiroler Informatik AG ì, di seguito "SIAG") che rappresenta il provider di servizi ICT in-house della Provincia autonoma di Bolzano.

In tale ambito il CSIRT Territoriale dell'Alto Adige (CSIRT-AA) è istituito presso la Provincia Autonoma di Bolzano che agisce con il supporto operativo di SIAG e rappresenta un servizio di cybersecurity di primaria importanza, tanto da essere rappresentato nell'ambito del Comitato Strategico Cybersecurity.

La seguente descrizione del Modello Cyber PAB non prevede l'identificazione puntuale di tutti i fornitori di sevizi centralizzati di cybersecurity ad eccezione del solo CSIRT-AA per la sua rilevanza.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

4.2 Mappa dei principali ambiti di competenza

FUNZIONI E AMBITI		CDC-GY	ENTI LOCALI	FORNITORI DI SERVIZI	CSIRT-AA
GV	Organizational Context (GV.OC)	A/R	C	C	C
	Risk Management Strategy (GV.RM)	A/R	C	C	C
	Roles, Responsibilities, and Authorities (GV.RR)	A/R	C	C	C
	Policy (GV.PO)	A/R	R	C	C
	Oversight (GV.OV)	A/R	R	C	C
	Cybersecurity Supply Chain Risk Management (GV.SC)	A/R	R	C	C
ID	Asset Management (ID.AM)	A/R	R	C	C
	Risk Assessment (ID.RA)	A/R	R	C	C
	Improvement (ID.IM)	A/R	R	C	C
PR	Identity MGMT, Authentication, and Access Control (PR.AA)	A	R/C	R	R
	Awareness and Training (PR.AT)	A	R/C	R	R
	Data Security (PR.DS)	A	R/C	R	R
	Platform Security (PR.PS)	A	R/C	R	R
	Technology Infrastructure Resilience (PR.IR)	A	R/C	R	R
DE	Continuous Monitoring (DE.CM)	I	R	C	A/R
	Adverse Event Analysis (DE.AE)	I	R	C	A/R
RS	Incident Management (RS.MA)	I	R	C	A/R
	Incident Analysis (RS.AN)	I	R	C	A/R
	Incident Response Reporting and Communication (RS.CO)	I	R	C	A/R
	Incident Mitigation (RS.MI)	I	R	C	A/R
RC	Incident Recovery Plan Execution (RC.RP)	I	R	C	A/R
	Incident Recovery Communication (RC.CO)	I	R	C	A/R

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

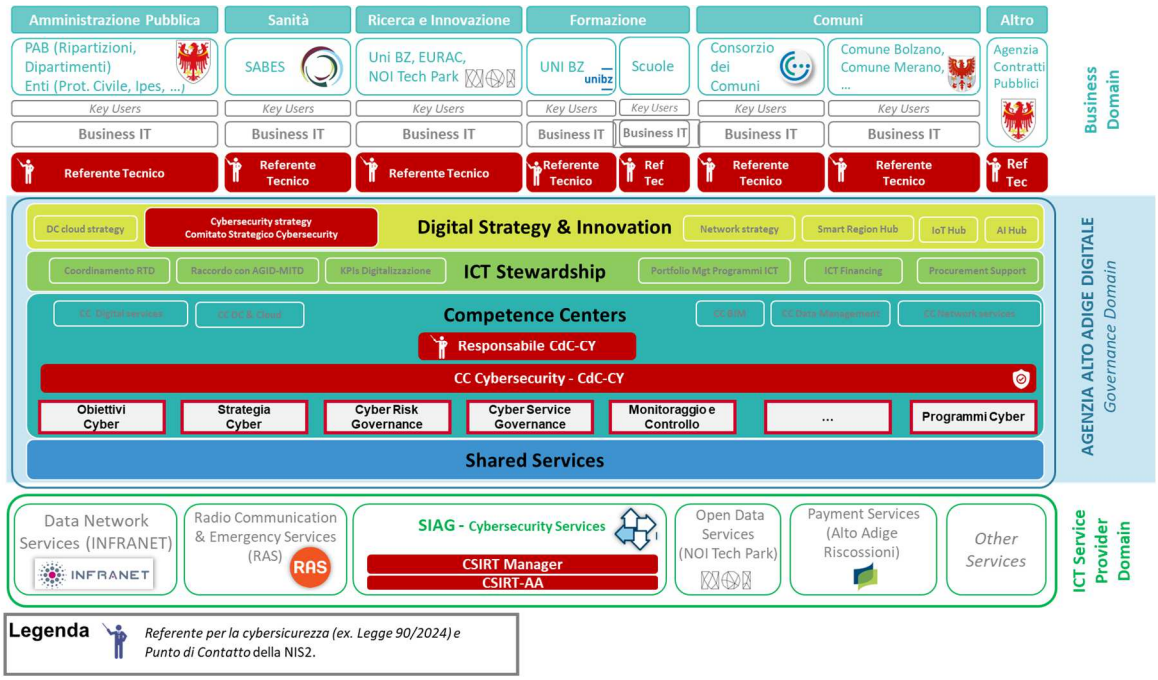
4.3 I ruoli rispetto alla NIS2 e alla Legge 90/2024

Dal punto di vista normativo, la Direttiva NIS2 richiede che sia identificato un Referente che funge da "Punto di Contatto" per gli aspetti di cybersecurity mentre la Legge 90/2024 – Art.8.1 richiede l'individuazione di una Struttura per la cybersecurity e, al suo interno, un "*Referente per la cybersicurezza, individuato in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza*" che si ritiene possa coincidere con il Punto di Contatto della NIS2.

Nell'ambito del presente Modello Cyber PAB, si definisce che **ogni Ente provinciale debba identificare, anche in forma associata** (*Rif. 1.2.2*)**, un Referente per la cybersicurezza che assicurino la piena conformità alla normativa**. Nel caso in cui il Referente per la cybersicurezza sia identificato in forma associata fuori dall'ente, quest'ultimo deve identificare comunque un "Referente Tecnico e/o portavoce dell'Ente pubblico".

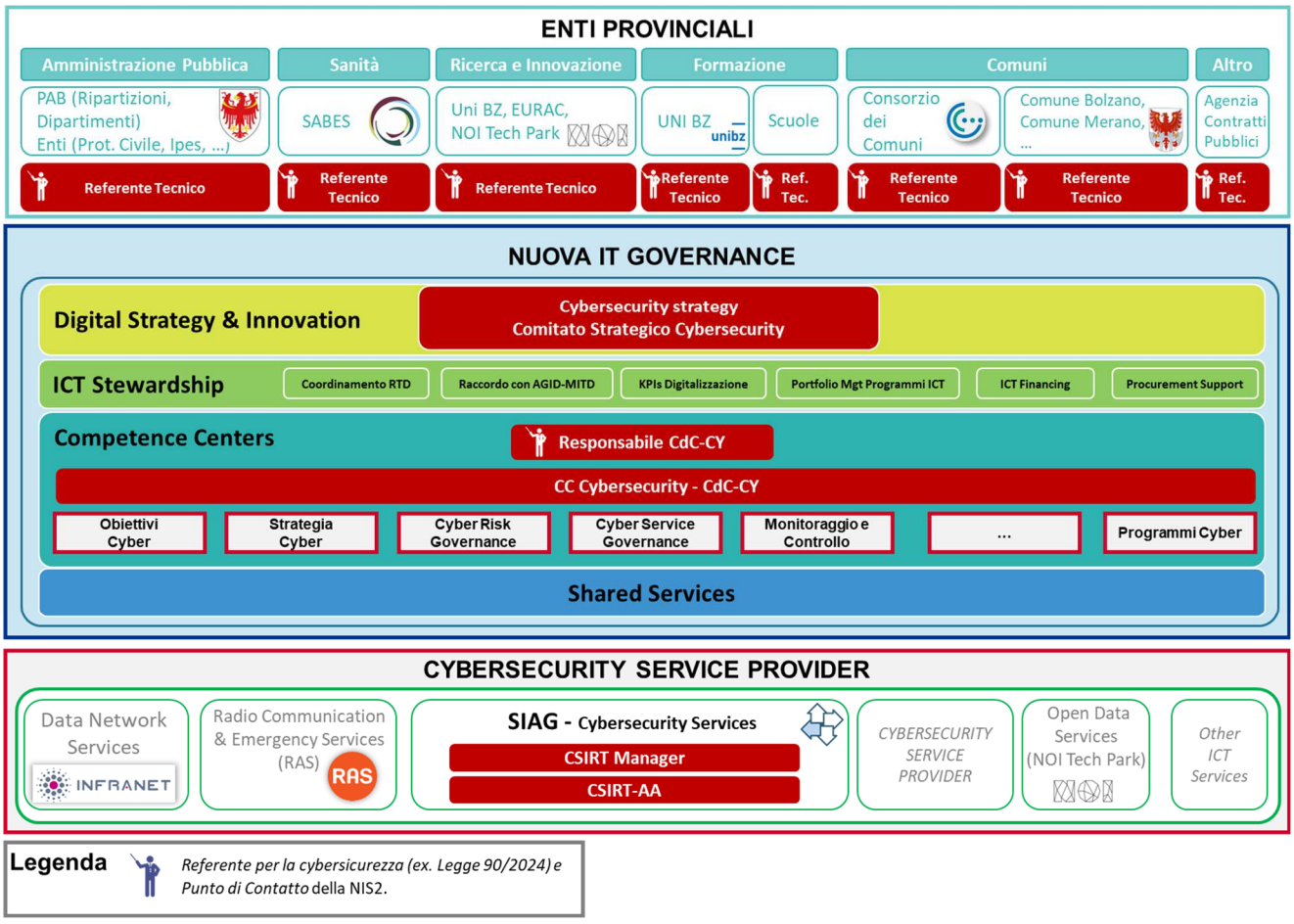
4.4 Modello Cyber PAB – Una rappresentazione complessiva

Di seguito si rappresentano gli attori del Modello Cyber PAB all'interno dello schema concettuale della Nuova Governance Digitale.



Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Tale rappresentazione sottolinea la coerenza del Modello Cyber PAB e del CdC-CY con l'impostazione generale della Nuova Governance Digitale. Una rappresentazione più di sintesi e ristretta alla cybersecurity è la seguente.



Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

5. Competence Center per la Cybersicurezza

5.1 Il Ruolo di governo complessivo

Il **CdC-CY ha un ruolo di governo e controllo in ambito cybersecurity** nell'ambito della Provincia autonoma di Bolzano e degli Enti provinciali correlati. In tale ruolo **analizza i rischi cyber e definisce la strategia di cybersecurity indirizzando iniziative progettuali, servizi di cybersecurity e monitorandone lo stato di avanzamento e la relativa efficacia**.

5.2 Il Ruolo all'interno della futura Agenzia

Il CdC-CY nell'ambito dell'Agenzia ricopre il ruolo di Struttura di Cybersecurity (richiesto dalla Legge 90/2024 – Art.8.1) che provvede:

- Allo **sviluppo delle politiche e delle procedure** di sicurezza delle informazioni;
- Alla **produzione e all'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico**;
- Alla **produzione e all'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni**;
- Alla **produzione e all'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture**;
- Alla **pianificazione e all'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici**;
- Alla **pianificazione e all'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale**;
- Al **monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità** dei sistemi per il loro pronto aggiornamento di sicurezza.

Un elemento fondamentale del piano di attuazione della strategia cyber della Provincia autonoma di Bolzano è la **istituzione del CSIRT-AA che eroga operativamente servizi di analisi delle minacce informatiche emergenti e di risoluzione degli incidenti di cybersecurity**.

5.3 Le Responsabilità

Il CdC-CY ha la responsabilità di articolare, sulla base del dettame normativo e dei più ampi obiettivi provinciali, **la strategia, le aspettative e la politica di gestione del rischio di cybersecurity della Provincia autonoma di Bolzano, assicurandone la comunicazione, la declinazione in piani di azione e il monitoraggio complessivo delle iniziative e del complessivo profilo del rischio cyber**.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

A tal fine il CdC-CY **analizza e considera le aspettative degli stakeholder**, le **dipendenze e requisiti normativi**, le **priorità, i vincoli per lo sviluppo di un framework per la gestione dei rischi cyber** che comprenda l'adozione di specifici presidi quali, ad esempio, quello relativo ai servizi operativi erogati dal CSIRT-AA nell'ambito della analisi delle minacce informatiche emergenti e della risoluzione degli incidenti di cybersecurity.

Il CdC-CY assicura una adeguata **definizione di ruoli e responsabilità nell'ambito della cybersecurity**, all'interno del contesto organizzativo della Provincia autonoma di Bolzano e dei propri fornitori di servizi. È suo compito **stabilire le più ampie politiche di cybersecurity che possano fornire una base comune alle specifiche declinazioni che i differenti Enti dovranno applicare** per cogliere le specificità del proprio contesto; deve prestare particolare attenzione alla definizione delle politiche e delle linee guida per i processi di gestione del rischio della catena di approvvigionamento informatico.

Deve assicurare adeguato **monitoraggio e supervisione rispetto ai risultati delle attività e delle prestazioni di gestione del rischio di cybersecurity al fine di informare, migliorare e adeguare la strategia di gestione del rischio**.

5.4 Le Attività

In tal senso la Funzione il CdC-CY declina le responsabilità nelle seguenti attività, principalmente associate alla **funzione "GOVERN" del CSF 2.0** e finalizzate all'analisi del contesto organizzativo, all'istituzione della strategia di cybersecurity, alla gestione dei rischi di cybersecurity e della catena di fornitura della sicurezza informatica, alla definizione di ruoli, responsabilità e politiche e alla supervisione della attuazione efficace della strategia di cybersecurity:

- Indentificare e analizzare il contesto della Provincia Autonoma di Bolzano e gli Enti a questa collegati;
- Recepire e analizzare gli obiettivi e le strategie provinciali con particolare riferimento a quanto relativo alla digitalizzazione della pubblica amministrazione e alle relative esigenze del territorio;
- Indentificare, condividere e consolidare gli obiettivi provinciali legati alla cybersecurity;
- Definire la strategia necessaria per il raggiungimento di tali obiettivi;
- Definire e istituire un sistema di gestione per la cybersecurity composto da ruoli, responsabilità, processi e strumenti, per implementare la strategia identificata;
- Definire e istituire un modello organizzativo e operativo complessivo per la gestione dei rischi di cybersecurity;
- Identificare i servizi offerti dai fornitori di servizi di cybersecurity (es. CSIRT-AA) che possono essere integrati e allineati con le strategie e il modello operativo;
- Coordinare il piano delle iniziative progettuali per implementare quanto necessario all'adozione del framework di cybersecurity;

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

- Governare e indirizzare l'erogazione dei servizi comuni di cybersecurity erogati alla Provincia Autonoma di Bolzano e gli Enti a questa collegati;
- Monitorare e analizzare nel continuo le prestazioni dei presidi di cybersecurity implementati;
- Monitorare nel continuo il profilo complessivo di rischio di cybersecurity della Provincia Autonoma di Bolzano e gli Enti a questa collegati.

5.5 Il Referente del CdC-CY

Nell'ambito di tale Competence Center per la Cybersecurity è posizionato il "Referente del CdC-CY" che guida e assicura la definizione e il continuo aggiornamento:

- Delle politiche e delle procedure di sicurezza delle informazioni;
- Dei sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico;
- Dell'organizzazione del sistema per la sicurezza delle informazioni;
- Del piano programmatico per la sicurezza di dati, sistemi e infrastrutture ICT;
- Della pianificazione e della attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici;
- Della pianificazione e dell'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale;
- Al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza.

Il "Referente del CdC-CY" può coincidere per l'Agenzia con il ruolo di "Referente per la cybersicurezza" *(Rif. 1.2.2)*.

6. Enti Provinciali

Come anticipato, gli Enti Provinciali devono identificare al loro interno opportuni ruoli (con le relative responsabilità) in ambito cybersecurity ("**Referente per la cybersicurezza**" e "**Referente Tecnico**").

Il Referente Tecnico, individuato in ciascun Ente ha la responsabilità di fungere da raccordo tra la propria organizzazione e le strutture centralizzate per la Cybersecurity (CdC-CY e Fornitori di servizi centralizzati di cybersecurity). In tale contesto, il Referente Tecnico ha la responsabilità di rendere efficaci le politiche definite e i servizi erogati dalle strutture centrali declinandoli opportunamente all'interno dello specifico. Le responsabilità previste per il ruolo di Referente Tecnico sono:

- Gestire l'implementazione, all'interno del proprio perimetro tecnologico e organizzativo di competenza, delle politiche definite centralmente;

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

- Monitorare l'efficacia delle misure di sicurezza implementate nell'ambito del proprio perimetro di competenza locale;
- Assicurare le risorse e le condizioni per permettere l'erogazione dei servizi di Cybersecurity centralizzati (es. assicurare la opportuna configurazione dei firewall in caso di VA/PT erogato centralmente, identificare il personale che deve partecipare al processo di Cyber Risk Assessment condotto dalla strutture centrali, …);
- Fornire al CdC-CY flussi informativi circa l'efficacia delle misure di sicurezza (es. KRI, KPI), le esigenze e gli obiettivi rilevati localmente;
- Contribuire in maniera organica al monitoraggio degli eventi di sicurezza per gestire globalmente eventuali attacchi e condividere buone pratiche comuni;
- Gestire operativamente, per quanto di competenza dei propri asset, il processo di gestione degli incidenti di cybersecurity lungo tutto il loro ciclo di vita.

Si noti che il **Referente Tecnico** corrisponde al **Referente per la cybersicurezza** nel caso in cui quest'ultimo sia stato identificato all'interno dell'ente e non in forma associata presso un altro soggetto.

7. CSIRT-AA

Nell'ambito di un più ampio governo e controllo dei temi cybersecurity operato dal CdC-CY**, il mandato del CSIRT-AA**, in linea con quanto previsto dalle linee guida ENISA nella costruzione dei CSIRT, sarà quello di **fornire, alla sua constituency (gli Enti provinciali che aderiranno al servizio), supporto e assistenza specialistica nell'analisi dei dati relativi alle minacce informatiche emergenti e nella risoluzione degli incidenti di cybersecurity**. Questo implicherà essere prontamente disponibili per offrire consulenza tecnica, supporto investigativo e soluzioni per affrontare e mitigare gli attacchi informatici.

La missione del CSIRT-AA sarà quella di agevolare la diffusione di informazioni tempestive e immediatamente utilizzabili sulla sicurezza informatica, fornendo avvisi e allerte riguardanti nuovi scenari di rischio, attacchi in corso e tendenze dei fenomeni cibernetici indirizzati a specifici settori, organizzazioni o territori. In questo modo, si contribuirà a migliorare la consapevolezza e la preparazione delle organizzazioni locali nella gestione dei rischi informatici.

Il CSIRT-AA avrà, altresì, il compito di incentivare l'applicazione dei processi di gestione della sicurezza e delle metodologie valutative per il governo della sicurezza cibernetica. Ciò implicherà promuovere l'adozione di best practice e linee guida per garantire la protezione delle risorse digitali e favorire la cultura della sicurezza informatica all'interno della sua constituency (cfr. Allegato Modello organizzativo CSIRT-AA).

Il CSIRT-AA è quindi l'unità operativa in ambito sicurezza informatica promossa dalla Provincia Autonoma di Bolzano e attiva presso Informatica Alto Adige. Opererà a livello territoriale a supporto di tutti gli enti pubblici che ne faranno esplicita richiesta.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Il CSIRT-AA erogherà servizi e linee guida per la gestione completa delle minacce e degli incidenti informatici prevedendo altresì anche un supporto attivo ai membri della constituency i quali, a loro volta, avranno facoltà di declinare tali indicazioni sulla propria realtà di appartenenza, in maniera autonoma, al fine di renderle quanto più efficace possibile.

L'organizzazione ibrida del CSIRT-AA, con le sue caratteristiche di campus incorporato, combinerà gli elementi di un'organizzazione centralizzata con un approccio distribuito. In dettaglio, il CSIRT-AA avrà una struttura centralizzata presso Informatica Alto Adige, con risorse appositamente dedicate, che fungerà da centro di coordinamento e punto di riferimento per tutte le attività operative del CSIRT.

Allo stesso tempo, grazie alla messa a disposizione di personale da parte di ogni ente (almeno uno per membro della constituency – Referente Tecnico), il CSIRT-AA sarà, virtualmente, presente sul campo per meglio supportare ed indirizzare le varie amministrazioni sui servizi offerti.

Si faccia riferimento al documento “Modello organizzativo CSIRT Territoriale dell’Alto Adige” per ulteriori dettagli.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Organisationsmodell
CSIRT-AA

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Zusammenfassung

1 Vorwort und Zweck 3
2 Akronyme 3
3 Referenzen 4
4 Mandat und Auftrag 5
5 Organisationsmodell 6
6 Constituency 7
7 Rollen und Verantwortlichkeiten 10
8 Dienstleistungskatalog 10
8.1 BASIC-Akkreditierung 11
8.1.1 Situational Awareness 11
8.2 INTERMEDIATE-Akkreditierung 11
8.2.1 Vulnerability Management 12
8.2.2 Knowledge Transfer 13
8.3 ADVANCED-Akkreditierung 16
8.3.1 Information Security Event Management 16
8.3.2 Information Security Incident Management 18

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

1 Vorwort und Zweck

Ziel dieses Dokuments ist es, eine detaillierte Beschreibung des für Südtirol zuständigen CSIRT (im Folgenden „CSIRT-AA“) zu erstellen. Darunter insbesondere:

- das Mandat,
- die Mission,
- die Organisationsstruktur,
- der anfängliche Zuständigkeitsbereich (Constituency),
- die Rollen und Verantwortlichkeiten,
- die angebotenen Dienstleistungen.

Dabei soll eine klare und umfassende Informationsbasis im Hinblick auf das CSIRT-AA geschaffen werden, um unter den Beteiligten das Verständnis seiner Funktionen und Dienstleistungen zu fördern.

Zweck dieses Dokuments ist es, eine genaue und transparente Beschreibung der Zuständigkeiten der CSIRT-AA, seiner operativen Funktionen, seiner Rolle bei der Bewältigung von Cybersicherheitsvorfällen und seiner Beziehung zu den Mitgliedsorganisationen der Constituency zu geben. Das Dokument stützt sich dabei auf Richtlinien, Vorschriften und Bestimmungen, die von den zuständigen Behörden festgelegt wurden, um die Einhaltung der Cybersicherheitsstandards und die Übereinstimmung mit national und international anerkannten bewährten Verfahren zu gewährleisten.

Dieses Dokument dient als Referenz für alle, die sich einen detaillierten Überblick über das CSIRT-AA verschaffen wollen, einschließlich der Mitglieder des Teams selbst, der beteiligten Organisationen, der zuständigen Behörden und anderer an der IT-Sicherheit des Landes Südtirol interessierter Stellen.

Den Nutzer:innen wird empfohlen, sich anhand dieses Dokuments ein umfassendes Bild von den Aktivitäten und Dienstleistungen des CSIRT-AA zu machen, um die Zusammenarbeit und die effektive Kommunikation zwischen dem CSIRT-AA und den beteiligten Akteur:innen zu erleichtern.

2 Akronyme

Akronym	Bedeutung
ACN	Agenzia per la cybersicurezza nazionale/Nationale Agentur für Cybersicherheit
CSIRT	Computer Security Incident Response Team
CSIRT-AA	für Südtirol zuständiges CSIRT
CERT	Computer Emergency Response Team

Akronym	Bedeutung
ENISA	European Union Agency for Cybersecurity
FIRST	Forum of Incident Response and Security Teams
GVCC	Consorzio dei Comuni della Provincia di Bolzano/Südtiroler Gemeindenverband Genossenschaft
PAL	Lokale öffentliche Verwaltungen
SOC	Security Operations Center

3 Referenzen

Abkürzung	Dokument	Anmerkung, Link
CSIRT set-up guide	ENISA-Leitlinien für die Einrichtung eines CSIRT	https://www.enisa.europa.eu/publications/csirt-setting-up-guide/@@download/fullReport
Establishing a CSIRT	FIRST-Leitlinien für die Implementierung eines CSIRT	https://www.first.org/resources/guides/Establishing-CSIRT-v1.2.pdf
LL CSIRT	ACN-Leitlinien für die Einrichtung eines CSIRT	https://www.acn.gov.it/portale/documents/d/guest/acn_linee_guida_csirt
LL CSIRT auf Landesebene	Leitlinien für die Entwicklung und Definition des nationalen Referenzmodells für regionale CERT	https://docs.italia.it/AgID/documenti-in-consultazione/lg-cert-regionali/it/bozza/index.html
SIM3	SIM3 v2 interim – Security Incident Management Maturity Model	https://opencsirt.org/csirt-maturity/sim3-and-references/
SOC and CSIRT set-up guide	ENISA-Richtlinien für die Implementierung von SOC- und CSIRT-Diensten	https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc/@@download/fullReport

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Abkürzung	Dokument	Anmerkung, Link
Klassifizierung Vorfälle ENISA	von der ENISA vorgeschlagene Klassifizierung von Sicherheitsvorfällen	https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy
Klassifizierung Vorfälle Perimetro Nazionale di Sicurezza	im nationalen Kontext vorgesehene Klassifizierung von Sicherheitsvorfällen	https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg

4 Mandat und Auftrag

Das Mandat des CSIRT-AA besteht darin, im Einklang mit den ENISA-Leitlinien für den Aufbau von CSIRT, seiner Constituency fachliche Unterstützung und Hilfe bei der Analyse von Daten im Zusammenhang mit aufkommenden Cyberbedrohungen und der Lösung von Cybersicherheitsvorfällen zu bieten. Dazu gehört auch, dass das CSIRT in der Lage ist, zeitnah technische Beratung, Unterstützung bei Nachforschungen und Lösungen zur Bekämpfung und Eindämmung von Cyberangriffen zu bieten.

Die Aufgabe des CSIRT-AA besteht darin, die frühzeitige Verbreitung unmittelbar verwertbarer Informationen zur Cybersicherheit zu erleichtern, indem es Warnungen und Hinweise auf neue Risikoszenarien, aktuelle Angriffe und Tendenzen bei Cyberphänomenen gibt, die auf bestimmte Sektoren, Organisationen oder Gebiete abzielen. Dies wird dazu beitragen, das Bewusstsein und die Vorbereitung lokaler Organisationen im Umgang mit Cyberrisiken zu verbessern.

Das CSIRT-AA hat darüber hinaus die Aufgabe, die Anwendung von Sicherheitsmanagementprozessen und Evaluierungsmethoden für die Governance im Bereich der Cybersicherheit zu fördern. Dazu gehört auch die Förderung der Übernahme bewährter Verfahren und Leitlinien, um den Schutz digitaler Güter zu gewährleisten und eine Kultur der Cybersicherheit in seiner Constituency zu fördern.

Ein weiterer zentraler Aspekt des Mandats des CSIRT-AA ist die Zusammenarbeit und Kooperation mit anderen nationalen und internationalen Organisationen bei der Stärkung und Verbesserung der Fähigkeiten zur Verteidigung im Bereich der Cybersicherheit. Dazu gehören der Austausch von Informationen, die Teilnahme an gemeinsamen Übungen und die Weitergabe bewährter Praktiken an andere italienische und nicht-italienische Einrichtungen, die auf dem Gebiet der Cybersicherheit tätig sind.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Außerdem setzt sich das CSIRT-AA dafür ein, die Fachkenntnisse von mit Cybersicherheit Beauftragten zu verbessern und die Sensibilisierung für diese Fragen auf lokaler Ebene zu verstärken. Dies bedeutet, dass kontinuierliche Schulungen, die Aufklärung über Cybersicherheit und die Verbreitung entsprechender Informationen gefördert werden, um das Bewusstsein der lokalen Zielgruppe für Cyberbedrohungen zu schärfen und sie besser darauf vorzubereiten.

5 Organisationsmodell

In Übereinstimmung mit dem allgemeinen Cybersecurity-Organisationsmodell der Autonomen Provinz Bozen (im Folgenden auch „Cyber-Modell Südtirol“) und dem Cybersecurity-Kompetenzzentrum der Agentur Südtirol Digital (im Folgenden „Kompetenzzentrum“) ist das CSIRT-AA eine grundlegende operative Einheit im Bereich der Cybersecurity in der Autonomen Provinz Bozen, die bei und mit der operativen Unterstützung der Südtiroler Informatik AG, die als Trägerorganisation fungiert, arbeitet. Sie ist auf dem gesamten Landesgebiet tätig und unterstützt alle öffentlichen Einrichtungen, die dies ausdrücklich beantragen, sowie private Einrichtungen bei bestimmten Dienstleistungen.

Unter Bezugnahme auf die AgID-Leitlinien für den Aufbau gebietsbezogener CSIRT wird innerhalb des CSIRT-AA ein **Modell der geteilten Zuständigkeit** gemäß einer **hybriden Organisation mit eingebetteten Campus-Merkmalen** angewandt.

Dieses Modell der geteilten Zuständigkeit fördert insbesondere eine enge Zusammenarbeit und einen wirksamen Informationsaustausch mit den Einrichtungen und Organisationen, die zu seiner Constituency gehören. Dieser Ansatz zielt darauf ab, die Zusammenarbeit im Umgang mit Cybersicherheitsvorfällen zu fördern und einen raschen und wirksamen Austausch von Informationen und Ressourcen zwischen den verschiedenen beteiligten Stellen zu ermöglichen, um so ein solides und synergetisches Netzwerk zur wirksamen Bekämpfung von Cyberbedrohungen zu schaffen.

Das CSIRT-AA stellt Leitlinien für eine lückenlose Handhabung von Cyber-Bedrohungen und -Vorfällen sowie aktive Unterstützung für die Mitglieder der Constituency bereit, die dadurch ihrerseits in der Lage sein werden, die Leitlinien eigenständig auf ihren eigenen Kontext anzupassen, um sie so effektiv wie möglich zu gestalten.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Die hybride Organisation des CSIRT-AA mit ihren eingebetteten Campus-Merkmalen kombiniert die Elemente einer **zentralisierten Organisation mit einem dezentralen Ansatz**. Im Detail verfügt das CSIRT-AA über eine zentralisierte Struktur in der Südtiroler Informatik AG, die mit eigens dafür vorgesehenen Ressourcen ausgestattet ist und als Koordinationszentrum und Bezugspunkt für alle operativen CSIRT-Aktivitäten dient.

Gleichzeitig ist das CSIRT-AA dank der Bereitstellung von Personal aus jeder Körperschaft (mindestens eine technische Kontaktperson pro Constituency) virtuell vor Ort präsent, um die verschiedenen Verwaltungen bei den angebotenen Diensten besser zu unterstützen und anzuleiten.

Dieser hybride Ansatz gewährleistet eine geeignete räumliche Abdeckung und die Fähigkeit, zeitnah auf IT-Sicherheitsvorfälle in ganz Südtirol zu reagieren. So können außerdem sowohl die Erfahrung und die zentralisierten Ressourcen der Südtiroler Informatik AG als auch das lokale Wissen und die speziellen Fähigkeiten der verschiedenen zur Constituency gehörenden Einrichtungen genutzt werden.

Auf diese Weise ist das CSIRT-AA in der Lage, sich an die spezifischen Bedürfnisse Südtirols anzupassen und eine rechtzeitige und wirksame Reaktion auf Cyber-Bedrohungen zu liefern und so zum Schutz und zur Sicherheit der gesamten Gemeinschaft beizutragen.

6 Constituency

Das CSIRT-AA bietet seine Dienste einem breiten Zuständigkeitsbereich an, der zunächst aus mehreren öffentlichen Einrichtungen in Südtirol besteht. Konkret handelt es sich um technische Kontaktpersonen der :

- Südtiroler Informatik AG
- Region Trentino-Südtirol
- ASDAA/SABES
- öffentlichen Verwaltung der Autonomen Provinz Bozen
- des Amtes für Zivilschutz der Autonomen Provinz Bozen
- des Gemeindenverbandes der Provinz Bozen und der Gemeinden Bozen, Meran und Vahrn

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Diese Einrichtungen repräsentieren eine Vielzahl von Sektoren und Organisationen, die eine entscheidende Rolle bei der Förderung des Wohlergehens, der Sicherheit und der Entwicklung in Südtirol spielen. Sie sind an Verwaltungstätigkeiten, der Erbringung grundlegender Dienstleistungen, der Verwaltung des öffentlichen Gesundheitswesens, an IT- und Katastrophenschutzmaßnahmen beteiligt.

Das CSIRT-AA sieht auch die Möglichkeit vor, dass andere öffentliche Verwaltungen und private Einrichtungen um Aufnahme in die Constituency ersuchen. Diese Einrichtungen werden einem **Akkreditierungsverfahren** unterzogen, das per Formular auf der CSIRT-AA-Website (<https://cert-aa.provincia.bz.it/>) beantragt werden kann.

Diese Initiative wird zur Stärkung der Widerstandsfähigkeit und des Schutzes der gesamten Gemeinschaft beitragen, indem sie den Austausch von Wissen, Erfahrungen und bewährten Praktiken zwischen den CSIRT-AA-Mitgliedsorganisationen und den neuen Einrichtungen, die der Gruppe beitreten sollen, erleichtert.

Darüber hinaus wird das CSIRT-AA beim CSIRT Italia als Referenzpunkt zwischen nationalen und lokalen Einrichtungen akkreditiert.

Es sind zwei verschiedene Formen der Akkreditierung vorgesehen:

1. *Akkreditierung des CSIRT-AA beim CSIRT Italia*: Das CSIRT-AA wird die Akkreditierung beim CSIRT Italia beantragen, um Teil des CSIRT Italia zu werden und dessen Dienste nutzen zu können. Dies wird die Zusammenarbeit und den Informationsaustausch mit anderen regionalen und nationalen CERT/CSIRT erleichtern und zu einer noch wirksameren und stärker koordinierten Reaktion auf Cybersicherheitsvorfälle auch außerhalb von Südtirol beitragen. Durch diese enge Zusammenarbeit mit dem CSIRT Italia wird das CSIRT-AA einen Beitrag zur Schaffung eines robusten und widerstandsfähigen Cybersicherheits-Ökosystems auf lokaler und nationaler Ebene leisten und mit anderen akkreditierten Einrichtungen zusammenarbeiten, um Cyberbedrohungen koordiniert und rechtzeitig zu bekämpfen.
2. *Akkreditierung von lokalen öffentlichen Verwaltungen und privaten Unternehmen in Südtirol beim CSIRT-AA*: Einzelne lokale öffentliche Verwaltungen können eine Akkreditierung beim CSIRT-AA beantragen, um Teil der Constituency zu werden. Es wird auch eine Form der Akkreditierung für Unternehmen in Südtirol geben, die sich speziell auf den Austausch von Informationen über Cyber-Bedrohungen bezieht. Die lokalen öffentlichen Verwaltungen, die die vom CSIRT-AA angebotenen Dienste in Anspruch nehmen möchten, müssen die Akkreditierung über die für IT-Sicherheit

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Beauftragten der lokalen öffentlichen Verwaltung beantragen, die sich über die entsprechenden Kanäle gemäß dem auf der offiziellen Website veröffentlichten Verfahren mit dem CSIRT-AA in Verbindung setzen.

Die Akkreditierung kann folgendermaßen erfolgen:

Akkreditierungsstufen	Dienste	Verfügbarkeit	Kosten
BASIC	• Situational Awareness	öffentliche Verwaltungen in Italien und private Unternehmen (Südtirol)	Kostenlos
INTERMEDIATE	• Vulnerability Management • Knowledge Transfer	Öffentliche Verwaltungen in Südtirol	Gebühr (*fee*) für die einzelnen Dienste und abhängig von der Größe der öffentlichen Verwaltung
ADVANCED	• Information Security Event Management • Information Security Incident Management	Öffentliche Verwaltungen in Südtirol	Gebühr (*fee*) für die einzelnen Dienste und abhängig von der Größe der öffentlichen Verwaltung

TABELLE1 : AKKREDITIERUNGSSTUFEN

Die Akkreditierung für eine bestimmte Stufe führt zum Erwerb der in den vorhergehenden Stufen enthaltenen Dienste. Das vollständige Profil des CSIRT-AA ist im Dokument RFC 2350 auf der offiziellen Website zu finden (Link: <https://cert-aa.provincia.bz.it/upload/rfc2350.Txt>).

Im Zeitraum 2025-2027 werden die anfänglichen Kosten für die Formalisierung, Umsetzung und Erbringung von Dienstleistungen innerhalb des CSIRT-AA von der Autonomen Provinz Bozen getragen.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

7 Rollen und Verantwortlichkeiten

Wie bereits erwähnt wird das für Südtirol zuständige CSIRT (CSIRT-AA) von der Autonomen Provinz Bozen eingerichtet, ist Teil des umfassenderen „Cyber-Modell Südtirol“ der APB und hat seinen operativen Sitz in der Südtiroler Informatik AG.

Es arbeitet mit einem Modell der geteilten Zuständigkeit, um die aktive Beteiligung und die gemeinsame Verantwortung der Mitglieder der Constituency zu fördern. Die folgenden Gremien werden eingerichtet:

- **Core Team:** Das CSIRT-AA wird operativ von einer als Kernteam bezeichneten Gruppe koordiniert, die die Projektaktivitäten rund um das CSIRT-AA leitet, die Vorgaben des Kompetenzzentrums in Übereinstimmung mit der im Cyber-Modell Südtirol definierten strategischen Linie umsetzt und die Umsetzung der Dienste der Südtiroler Informatik AG überprüft. Das Kernteam besteht aus einem:r CSIRT-Manager und der Kontaktperson für Technik, die von den Mitgliedern der Constituency delegiert werden. Die Mitglieder des Kernteams, die mindestens alle zwei Monate zusammenkommen, sind befugt, weitere Mitglieder vorzuschlagen, die ausschließlich die Einrichtungen der Constituency vertreten.
- **CSIRT-AA Manager:** Die CSIRT-AA wird von einem:r CSIRT-Manager geleitet, der:die für die operativen Tätigkeiten, die Koordinierung der Reaktion auf Vorfälle und die Verwaltung der CSIRT-AA-Ressourcen verantwortlich ist. Er:sie fungiert als Hauptansprechpartner:in für die Constituency und koordiniert die Aktionen des gesamten technischen Teams.
- **Technik-Team:** Das CSIRT-AA verfügt über ein technisches Team, das bei der Südtiroler Informatik AG angesiedelt ist und sich aus IT-Sicherheitsfachleuten mit interdisziplinären Fähigkeiten zusammensetzt. Diese Gruppe spielt eine entscheidende Rolle beim Umgang mit Zwischenfällen und der Erbringung von Dienstleistungen, wie im nächsten Absatz beschrieben. Mit operativer Unterstützung der technischen Kontaktpersonen der Constituency arbeiten die Mitglieder dieser Gruppe eng zusammen, um auf Sicherheitsvorfälle zu reagieren, Informationen und Empfehlungen auszutauschen und bewährte Verfahren zur Gefahrenabwehr zu entwickeln.

8 Dienstleistungskatalog

Der Dienstleistungskatalog wurde unter Berücksichtigung der Leitlinien von ACN, AgID und ENISA für den Aufbau von CSIRT und SOC entwickelt, um den Mitgliedern der Constituency wertvolle Hilfsmittel für ein umfassendes und zielgerichtetes Management von Cyber-Bedrohungen an die Hand zu geben.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Die Dienste sind in fünf Bereiche ("*Service Areas*") unterteilt, die die Einsatzbereiche eines CSIRT (Ebene 1) definieren. Innerhalb eines jeden dieser Bereiche gibt es eine Reihe von Diensten, die sich wiederum aus operativen Maßnahmen (Funktionen) zusammensetzen.

Die Inhalte sind im Folgenden, aufgeteilt nach Akkreditierungsstufen, beschrieben:

8.1 BASIC-Akkreditierung

Der Zugang zu diesen Diensten ist, nach einer ersten Akkreditierung, kostenlos.

8.1.1 Situational Awareness

Dieser Bereich umfasst alle Dienste, die darauf abzielen, kritische Elemente, die sich auf die Constituency auswirken können, zu identifizieren, verarbeiten, verstehen und kommunizieren. Das Hauptziel ist hier die Erfassung von Daten über relevante Aktivitäten, die sich auf das Lagebild der Constituency auswirken könnten.

8.1.1.1 Data Acquisition

Der Datenerfassungsdienst ist so strukturiert, dass er das Wissen und die Sicht des CSIRT-AA im Verhältnis zu den akkreditierten Einrichtungen erhöht. Auf der Grundlage der erfassten Informationen und Daten passt das CSIRT-AA sein Angebot an Diensten und Aktivitäten zur Verbesserung der Sicherheitslage der akkreditierten Einrichtungen dynamisch an, um die Abdeckung und Wirksamkeit zu maximieren.

Der Dienst soll insbesondere die Informationen der verschiedenen akkreditierten Organisationen in Bezug auf folgende Aspekte erfassen und kartieren:

- Güter im Umkreis, einschließlich der technischen Merkmale und der erwarteten Baselines,
- Informationen, Rollen und Zuständigkeiten in Bezug auf die an der Überwachung und Reaktion auf Sicherheitsvorfälle beteiligten Akteur:innen.

Der Dienst zielt auch darauf ab, aus internen und externen Quellen Informationen und Daten zu beschaffen, die zur Unterstützung der anderen in diesem Dokument beschriebenen Dienste genutzt werden können.

8.2 INTERMEDIATE-Akkreditierung

Der Zugang zu diesen Diensten erfolgt über eine erste Akkreditierungsphase. Etwaige Kosten werden auf der Grundlage des Umfangs der öffentlichen Verwaltung in Südtirol festgelegt, die als einzige berechtigt ist,

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

den Zugang zu beantragen, unbeschadet der bereits bestehenden finanziellen Deckung für den Zeitraum 2025-2027 durch die APB.

8.2.1 Vulnerability Management

Dieser Dienst soll alle beim CSIRT-AA akkreditierten Stellen in Fragen des Umgangs mit Schwachstellen und der Reaktion darauf unterstützen. Ziel ist insbesondere Folgendes:

- **Schwachstellen-Koordinierung**: Informationsaustausch und Koordinierung der Aktivitäten mit allen internen und externen Stellen, die am Prozess der Offenlegung von Schwachstellen beteiligt sind,
- **Offenlegung von Schwachstellen**: Weitergabe von Informationen über bekannte Schwachstellen an die Constituency, um die Vorbeugung, Identifizierung und Behebung/Entschärfung von Schwachstellen zu ermöglichen,
- **Reaktion auf Schwachstellen**: aktive Nutzung von Informationen über bekannte Schwachstellen mit dem Ziel, diese zu verhindern, zu entdecken und zu entschärfen.

Es folgt eine ausführliche Erörterung der angebotenen Aktivitäten.

8.2.1.1 Vulnerability Coordination

Die Koordinierung der Aktivitäten umfasst die Bereitstellung von Anleitungen und Informationen zur Behebung von Schwachstellen sowie deren verantwortungsvolle Verbreitung in der Constituency, um das Bewusstsein zu fördern und die Sicherheitslage zu verbessern.

Insbesondere ist es Aufgabe des CSIRT-AA, die Mitglieder der Constituency über neu aufgetretene Schwachstellen zu informieren und zu benachrichtigen. Das CSIRT-AA ist auch für die Koordinierung des Informationsaustauschs zwischen allen Beteiligten, wie z. B. Dritten oder anderen Gemeinschaften, zuständig, um eine korrekte Zusammenarbeit zur Behebung von Schwachstellen zu ermöglichen.

Darüber hinaus ist das CSIRT-AA auch für die Zusammenarbeit mit den verschiedenen Interessengruppen zuständig und koordiniert diese, um sicherzustellen, dass die Informationen auf verantwortungsvolle und präzise Weise an die Betroffenen weitergegeben werden.

8.2.1.2 Vulnerability Disclosure

Der Informationsaustausch mit der CSIRT-AA-Gemeinschaft zielt darauf ab, die Fähigkeiten zur Vorbeugung, Erkennung und Behebung von Schwachstellen zu verbessern.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Das CSIRT-AA ist bestrebt, Richtlinien und Verfahren zur Unterstützung des Austauschs über Schwachstellen und der Offenlegung von Informationen bereitzustellen und weiterzugeben, um die Methoden für einen präzisen und verantwortungsvollen Informationsaustausch klar zu definieren.

Zweitens ist das CSIRT-AA für die Entwicklung von Informationskampagnen durch gezielte Ankündigungen und Mitteilungen zuständig, um die Constituency zu informieren oder Informationen über neue, noch nicht identifizierte Schwachstellen zu veröffentlichen. Diese Maßnahme dient dazu, die Sicherheitsvorkehrungen der beteiligten Stellen so anzupassen, dass die Ausnutzung der Schwachstelle eingedämmt oder verhindert wird, oder dass sie entdeckt wird, falls sie bereits im Gange ist. Wenn neue Sicherheitslücken festgestellt werden, die ihre Systeme oder Anwendungen beeinträchtigen könnten, werden die Organisationen rechtzeitig benachrichtigt und gewarnt.

Das CSIRT-AA steht auch zur Verfügung, um Rückmeldungen in Bezug auf Technik und Vorgehensweisen an alle akkreditierten Einrichtungen zu geben, die um Beratung zu bereits bekannten oder noch unbekannten Schwachstellen bitten.

8.2.1.3 Vulnerability Response

Der Zweck dieses Dienstes besteht darin, festzustellen, ob eine gemeldete Sicherheitslücke in den Systemen eines Mitglieds der Constituency vorhanden ist, oftmals durch eine aktive Suche nach dem Vorhandensein einer solchen Sicherheitslücke. Dies kann auch Folgemaßnahmen zur Behebung oder Entschärfung der Schwachstelle durch die Verteilung von Patches oder Workarounds enthalten.

Der Dienst umfasst die Erkennung und/oder das Scannen bekannter Schwachstellen in den eingesetzten Systemen und ihre Behebung und/oder Entschärfung, um ihre Ausnutzung zu verhindern – in der Regel durch die rechtzeitige Anwendung von Patches oder anderen Lösungen, die von den Anbietern veröffentlicht werden.

8.2.2 Knowledge Transfer

Das CSIRT-AA beteiligt sich aktiv an Maßnahmen zum Wissensaustausch, was von größter Bedeutung ist, da dies den Nutzer:innen die erworbenen Kenntnisse und Fähigkeiten vermittelt. Wenn diese weitergegeben werden, wirken sie sich positiv auf die Fähigkeit der gesamten Organisation aus, Cybersicherheitsbedrohungen zu erkennen, abzuschwächen und zu verhindern. Die verschiedenen Maßnahmen werden im Folgenden beschrieben.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

8.2.2.1 Awareness Building

Das CSIRT-AA unterstützt die allgemeine Verbesserung der Sicherheitslage in der Constituency durch den Aufbau von Kompetenzen, die ihm eine bestmögliche Steuerung der Informationssicherheit innerhalb der Organisation ermöglichen.

Zu diesem Zweck baut das CSIRT-AA auf einen kontinuierlichen Prozess der Suche und Korrelation von Informationen, die sich stets auf aktuelle Ereignisse beziehen und den Nutzer:innen einen Mehrwert bieten und Bewusstsein schaffen.

Dieses Wissen wird in Informationsmaterial zusammengefasst, das spontan in verschiedenen Formaten (Präsentationen, Videos, Broschüren, Newsletter, Bulletins usw.) verwendet und über verschiedene Plattformen verbreitet werden kann.

Das CSIRT-AA verbreitet auch Informationen zur Computersicherheit, um das Bewusstsein der Nutzer:innen der Constituency zu schärfen und sie bei der Umsetzung bewährter Sicherheitsverfahren zu unterstützen.

Ein Schlüsselfaktor, den das CSIRT-AA berücksichtigt, ist die kontinuierliche Entwicklung und Pflege von Beziehungen zu Branchenexpert:innen und anderen Organisationen, einschließlich anderer CSIRT, um ein Netzwerk zu schaffen, das sich gegenseitig bei dem Erreichen der im Mandat festgelegten Ziele unterstützen kann.

8.2.2.2 Training and Education

Das CSIRT-AA bietet dem Personal der Constituency Schulungen zu Themen rund um Computer- und Informationssicherheit sowie den Umgang mit Vorfällen an, um die Kenntnisse und Fähigkeiten des Personals zu verbessern.

Zunächst analysiert, bestimmt und dokumentiert das CSIRT-AA die Bedürfnisse – in Bezug auf Wissen, Fähigkeiten und Fertigkeiten – der Constituency, um geeignetes Schulungsmaterial zu entwickeln, das auf die Bedürfnisse der Zielgruppe abgestimmt ist. Auf der Grundlage der gesammelten Informationen wird Bildungs-, Schulungs- und Lehrmaterial entwickelt und über die für die Zielgruppe und den Inhalt am besten geeigneten Schulungskanäle verbreitet. Diese Unterstützung und Weitergabe erfolgt über zuvor definierte Kanäle und Prozesse.

Das CSIRT-AA wird auch ein Tutoring-Verfahren für Ressourcen entwickeln, das spezialisierten Mitarbeiter:innen mit mehrjähriger Erfahrung die Möglichkeit gibt, Wissen und Perspektiven mit den

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Nutzer:innen der Constituency zu teilen. In Zusammenhang damit wird das CSIRT-AA auch einen Karriereentwicklungsplan für das Support-Personal entwickeln.

8.2.2.3 Exercises

Im Anschluss an die theoretischen Aktivitäten führt das CSIRT-AA praktische Übungen durch, die sich sowohl an seine Mitglieder als auch an die akkreditierten Einrichtungen und deren Mitarbeiter:innen richten. Ähnlich wie oben beschrieben und daher im Einklang mit der bereits für die theoretischen Sitzungen beschriebenen Methodik entwickelt das CSIRT-AA das Material basierend auf den Schulungszielen, die entsprechend dem Organisations- und Sicherheitskontext festgelegt wurden.

Die Aktivitäten werden von spezialisiertem Personal durchgeführt und stellen Szenarien und Situationen dar, die gezielt entwickelt wurden, um die Reaktionsfähigkeit der Mitarbeiter:innen in Bezug auf Effizienz und Effektivität zu verbessern.

Am Ende der Aktivitäten gibt das CSIRT-AA den Teilnehmer:innen schriftliches Feedback in Form eines Berichts über die durchgeführten Aktivitäten und die dabei gemachten Beobachtungen. Dabei werden Verbesserungsmöglichkeiten und die für das Erreichen der Ziele notwendigen Maßnahmen besonders hervorgehoben.

8.2.2.4 Technical and Policy Advisor

Das CSIRT-AA unterstützt die Constituency bzw. die beteiligten Schlüsselpersonen bei der Festlegung spezifischer Strategien und Verfahren, um geeignete Methoden für das Management von Zwischenfällen zu ermöglichen, mit Bedrohungen und Risiken angemessen umzugehen und damit auch die Wirksamkeit der vom CSIRT-AA durchgeführten Aktivitäten zu erhöhen.

Besonderes Augenmerk wird auf die Einhaltung von Vorschriften und das Risikomanagement sowie auf die Aufrechterhaltung des Betriebs (business continuity) und die Wiederherstellung im Katastrophenfall (disaster recovery) gelegt.

In Verbindung mit diesen Aktivitäten wird das CSIRT-AA fortlaufend fachliche technische Unterstützung leisten, um eine kontinuierliche Verbesserung der Infrastruktur in Bezug auf Sicherheitsgüter und -instrumente zu gewährleisten, mit dem Ziel einer allgemeinen Verbesserung der Sicherheitslage, der Betriebsmethoden und der angewandten bewährten Verfahren.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

8.3 ADVANCED-Akkreditierung

Der Zugang zu diesen Diensten kann über eine erste Akkreditierungsphase erfolgen. Etwaige Kosten werden auf der Grundlage des Umfangs der öffentlichen Verwaltung in Südtirol festgelegt, die als einzige berechtigt ist, den Zugang zu beantragen, unbeschadet der bereits bestehenden finanziellen Deckung für den Zeitraum 2025-2027 durch die APB.

8.3.1 Information Security Event Management

Dieser Dienst wird sich auf die Vorbereitung, Pflege und Entwicklung von Diensten für die Sammlung, Überwachung und Analyse von Informationen konzentrieren, die von den CSIRT-AA-akkreditierten Stellen ausgetauscht werden. Diese Maßnahmen zielen darauf ab:

- alle Informationen von akkreditierten Stellen (Informationen, Quellen, Anwendungsfälle) optimal zu verwalten,
- Erkenntnisse für Verbesserungen und Aktualisierungen im Hinblick auf geteilte Informationen und Praktiken zu liefern,
- Überwachungsmaßnahmen durchzuführen, um Anomalien oder verdächtige Ereignisse zu identifizieren und zu analysieren,
- Korrelationsmaßnahmen zwischen Ereignissen und den erhaltenen Informationen durchzuführen, um die Sichtbarkeit zu erhöhen und eine genauere und schnellere Identifizierung von sicherheitsrelevanten Vorfällen oder Ereignissen zu ermöglichen.

8.3.1.1 Monitoring and Detection

Der von Alfa angebotene Dienst zielt darauf ab, einen automatisierten und kontinuierlichen Prozess der Verarbeitung von Sicherheitsereignissen zu ermöglichen, mit dem Ziel, Anomalien zu erkennen, die als Sicherheitsvorfälle eingestuft werden können. Dieser Dienst umfasst die Verwaltung von Datenquellen, die Implementierung und Konfiguration von Monitoring-Anwendungsfällen und die Integration von Kontextdaten zur Verbesserung der Korrelation und Analyse von Ereignissen.

Das CSIRT-AA befasst sich insbesondere mit:

- **Protokoll- und Sensorverwaltung**: Gewährleistung eines konstanten Flows von Sicherheitsereignissen durch eine effiziente Verwaltung der verschiedenen Protokoll- und

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Sensorquellen. Auf diese Weise können die Überwachungs- und Analysetools mit den für die Erkennung von Vorfällen erforderlichen Daten versorgt werden.

- **Handhabung von Monitoring-Anwendungsfällen**: Definition, Überprüfung, Aktualisierung und kontinuierliche Verbesserung im Hinblick auf Monitoring-Anwendungsfälle zur Unterstützung der Analyst:innen bei der rechtzeitigen Erkennung von Sicherheitsereignissen. Dieser Prozess umfasst die Konfiguration und Optimierung von Use Cases innerhalb der Monitoring-Infrastruktur.
- **Kontextbezogenes Datenmanagement**: Sammlung und Nutzung von Daten aus Quellen wie Konfigurationsmanagement-Datenbanken (CMDB), Threat-Intelligence-Systemen und Identitäts- und Zugriffsmanagementsystemen (IAM). Diese Daten sind für die Überwachung und Korrelation von Sicherheitsereignissen unerlässlich und verbessern die Fähigkeit, Vorfälle zu identifizieren und zu qualifizieren.

Der Dienst soll eine kontinuierliche Überwachung und einen effizienten Umgang mit Sicherheitsereignissen sicherstellen, um ein hohes Maß an Schutz vor Cyber-Bedrohungen zu gewährleisten.

8.3.1.2 Event Analysis

Das CSIRT-AA führt eingehende Analysen der empfangenen Daten durch, wenn diese in den Kontroll- und Überprüfungsphasen der verschiedenen Anwendungsfälle positiv bewertet werden. Diese Analysen zielen darauf ab, etwaige falsch-positive Meldungen zu beseitigen und im umgekehrten Fall tiefergehende Bewertungen vorzunehmen.

Die Ereigniskorrelation spielt eine entscheidende Rolle bei der Analyse eingehender Informationen, da sie durch die Kombination von Daten aus verschiedenen Quellen und in Bezug auf verschiedene Geräte eine größere Transparenz und Reichweite ermöglicht. Dies verbessert die Geschwindigkeit der Identifizierung, die Genauigkeit der Analyse und die Wirksamkeit der Reaktionsmaßnahmen.

Darüber hinaus führt das CSIRT-AA eine Kategorisierung und Qualifizierung der identifizierten Sicherheitsereignisse durch, so dass sie korrekt als Sicherheitsvorfälle eingestuft werden. Zur Unterstützung dieser Bewertung werden die Auswirkungen und die Dringlichkeit des Ereignisses ermittelt, wodurch das damit verbundene Risiko identifiziert werden kann.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

8.3.2 Information Security Incident Management

Das CSIRT-AA bietet einen Dienst für den Umgang mit Vorfällen im Bereich der Informationssicherheit, der durch den Einsatz eines maßgeschneiderten Trouble-Ticket-Systems unterstützt wird, um einerseits Hinweise auf Taktiken, Techniken und Verfahren gemäß dem Mitre-Attack-Rahmenwerk zu erhalten und andererseits die mit dem nationalen Sicherheitsbereich (Perimetro Nazionale di Sicurezza) und der allgemeineren ENISA-Systematik verbundene Klassifizierung von Vorfällen umzusetzen.

Dabei dient die ISO/IEC 27035 als Referenznorm, durch die den Mitgliedern der Constituency rechtzeitig Leitlinien für den Umgang mit Sicherheitsvorfällen und bei Bedarf operative Unterstützung zur Verfügung gestellt werden.

Das Hauptziel besteht darin, die Organisationen bei der Entwicklung eines strukturierten und wirksamen Konzepts für den Umgang mit Sicherheitsvorfällen zu unterstützen, um die negativen Auswirkungen zu minimieren und den normalen Betrieb schnell wiederherzustellen. Einige der wichtigsten Aktivitäten, die im Rahmen des Dienstes angeboten werden, sind im Folgenden beschrieben.

8.3.2.1 Information Security Incident Report Acceptance

Hierbei wird die Bedeutung eines Systems zur frühzeitigen Erkennung von Informationssicherheitsvorfällen betont. Dies beinhaltet die Einführung von Mechanismen zur Überwachung, Erkennung und Meldung von Sicherheitsereignissen, die auf einen Vorfall hindeuten könnten; diese Dienstleistung wird derzeit vom SOC der Südtiroler Informatik AG erbracht. Eine genaue und detaillierte Aufzeichnung von Vorfällen zu Analyse-, Verfolgungs- und Lernzwecken wird direkt vom CSIRT-AA bereitgestellt.

Im Detail wird das CSIRT-AA definierte und zeitnahe Mechanismen und Verfahren für den Erhalt und die Sammlung von Vorfallberichten der Einrichtungen in der Constituency bereitstellen. Diese werden dann umgehend analysiert, um die Ursache des jeweiligen Vorfalls zu ermitteln und einen Überblick über mögliche Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten zu geben.

8.3.2.2 Information Security Incident Analysis

Die Phase der Vorfallanalyse zielt darauf ab, alle möglichen detaillierten Informationen über die Ursachen, Auswirkungen, Dynamiken und technischen Aspekte eines Sicherheitsvorfalls zu ermitteln und den akkreditierten Einrichtungen zur Verfügung zu stellen.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Das CSIRT-AA führt dann eine erste Analyse des Vorfalls (Triage) durch, klassifiziert nach Schwere und Auswirkung und schließt mit der Zuweisung einer Priorität ab. Darüber hinaus wird die Sammlung und Identifizierung aller Informationen, die für die Analyse und Reaktion auf den Sicherheitsvorfall relevant sind, laufend unterstützt. Eine strukturierte Erfassung ist von größter Bedeutung, um eine vollständige und genaue Erfassung zu gewährleisten, die auch die Wiederverwendung der Daten in den nachfolgenden Phasen ermöglicht.

Das CSIRT-AA koordiniert oder führt direkt technische Analysen durch, wenn dies zur Untersuchung bestimmter Aspekte oder Fragen für notwendig erachtet wird. Ebenso wird Unterstützung bei der Ursachenanalyse geleistet, die äußerst wichtig ist, um strukturelle Schwachstellen zu erkennen, die den Angriff ermöglichten, und um ihn in der Folge einzudämmen.

Außerdem wird das CSIRT-AA dank seiner weitreichenden Übersicht über alle Mitglieder der Constituency die verschiedenen Informationen, die es über frühere Sicherheitsvorfälle erhalten hat, korrelieren und vergleichen, und so die Chancen erweitern, Abhilfe- oder Minderungsmaßnahmen zu ermitteln, die auf das aktuelle Szenario anwendbar sind.

8.3.2.3 Artifact and Forensic Evidence Analysis

Das CSIRT-AA unterstützt die technischen Abläufe bei der Analyse der beschafften Artefakte und der verschiedenen forensischen Beweismittel, wobei es eine für die Aufrechterhaltung der Überwachungskette geeignete Methodik garantiert, um die Integrität, Unbestreitbarkeit und Zulässigkeit der Beweismittel zu wahren.

Diese Analysen betreffen die folgenden Bereiche:

- Extraktion von Informationen aus Medien und Datenträgern, Analyse von Beweismaterial, Vergleich mit zulässigen Quellen und öffentlich zugänglichen Daten zur Bestimmung der exponierten Oberflächen,
- Reverse-Engineering durch statische Analysen von Artefakten mit dem Ziel, ihre Funktionalitäten (z. B. Aktivierungsmethoden, Auswirkungen, Verbreitungsmethoden, Schadensbegrenzung usw.) unabhängig von der Umgebung, in der sie ausgeführt werden können, vollständig zu bestimmen,
- Durchführung von dynamischen Artefakt-Analysen, um das Verhalten in separaten und entsprechend kontrollierten Umgebungen zu bewerten,

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

- vergleichende Analysen mit anderen Artefakten, die in ähnlichen Fällen identifiziert wurden, um mögliche Übereinstimmungen zu ermitteln.

8.3.2.4 Information Security Incident Coordination

Das CSIRT-AA koordiniert darüber hinaus die Reaktion auf Sicherheitsvorfälle, die in seiner Constituency auftreten können.

Diese Maßnahmen zielen hauptsächlich darauf ab, die Wiederherstellung des Betriebs zu unterstützen, wofür Anweisungen für die Durchführung von Korrekturmaßnahmen, die Überprüfung der Wirksamkeit dieser Maßnahmen, die Wiederherstellung der betroffenen Systeme und Anwendungen sowie die Bewertung der Auswirkungen des Vorfalls auf den Betrieb gegeben werden.

Das CSIRT-AA definiert und unterhält sichere, geeignete und zügig einsetzbare Kommunikationskanäle, um eine vertrauliche und direkte Kommunikation mit den Mitgliedern der Constituency zu gewährleisten. Diese Kanäle dienen dem Informationsaustausch mit den von einem Vorfall betroffenen Einrichtungen während der Reaktionsphasen. Zu diesem Zweck ist es wichtig, alle beteiligten Stakeholder, einschließlich Dritter, zu definieren, damit sie alle aktuellen und notwendigen Informationen für die Koordinierung und Durchführung der Aktivitäten erhalten können.

Das CSIRT-AA sammelt und katalogisiert Informationen über den aktuellen Stand der Durchführung von Aktivitäten, um Material und adäquate Unterstützung für eine Analyse nach einem Unfall zu liefern, die die Überprüfung von Prozessen, die Erfassung der gewonnenen Erkenntnisse, die Aktualisierung von Verfahren und die Umsetzung von Präventivmaßnahmen zur Verringerung des Risikos künftiger Vorfälle umfasst.

Es ist die Aufgabe des CSIRT-AA, die Einrichtungen bei der Vorbereitung und Weitergabe gezielter und akkurater Informationen für die Medien zu unterstützen, um präzise, wahrheitsgemäße und kontrollierte Informationen zu übermitteln.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Modello organizzativo
CSIRT Territoriale dell'Alto Adige

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Sommario

1 Premessa e Scopo 3

2 Acronimi 3

3 Riferimenti 4

4 Mandato e Mission 5

5 Modello organizzativo 6

6 Constituency 7

7 Ruoli e responsabilità 9

8 Catalogo dei servizi 10

8.1 Accreditamento BASE 10

8.1.1 Situational Awareness 11

8.2 Accreditamento INTERMEDIO 11

8.2.1 Vulnerability Management 11

8.2.2 Knowledge Transfer 13

8.3 Accreditamento AVANZATO 15

8.3.1 Information Security Event Management 15

8.3.2 Information Security Incident Management 17

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

1 Premessa e Scopo

Il presente documento ha lo scopo di fornire una descrizione dettagliata del CSIRT territoriale dell'Alto Adige (di seguito denominato "**CSIRT-AA**"); nello specifico ne verrà formalizzato:

- il mandato;
- la mission;
- la struttura organizzativa;
- la constituency iniziale;
- i ruoli e le responsabilità;
- i servizi offerti.

Obiettivo è fornire una base informativa chiara e completa sul CSIRT-AA, al fine di promuovere la comprensione delle sue funzioni e dei suoi servizi da parte delle parti interessate.

Tramite questo documento si mira a fornire una descrizione accurata e trasparente delle responsabilità del CSIRT-AA, delle sue funzioni operative, del suo ruolo nella gestione degli incidenti di sicurezza informatica e delle relazioni con le organizzazioni membri della constituency. Il documento si basa su linee guida, regolamenti e disposizioni stabiliti dalle autorità competenti, al fine di garantire l'aderenza alle norme di sicurezza informatica e la conformità con le migliori pratiche riconosciute a livello nazionale ed internazionale.

Questo documento è utilizzato come riferimento per tutti coloro che desiderano acquisire una panoramica approfondita del CSIRT-AA, inclusi i membri del CSIRT stesso, le eventuali organizzazioni coinvolte, le autorità competenti e altre entità interessate alla sicurezza informatica nell'ambito territoriale dell'Alto Adige.

Si raccomanda agli utenti di fare riferimento a questo documento per acquisire una comprensione completa delle attività e dei servizi offerti dal CSIRT-AA al fine di facilitare la cooperazione e la comunicazione efficace tra il CSIRT-AA e le parti interessate coinvolte.

2 Acronimi

Acronimo	Descrizione
ACN	Agenzia per la cybersicurezza nazionale
CSIRT	Computer Security Incident Response Team

Acronimo	Descrizione
CSIRT-AA	CSIRT territoriale dell'Alto Adige
CERT	Computer Emergency Response Team
ENISA	European Union Agency for Cybersecurity
FIRST	Forum of Incident Response and Security Teams
GVCC	Consorzio dei Comuni della Provincia di Bolzano
PAL	Pubbliche Amministrazioni Locali
SOC	Security Operation Center

3 Riferimenti

Abbreviation	Document	Notes
CSIRT setting up guide	Linee guida ENISA per la realizzazione di CSIRT	https://www.enisa.europa.eu/publications/csirt-setting-up-guide/@@download/fullReport
Estabilish CSIRT	Linee guida del FIRST per l'implementazione di CSIRT.	https://www.first.org/resources/guides/Establishing-CSIRT-v1.2.pdf
LG CSIRT	Linee guida ACN per la realizzazione di CSIRT	https://www.acn.gov.it/portale/documents/d/guest/acn_linee_guida_csirt
LG CSIRT territoriali	Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali	https://docs.italia.it/AgID/documenti-in-consultazione/lg-cert-regionali/it/bozza/index.html
SIM3	SIM3 v2 interim – Security Incident Management Maturity Model	https://opencsirt.org/csirt-maturity/sim3-and-references/
SOC and CSIRT set up	Linee guida ENISA per la realizzazione di servizi SOC e CSIRT	https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc/@@download/fullReport

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Abbreviation	Document	Notes
Tassonomia Incidenti ENISA	Tassonomia incidenti di sicurezza suggerita da ENISA	https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy
Tassonomia Incidenti Perimetro	Tassonomia incidenti di sicurezza cprevista dal perimetro di sicurezza nazionale	https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg

4 Mandato e Mission

Il mandato di CSIRT-AA, in linea con quanto previsto dalle linee guida ENISA ed ACN nella costruzione dei CSIRT, è fornire alla sua constituency supporto e assistenza specialistica nell'analisi dei dati relativi alle minacce informatiche emergenti e nella risoluzione degli incidenti di cybersecurity. Questo implica essere prontamente disponibili per offrire consulenza tecnica, supporto investigativo e soluzioni per affrontare e mitigare gli attacchi informatici.

La mission di CSIRT-AA è agevolare la diffusione di informazioni tempestive e immediatamente utilizzabili sulla sicurezza informatica, fornendo avvisi e allerte riguardanti nuovi scenari di rischio, attacchi in corso e tendenze dei fenomeni cibernetici indirizzati a specifici settori, organizzazioni o territori. In questo modo, si contribuirà a migliorare la consapevolezza e la preparazione delle organizzazioni locali nella gestione dei rischi informatici.

CSIRT-AA ha, altresì, il compito di incentivare l'applicazione dei processi di gestione della sicurezza e delle metodologie valutative per il governo della cybersecurity. Ciò implicherà promuovere l'adozione di best practice e linee guida per garantire la protezione delle risorse digitali e favorire la cultura della sicurezza informatica all'interno della sua constituency.

La collaborazione e la cooperazione con altre organizzazioni nazionali ed internazionali nel potenziamento e miglioramento della capacità difensiva in materia di cybersecurity sarà un altro aspetto centrale del mandato del CSIRT-AA. Questo implicherà lo scambio di informazioni, la partecipazione a esercitazioni congiunte e la condivisione delle migliori pratiche con altre entità, italiane e no, che operano nel campo della sicurezza informatica.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

CSIRT-AA si impegna, infine, ad accrescere le competenze specialistiche degli addetti alla sicurezza cibernetica e a migliorare le attività di sensibilizzazione su questi temi a livello locale. Ciò significa promuovere la formazione continua, l'educazione sulla sicurezza informatica e la divulgazione delle informazioni pertinenti per aumentare la consapevolezza e la preparazione della comunità locale nei confronti delle minacce informatiche.

5 Modello organizzativo

In coerenza con il modello organizzativo per la cybersecurity complessivo della Provincia Autonoma di Bolzano (di seguito anche “Modello Cyber PAB”) e del Centro di Competenza Cybersecurity dell’Agenzia Alto Adige Digitale (di seguito anche CdC-CY), il CSIRT-AA è una fondamentale unità operativa in ambito sicurezza informatica istituita presso la Provincia Autonoma di Bolzano e agisce presso e con il supporto operativo di Informatica Alto Adige, che funge da organizzazione ospitante. Opera a livello territoriale a supporto di tutti gli enti pubblici che ne faranno esplicita richiesta nonché di quelli privati su specifici servizi.

In riferimento a quanto previsto dalle linee guida AgID in merito alla costruzione di CSIRT Territoriali, all’interno del CSIRT-AA è adottato un **modello di autorità condivisa** secondo un'**organizzazione ibrida con caratteristiche di campus incorporato**.

Nello specifico, il modello di autorità condiviso di CSIRT-AA favorisce una stretta collaborazione e uno scambio informativo efficace con gli enti e le organizzazioni membri della sua constituency. Tale approccio mira a promuovere la cooperazione nel campo della gestione degli incidenti di sicurezza informatica, consentendo un rapido ed efficace scambio di informazioni e risorse tra le diverse entità coinvolte andando a creare una rete solida e sinergica per affrontare le minacce cibernetiche in modo efficace.

CSIRT-AA fornisce le linee guida per la gestione completa delle minacce e degli incidenti informatici prevedendo altresì anche un supporto attivo ai membri della constituency i quali, a loro volta, hanno facoltà di declinare tali indicazioni sulla propria realtà di appartenenza, in maniera autonoma, al fine di renderle quanto più efficace possibile.

L'organizzazione ibrida di CSIRT-AA, con le sue caratteristiche di campus incorporato, combina gli elementi di un'**organizzazione centralizzata con un approccio distribuito**. In dettaglio, CSIRT-AA ha una struttura centralizzata presso Informatica Alto Adige, con risorse appositamente dedicate, che funge da centro di coordinamento e punto di riferimento per tutte le attività operative del CSIRT. Allo stesso tempo, grazie alla messa a disposizione di personale da parte di ogni ente (“Referente Tecnico” almeno uno per membro della

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

constituency), CSIRT-AA è, virtualmente, presente sul campo per meglio supportare ed indirizzare le varie amministrazioni sui servizi offerti.

Questo approccio ibrido garantisce una copertura territoriale adeguata e una capacità di risposta tempestiva agli incidenti di sicurezza informatica in tutto l'Alto Adige. Tale approccio consente inoltre di sfruttare sia l'esperienza e le risorse centralizzate di Informatica Alto Adige, sia la conoscenza locale e le competenze specifiche delle diverse entità appartenenti alla constituency.

In questo modo, CSIRT-AA è in grado di adattarsi alle esigenze specifiche del territorio dell'Alto Adige e fornire una risposta tempestiva ed efficace alle minacce informatiche, contribuendo così alla protezione e alla sicurezza dell'intera comunità.

6 Constituency

CSIRT-AA offre i suoi servizi ad una vasta constituency composta, inizialmente, da diverse entità pubbliche nell'ambito territoriale dell'Alto Adige. Nello specifico, include i referenti tecnici di:

- Informatica Alto Adige S.p.A.
- Regione Trentino-Alto Adige;
- Azienda Sanitaria dell'Alto Adige;
- Amministrazione Pubblica della Provincia Autonoma di Bolzano;
- Agenzia per la Protezione Civile della Provincia Autonoma di Bolzano;
- Consorzio dei Comuni della Provincia di Bolzano e i Comuni di Bolzano, Merano e Varna

Queste entità rappresentano una varietà di settori e organizzazioni che rivestono un ruolo cruciale nella promozione del benessere, della sicurezza e dello sviluppo dell'Alto Adige; sono infatti coinvolte nelle attività amministrative, nell'erogazione di servizi essenziali, nella gestione della sanità pubblica, nell'informatica e nelle operazioni di protezione civile.

CSIRT-AA prevede altresì la possibilità, per altre pubbliche amministrazioni ed enti privati, di richiedere di entrare a far parte della propria constituency. Queste entità saranno sottoposte ad una **procedura di accreditamento** che potrà essere richiesta con apposito modulo presente sul sito istituzionale di CSIRT-AA (<https://cert-aa.provincia.bz.it/>).

Questa iniziativa contribuirà a rafforzare la resilienza e la protezione dell'intera comunità, facilitando lo scambio di conoscenze, esperienze e buone pratiche tra le organizzazioni membri di CSIRT-AA e le nuove entità che si uniranno alla constituency.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

D’altro canto, CSIRT-AA si accrediterà presso CSIRT-Italia facendo da punto di riferimento tra le istituzioni nazionali e quello locali.

Saranno previsti, pertanto, due differenti forme di accreditamento:

1. *Accreditamento di CSIRT-AA nei confronti di CSIRT Italia:* CSIRT-AA richiederà l'accreditamento presso CSIRT Italia per diventare parte della sua constituency al fine di poter utilizzare i servizi da esso offerti; ciò faciliterà la cooperazione e lo scambio di informazioni con gli altri CERT/CSIRT regionali e nazionali, contribuendo a una risposta ancora più efficace e coordinata agli incidenti di sicurezza informatica a livello extra territoriale. Attraverso questa stretta collaborazione con CSIRT Italia, CSIRT-AA si impegnerà a contribuire alla creazione di un ecosistema di sicurezza informatica robusto e resiliente a livello locale e nazionale, lavorando in sinergia con altre entità accreditate per affrontare le minacce informatiche in modo coordinato e tempestivo;
2. *Accreditamento delle Pubbliche Amministrazioni Locali (PAL) e aziende private del territorio dell’Alto Adige nei confronti di CSIRT-AA:* le singole PAL potranno richiedere l'accreditamento presso CSIRT-AA per diventare parte della sua constituency. Sarà prevista altresì una forma di accreditamento per le aziende del territorio con specifico riferimento alla condivisione delle informazioni di intelligence sulle minacce cibernetiche. Le PAL che desidereranno accedere ai servizi offerti da CSIRT-AA dovranno richiede l'accreditamento attraverso il responsabile della sicurezza informatica della PAL stessa che contatterà CSIRT-AA attraverso i canali appropriati secondo la procedura messa a disposizione sul sito istituzionale.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

L'accreditamento potrà avvenire nelle seguenti forme:

Livello di accreditamento	Servizi	Accessibilità	Costo
BASE	• Situational Awareness	Pubbliche amministrazioni italiane e aziende private (territorio dell'Alto Adige)	Gratuito
INTERMEDIO	• Vulnerability Management • Knowledge Transfer	Pubbliche amministrazioni dell'Alto Adige	Commissione (*fee*) associata a singolo servizio e dipendente dalle dimensioni della PAL
AVANZATO	• Information Security Event Management • Information Security Incident Management	Pubbliche amministrazioni dell'Alto Adige	Commissione (*fee*) associata a singolo servizio e dipendente dalle dimensioni della PAL

TABELLA 1: LIVELLI DI ACCREDITAMENTO

L'accreditamento per uno specifico livello comporterà l'acquisizione dei servizi contenuti nei livelli precedenti. Il profilo completo di CSIRT-AA è contenuto nel documento RFC 2350 presente nel sito web istituzionale (link: <https://cert-aa.provincia.bz.it/upload/rfc2350.Txt>).

I costi iniziali per la formalizzazione, realizzazione ed erogazione di servizi all'interno di CSIRT-AA per il triennio 2025-2027 saranno a carico della Provincia Autonoma di Bolzano.

7 Ruoli e responsabilità

Come anticipato nei paragrafi precedenti, lo CSIRT territoriale dell'Alto Adige (CSIRT-AA) è istituito dalla Provincia Autonoma di Bolzano, si inserisce nel più ampio "Modello Cyber PAB" della Provincia Autonoma di Bolzano e trova la sua collocazione operativa presso Informatica Alto Adige.

Opera con un modello di autorità condivisa al fine di promuovere la partecipazione attiva e la condivisione delle responsabilità tra i membri della constituency. Sono istituiti i seguenti organi:

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

- **Core Team:** CSIRT-AA è coordinato operativamente da un gruppo noto come "Core Team", che guida le attività progettuali che ruotano intorno a CSIRT-AA, recependo le indicazioni del CdC-CY in coerenza con la linea strategica definita nel Modello Cyber PAB e verificando l'attuazione dei servizi presso Informatica Alto Adige. Il Core Team è composto dal CSIRT Manager e dai Referenti Tecnici delegati dai membri della constituency.

  È data facoltà ai membri del Core Team, che si riuniscono con cadenza almeno bimestrale, proporre l'ingresso di ulteriori membri solo ed esclusivamente in rappresentanza delle entità facenti parte della constituency.
- **CSIRT-AA Manager:** Il CSIRT-AA è guidato da un CSIRT Manager, responsabile delle attività operative, del coordinamento delle risposte agli incidenti e della gestione delle risorse del CSIRT-AA. Il CSIRT Manager agisce come punto di contatto principale per la constituency e coordina le azioni di tutto il gruppo tecnico
- **Team Tecnico:** Il CSIRT-AA dispone di un gruppo tecnico, istituito presso Informatica Alto Adige, composto da specialisti di sicurezza informatica con competenze trasversali.

  Questo gruppo svolge un ruolo cruciale nella gestione degli incidenti e nell'erogazione dei servizi di cui i dettagli al paragrafo successivo.

  I membri di tale gruppo, con il supporto operativo dei Referenti Tecnici dei membri della constituency, collaborano strettamente per rispondere agli incidenti di sicurezza, condividere informazioni e raccomandazioni, e sviluppare le migliori pratiche per la prevenzione delle minacce.

8 Catalogo dei servizi

Il catalogo dei servizi è stato sviluppato tenendo conto delle linee guida fornite da ACN, AgID ed ENISA nella costruzione di CSIRT e SOC, con l'intento di fornire, ai membri della constituency, validi strumenti per un approccio completo e mirato alla gestione delle minacce informatiche.

I servizi si articolano sulle cinque Aree di servizi ("*Service Area*") che definiscono le aree di operatività per un CSIRT (livello 1). All'interno di ognuna di queste aree ricadono una serie di servizi, i quali si compongono poi di azioni operative (funzioni).

Di seguito se ne dettagliano i contenuti, differenziandoli per livello di accreditamento.

8.1 Accreditamento BASE

L'accesso a tali servizi, dopo una fase iniziale di accreditamento, è a titolo gratuito.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

8.1.1 Situational Awareness

Nella presente area sono inclusi tutti quei servizi che hanno lo scopo di identificare, elaborare, comprendere e comunicare gli elementi critici che possono impattare la Constituency.

Il principale obiettivo perseguito da questa area è l'acquisizione di dati circa attività rilevanti che potrebbero impattare il quadro situazionale della Constituency.

8.1.1.1 Data acquisition

Il servizio di acquisizione dei dati è strutturato in modo da aumentare la conoscenza e visibilità di CSIRT-AA relativamente alle entità accreditate. Sulla base delle informazioni e dei dati acquisiti, CSIRT-AA modula dinamicamente e adatta l'offerta in termini di servizi e attività volti al miglioramento della postura di sicurezza delle entità accreditate in modo da massimizzarne la copertura e l'efficacia.

In particolare, il servizio avrà l'obiettivo di acquisire e mappare le informazioni delle varie organizzazioni accreditate in termini di:

- asset in perimetro, completi di caratteristiche tecniche e baseline attese;
- informazioni, ruoli e responsabilità relativamente agli stakeholders coinvolti nelle operazioni di monitoraggio e risposta agli incidenti di sicurezza.

Il servizio mirerà inoltre ad acquisire, da fonti interne ed esterne, informazioni e dati che possono essere utilizzati a supporto degli altri servizi descritti all'interno del presente documento.

8.2 Accreditamento INTERMEDIO

L'accesso a tali servizi avviene mediante una fase iniziale di accreditamento. Gli eventuali costi sono determinati in base all'estensione della pubblica amministrazione dell'Alto Adige, unica entità abilitata a richiederne l'accesso, fermo restando la già presente copertura finanziaria per il triennio 2025-2027 ad opera di PAB.

8.2.1 Vulnerability Management

Il servizio di Vulnerability Management mira a supportare tutte le entità accreditate presso CSIRT-AA relativamente alle tematiche di gestione e risposta alle vulnerabilità. In particolare, l'obiettivo delle attività sarà quello di:

- **Vulnerability coordination**: scambiare informazioni e coordinare le attività con tutte le entità, sia interne che esterne, coinvolte nel processo di divulgazione responsabile delle vulnerabilità;

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

- **Vulnerability disclosure**: condivisione delle informazioni relative alle vulnerabilità note verso la Constituency al fine di abilitare la prevenzione, l'identificazione e la risoluzione/mitigazione delle vulnerabilità stesse;
- **Vulnerability response**: utilizzare attivamente le informazioni sulle vulnerabilità note con lo scopo di adoperarle per prevenire, rilevare e mitigare le stesse.

Di seguito si riporta una trattazione più dettagliata relativamente alle attività fornite.

8.2.1.1 Vulnerability coordination

Il coordinamento delle attività consiste nel fornire guida e informazioni rilevanti per la risoluzione delle vulnerabilità e la loro divulgazione responsabile all'interno della constituency al fine di incoraggiare la consapevolezza e migliorare la postura di sicurezza.

In particolare, è cura di CSIRT-AA informare e notificare i membri della constituency relativamente a nuove vulnerabilità emerse. CSIRT-AA è inoltre investito della responsabilità di coordinare lo scambio di informazioni tra tuti gli stakeholders coinvolti, come terze parti o altre comunità, al fine di consentire una corretta collaborazione volta alla risoluzione della vulnerabilità.

CSIRT-AA si incarica inoltre dell'interfacciamento con i vari stakeholders e del loro coordinamento, al fine da garantire la condivisione delle informazioni verso le parti interessate in maniere responsabile e precisa.

8.2.1.2 Vulnerability disclosure

Le attività di condivisione delle informazioni verso la constituency di CSIRT-AA hanno come obiettivo quello di migliorare le capacità di prevenzione, identificazione e risoluzione delle vulnerabilità.

CSIRT-AA si adopera per fornire e condividere politiche e procedure a supporto delle attività di condivisione e divulgazione delle vulnerabilità, in modo da definire chiaramente le modalità impiegate per effettuare una condivisione precisa e responsabile delle informazioni.

In secondo luogo, il CSIRT-AA si occupa di sviluppare campagne informative, tramite annunci e comunicazioni mirate, che consentono di informare la constituency o rendere pubbliche informazioni relative a nuove vulnerabilità non ancora identificate. Tale azione è svolta al fine di permettere di adeguare la postura di sicurezza delle entità facenti parte della constituency al fine di mitigare o prevenire lo sfruttamento della vulnerabilità, o di rilevarlo nel caso fosse già in corso. Sono quindi forniti notifiche e avvisi tempestivi alle

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

organizzazioni quando verranno identificate nuove vulnerabilità che potrebbero interessare i loro sistemi o applicazioni.

Il CSIRT-AA è inoltre a disposizione per fornire riscontri tecnici e comportamentali a qualsiasi entità accreditata che richieda consulto relativamente a vulnerabilità note o non note.

8.2.1.3 Vulnerability response

Questo servizio ha lo scopo di determinare se una vulnerabilità divulgata esiste sui sistemi di un membro della constituency, spesso attraverso la ricerca attiva di presenza di tali vulnerabilità. Il servizio può anche includere le azioni successive per rimediare o mitigare la vulnerabilità attraverso la distribuzione di patch o strategie di workaround.

Il servizio comprende le attività di detection e/o scansione di vulnerabilità note nei sistemi impiegati e le attività di rimedio e/o mitigazione di vulnerabilità per prevenire che siano sfruttate, tipicamente tramite l'applicazione tempestiva di patch pubblicate da fornitori o altre soluzioni.

8.2.2 Knowledge Transfer

Il CSIRT-AA è operativo nelle azioni di condivisione della conoscenza, le quali risultano di estrema importanza in quanto consentono di fornire ai propri utenti conoscenze e competenze acquisite. Una volta trasferite, queste avranno un effetto migliorativo sulle capacità di tutta l'organizzazione di identificare, mitigare e prevenire le minacce alla sicurezza informatica. Si riportano di seguito le varie azioni.

8.2.2.1 Awareness Building

Il CSIRT-AA supporta il miglioramento generale della postura di sicurezza della Constituency, costruendo competenze che consentano loro di gestire in modo adeguato la sicurezza informatica all'interno dell'organizzazione.

Per fare ciò, CSIRT-AA svolge un processo continuo di ricerca e correlazione di informazioni, sempre legate all'attualità, in grado di fornire valore aggiunto e consapevolezza agli utenti.

Tale informazione saranno poi racchiuse all'interno di materiale informativo ad-hoc fruibile in diversi formati (presentazioni, video, opuscoli, newsletter, bulletin, etc.) e condivisibile tramite diverse piattaforme.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

CSIRT-AA provvede inoltre a diffondere informazioni relative alla sicurezza informatica al fine di accrescere la consapevolezza degli utenti della Constituency e a supportare la stessa nell'implementazione delle best practice di sicurezza.

Un fattore chiave che il CSIRT-AA tiene in considerazione è il continuo sviluppo e mantenimento di relazioni con esperti di settore e altre organizzazioni, inclusi altri CSIRT, in modo da creare una rete in grado di supportarsi nel raggiungimento degli obiettivi prefissati nel mandato.

8.2.2.2 Training and education

Il CSIRT-AA eroga servizi di formazione al personale della Constituency, riguardante argomenti relativi alla sicurezza informatica, la sicurezza delle informazioni e la gestione degli incidenti, volte al miglioramento delle conoscenze e delle capacità del personale impiegato.

Inizialmente, CSIRT-AA analizza, identifica e documenta le necessità – in termini di conoscenze, competenze e abilità – della Constituency, al fine di poter sviluppare materiale di training appropriato ed in linea con i loro bisogni. In base alle informazioni raccolte, sviluppa il materiale educativo, didattico e di formazione e lo condivide mediante i canali di formazioni più appropriati all'audience ed al contenuto. Tale supporto e condivisione verrà fornito secondo canali e processi predefiniti.

Il CSIRT-AA svilupperà inoltre un processo di tutoraggio delle risorse, mettendo a disposizione personale specializzato e con svariati anni di esperienza al fine di condividere nozioni e prospettive con gli utenti della constituency. Unitamente a tale attività, il CSIRT-AA svilupperà anche un piano evolutivo di carriera per il personale a supporto.

8.2.2.3 Exercises

A seguito delle attività teoriche, CSIRT-AA effettua esercitazioni pratiche indirizzate sia ai membri del CSIRT-AA che alle entità accreditate e il loro personale. Analogamente a quanto descritto in precedenza, e quindi coerentemente con la metodologia già descritta per le sessioni teoriche, il CSIRT-AA svilupperà il materiale a partire dagli obiettivi formativi individuati in base al contesto organizzativo e di sicurezza.

Le attività sono condotte da personale specializzato e rappresentano scenari e situazioni pensati specificamente per il potenziamento delle capacità di risposta agli incidenti del personale, in termini di efficienza ed efficacia.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Al termine delle attività, è cura di CSIRT-AA condividere con i partecipanti un riscontro scritto, sotto forma di relazione, relativo alle attività svolte e alle osservazioni emerse: saranno particolarmente evidenziate possibili aree di miglioramento e le azioni necessarie da implementare per raggiungere gli obiettivi prefissati.

8.2.2.4 Technical and policy advisor

CSIRT-AA supporta la Constituency, o eventuali persone chiave coinvolte, nella costituzione di specifiche politiche e procedure al fine di abilitare appropriate modalità di gestione degli incidenti, gestire adeguatamente minacce e rischi, incrementando così anche l'efficacia delle attività eseguite da CSIRT-AA.

In particolare, verrà posta particolare attenzione alle tematiche di compliance e gestione del rischio, così come quelle di continuità operativa (*business continuity*) e disaster recovery.
Unitamente a queste attività, il CSIRT-AA fornirà costante supporto tecnico specialistico per assicurarsi il miglioramento continuo delle infrastrutture, in termini di asset e strumenti di sicurezza, con l'obiettivo di eseguire un miglioramento generale della postura di sicurezza, delle modalità operative e delle best practice adottate.

8.3 Accreditamento AVANZATO

L'accesso a tali servizi potrà avvenire mediante una fase iniziale di accreditamento. Gli eventuali costi saranno determinati in base all'estensione della pubblica amministrazione dell'Alto Adige, unica entità abilitata a richiederne l'accesso, fermo restando la già presente copertura finanziaria per il triennio 2025-2027 ad opera di PAB.

8.3.1 Information Security Event Management

Il servizio di Information Security Event Management si concentrerà sulla preparazione, sulla manutenzione e sullo sviluppo dei servizi di raccolta, monitoraggio e analisi delle informazioni condivise dalle entità accreditate al CSIRT-AA. Tali azioni avranno come obiettivi quelli di:

- gestire in maniera ottimale tutte le informazioni provenienti dalle entità accreditate (informazioni, sorgenti, use-case);

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

- fornire spunti di miglioramento e aggiornamento relativamente alle informazioni e alle pratiche condivise;
- svolgere azioni di monitoraggio per l'identificazione e l'analisi di anomalie o eventi sospetti.
- effettuare azioni di correlazione tra gli eventi e le informazioni ottenute in modo da aumentare la visibilità e consentire un'identificazione più precisa e celere di incidenti o eventi di sicurezza.

8.3.1.1 Monitoring and Detection

Il servizio proposto da Alfa mira all'abilitazione di un processo automatizzato e continuo di elaborazione degli eventi di sicurezza, con l'obiettivo di rilevare anomalie che possono essere qualificate come incidenti di sicurezza. Questo servizio include la gestione delle sorgenti di dati, l'implementazione e la configurazione degli use case di monitoraggio, e l'integrazione di dati contestuali per migliorare la correlazione e l'analisi degli eventi.

In particolare, CSIRT-AA si occupa di:

- **Gestione dei log e dei sensori**: garantire un flusso costante di eventi di sicurezza attraverso una gestione efficace delle varie sorgenti di log e sensori. Questo permetterà di alimentare gli strumenti di monitoraggio e analisi con i dati necessari per il rilevamento degli incidenti.
- **Gestione degli *use case* di rilevamento**: definizione, verifica, aggiornamento e miglioramento continuo degli use case di monitoraggio, per supportare gli analisti nell'identificazione tempestiva degli eventi di sicurezza. Questo processo include la configurazione e l'ottimizzazione degli *use case* all'interno dell'infrastruttura di monitoraggio.
- **Gestione dei dati contestuali**: raccolta e utilizzo di dati provenienti da fonti come i database di gestione delle configurazioni (CMDB), i sistemi di threat intelligence e quelli di gestione delle identità e degli accessi (IAM). Questi dati sono essenziali per il monitoraggio e la correlazione degli eventi di sicurezza, migliorando la capacità di identificare e qualificare gli incidenti.

Il servizio è progettato per garantire un monitoraggio continuo e una gestione efficiente degli eventi di sicurezza, con l'obiettivo di mantenere un elevato livello di protezione contro le minacce informatiche.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

8.3.1.2 Event Analysis

Il CSIRT-AA svolge approfondite azioni di analisi sui dati ricevuti, nel caso essi dovessero essere valutati positivamente nelle fasi di controllo e verifica dei vari use-case. Tali analisi hanno l'obiettivo di rimuovere eventuali falsi positivi e fornire valutazioni più approfondite in caso contrario.

La correlazione degli eventi gioca un ruolo cruciale nell'analisi delle informazioni ricevute in quanto consente aumentare la visibilità e il campo di azione combinando dati da diverse sorgenti e relativi a diversi apparati. Grazie a queste operazioni è possibile migliorare la velocità di identificazione, la precisione dell'analisi e l'efficacia delle azioni di risposta.

Il CSIRT-AA svolge infine azioni di categorizzazione e qualificazione degli eventi di sicurezza individuati, in modo da categorizzarli correttamente come incidenti di sicurezza. A supporto di questa valutazione sono identificati l'impatto e l'urgenza generati dall'evento, grazie ai quali è possibile identificare il rischio associato.

8.3.2 Information Security Incident Management

CSIRT-AA eroga un servizio di Information Security Incident Management che è supportato dall'utilizzo di un sistema di trouble ticket personalizzato, da un lato, per recepire le indicazioni su tattiche, tecniche e procedure secondo framework Mitre Attack e, dall'altro, per implementare la tassonomia degli incidenti legata al Perimetro di Sicurezza Nazionale e a quella più generica di ENISA.

Si utilizza, come standard di riferimento, la ISO/IEC 27035, attraverso la quale si forniranno, ai membri della constituency, linee guida puntuali per la gestione degli incidenti di sicurezza e supporto operativo in caso di necessità.

Obiettivo principale sarà quello di aiutare le organizzazioni a sviluppare un approccio strutturato ed efficace per la gestione degli incidenti di sicurezza, al fine di ridurre al minimo gli impatti negativi e ripristinare rapidamente la normalità delle operazioni. Alcune delle principali attività offerte all'interno del servizio vengono di seguito riportate.

8.3.2.1 Information security incident report acceptance

Verrà sottolineata l'importanza di disporre di un sistema per la rilevazione tempestiva degli incidenti di sicurezza delle informazioni. Ciò implicherà la messa in atto di meccanismi di monitoraggio, rilevazione e segnalazione degli eventi di sicurezza che potrebbero indicare la presenza di un incidente (servizio attualmente fornito dal SOC di Informatica Alto Adige). Le operazioni di registrazione accurata e dettagliata degli incidenti per scopi di analisi, tracciabilità e apprendimento saranno fornite direttamente da CSIRT-AA.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Più dettagliatamente, CSIRT-AA predisporrà meccanismi e processi definiti e puntuali per la ricezione e raccolta delle segnalazioni di incidente provenienti dalle entità della constituency. Tali dati saranno prontamente analizzati in modo da individuare la causa principale (root cause) dell'incidente e in modo da fornire una panoramica sui possibili impatti alla confidenzialità, integrità e disponibilità dei dati trattati.

8.3.2.2 Information security incident analysis

La fase di analisi dell'incidente ha come obiettivo quello di identificare e fornire alle entità accreditate tutte le possibili informazioni di dettaglio circa le cause, gli impatti, le dinamiche e gli aspetti tecnici legati all'incidente di sicurezza.

CSIRT-AA svolge quindi una analisi iniziale dell'incidente (*triage*), procedendo con la sua classificazione in base a gravità e impatto, e concludendo con l'assegnazione della priorità. Viene inoltre fornito supporto costante al fine di garantire la raccolta e l'identificazione di tutte le informazioni rilevanti ai fini dell'analisi e risposta all'incidente di sicurezza. Una raccolta strutturata sarà di fondamentale importanza al fine di garantire una raccolta completa e precisa, che garantisca la possibilità di riutilizzare i dati anche nelle fasi successive a questa.

CSIRT-AA coordina o svolge direttamente le azioni di analisi tecnica, ove ritenute necessarie al fine di approfondire certi aspetti o tematiche. Allo stesso modo, viene fornito supporto durante l'analisi della causa principale (root cause), elemento molto importante ai fini del riconoscimento delle debolezze strutturali che hanno reso possibile l'attacco e, conseguentemente, del contenimento dello stesso.

Infine, CSIRT-AA, grazie alla sua estesa visibilità su tutti i membri della constituency, effettuerà attività di correlazione e confronto tra le varie informazioni ricevute in merito ad incidenti di sicurezza pregressi, ampliando la possibilità di trovare azioni di rimedio o mitigazione applicabili allo scenario corrente.

8.3.2.3 Artifact and forensic evidence analysis

CSIRT-AA fornisce supporto relativamente alle operazioni tecniche di analisi degli artefatti acquisiti e delle varie evidenze forensi, garantendo una metodologia appropriata per il mantenimento della catena di custodia al fine di mantenere le proprietà di integrità, non ripudio e ammissibilità delle prove.

Tali analisi coprono i seguenti ambiti:

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

- estrazione delle informazioni da supporti mediatici ed informatici ed analisi delle evidenze. Comparazione con fonti ammissibili e dati di pubblico dominio che permettano di determinare la superficie esposta;
- attività di reverse engineering tramite l'esecuzione di analisi statiche su artefatti con l'obiettivo di determinare, in modo esaustivo, le sue funzionalità (esempio, metodi di attivazione, impatti, metodi di propagazione, mitigazione, ecc.) indipendentemente dall'ambiente in cui può essere eseguito;
- esecuzione di attività di analisi dinamica di un artefatto al fine di valutare il loro comportamento all'interno di ambienti segregati e opportunamente controllati;
- attività di analisi comparativa con altri artefatti identificati in casistiche analoghe in modo da identificare possibili allineamenti.

8.3.2.4 Information security incident coordination

CSIRT-AA è inoltre impegnato nelle operazioni di coordinamento della risposta agli incidenti di sicurezza che dovessero occorrere all'interno della sua constituency.

Tali azioni mirano principalmente al supporto al ripristino delle attività operative, per le quali sono fornite istruzioni circa l'implementazione di misure correttive, la verifica dell'efficacia di tali misure, il ripristino dei sistemi e delle applicazioni interessate e la valutazione dell'impatto dell'incidente sulle operazioni aziendali.

CSIRT-AA definisce e mantiene canali di comunicazione sicuri, adeguati e puntuali al fine di garantire una comunicazione riservata e diretta con i membri della sua constituency. Tali canali sono sfruttati per scambiare informazioni con entità impattate da un incidente durante le fasi di risposta. A tale scopo, sarà importante definire tutti gli stakeholders coinvolti, comprese le terze parti, in modo che possano essere destinatari di tutte le informazioni aggiornate e necessarie al coordinamento e svolgimento delle attività.

CSIRT-AA raccoglie e cataloga le informazioni relative allo stato attuale di completamento delle attività, al fine di fornire materiale e adeguato supporto per una analisi post-incidente che comprenda la revisione dei processi, l'identificazione delle lezioni apprese, l'aggiornamento delle procedure e l'implementazione di misure preventive per ridurre il rischio di futuri incidenti.

Infine, sarà cura del CSIRT-AA supportare le entità nella preparazione e condivisione di informazioni mirate e accurate per i media, in modo da veicolare un'informazione precisa, veritiera e controllata.

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Sichtvermerke i. S. d. Art. 13 L.G. 17/93 und L.G. 6/22 über die fachliche, verwaltungsmäßige und buchhalterische Verantwortung

Visti ai sensi dell'art. 13 L.P. 17/93 e della L.P. 6/22 sulla responsabilità tecnica, amministrativa e contabile

Der Abteilungsdirektor / Il Direttore di ripartizione	HOFER JOSEF THOMAS	26/03/2025 11:39:58
Der Generaldirektor / Il Direttore generale	STEINER ALEXANDER	26/03/2025 11:42:03
Der Abteilungsdirektor / Il Direttore di ripartizione	HOFER JOSEF THOMAS	26/03/2025 11:38:14

Laufendes Haushaltsjahr — Esercizio corrente

La presente delibera non dà luogo a impegno di spesa.
Dieser Beschluss beinhaltet keine Zweckbindung

zweckgebunden		impegnato
als Einnahmen ermittelt		accertato in entrata
auf Kapitel		sul capitolo
Vorgang		operazione

Der Direktor des Amtes für Ausgaben	07/04/2025 18:15:14 TACCHINARDI MARTA	Il Direttore dell'Ufficio spese
Der Direktor des Amtes für Finanzaufsicht		Il Direttore dell'Ufficio Vigilanza finanziaria
Der Direktor des Amtes für Einnahmen		Il Direttore dell'Ufficio entrate

Diese Abschrift entspricht dem Original

Per copia conforme all'originale

Datum / Unterschrift

data / firma

Abschrift ausgestellt für

Copia rilasciata a

Beschluss Nr./N. Delibera: 0151/2025. Digital unterzeichnet / Firmato digitalmente: Arno Kompatscher, 00DB5FC8 - Eros Magnago, 00C4589D

Der Landeshauptmann Il Presidente	KOMPATSCHER ARNO	08/04/2025
Der Generalsekretär Il Segretario Generale	MAGNAGO EROS	08/04/2025

Es wird bestätigt, dass diese analoge Ausfertigung, bestehend - ohne diese Seite - aus 96 Seiten, mit dem digitalen Original identisch ist, das die Landesverwaltung nach den geltenden Bestimmungen erstellt, aufbewahrt, und mit digitalen Unterschriften versehen hat, deren Zertifikate auf folgende Personen lauten:

nome e cognome: Arno Kompatscher
codice fiscale: TINIT-KMPRNA71C19D571S
certification authority: InfoCert Qualified Electronic Signature CA 3
numeri di serie: 00DB5FC8
data scadenza certificato: 04/01/2026

Am 08/04/2025 erstellte Ausfertigung

Si attesta che la presente copia analogica è conforme in tutte le sue parti al documento informatico originale da cui è tratta, costituito da 96 pagine, esclusa la presente. Il documento originale, predisposto e conservato a norma di legge presso l'Amministrazione provinciale, è stato sottoscritto con firme digitali, i cui certificati sono intestati a:

nome e cognome: Eros Magnago
codice fiscale: TINIT-MGNRSE66H24H612Y
certification authority: InfoCert Qualified Electronic Signature CA 3
numeri di serie: 00C4589D
data scadenza certificato: 03/10/2025

Copia prodotta in data 08/04/2025

Die Landesverwaltung hat bei der Entgegennahme des digitalen Dokuments die Gültigkeit der Zertifikate überprüft und sie im Sinne der geltenden Bestimmungen aufbewahrt.

L'Amministrazione provinciale ha verificato in sede di acquisizione del documento digitale la validità dei certificati qualificati di sottoscrizione e li ha conservati a norma di legge.

Ausstellungsdatum / Data di emanazione

11/03/2025

Diese Ausfertigung entspricht dem Original

Per copia conforme all'originale

Datum/Unterschrift

Data/firma