Allegato P591
Requisiti minimi per l’implementazione organizzativa e tecnica

Allegato alla prescrizione sulle disposizioni in materia di protezione contro i ciber-rischi e sicurezza dei dati per i sistemi collegati alla piattaforma NOVA e i relativi utenti (utenti NOVA)

Edizione 28.04.2025

Modifiche valevoli dal 1.07.2025 (v1.4)

Capitolo/cifra	**Modifiche**
12, 13, 31, 32	Precisazioni in caso di crittografia durante la trasmissione o l'archiviazione.
Glossario, 6, 10, 12, 13, 16, 17, 19, 23, 27, 31, 32	Precisazioni della formulazione
11	Termine di conservazione ridotto da 2 anni a 6 mesi
19	Precisazione del termine "contratto" a "almeno l'allegato 12 della Ue500"
14	X aggiunto per Lm
In tutto il documento	Aggiunte e precisazioni per migliorare la comprensione

Alliance SwissPass Länggassstrasse 7 3012 Berna Tel +41 31 359 22 40
info@allianceswisspass.ch allianceswisspass.ch

Contenuto

Osservazioni preliminari

Aspetti generali e finalità

Il presente allegato alla P591 Protezione contro i ciber-rischi e sicurezza dei dati descrive i requisiti organizzativi e tecnici minimi per il collegamento all'ambiente di sistema NOVA. Tutte le convenzioni che se ne discostano devono essere documentate in modo verificabile e trasparente. Lo scostamento deve essere accertato in maniera dimostrabile almeno una volta all'anno e bisogna passare il prima possibile ai collegamenti standard. Oltre alle P591, in relazione alla protezione contro i ciber-rischi e alla sicurezza dei dati si applicano anche le seguenti prescrizioni e disposizioni esistenti:

- Condizioni di utilizzo NOVA (C500 allegato 12)
- Regolamento sull'utilizzo dei dati tp (C500 allegato 16)

Le imprese di trasporto (IT) che non appartengono al SDN, così come i terzi, devono inoltre concludere un contratto standard. Questo contratto stabilisce che i requisiti della P591 sono vincolanti anche per loro, a meno che non siano già soggetti alla C500.

- Contratto standard NOVA per terzi e IT non appartenenti al SDN

Premessa (sicurezza delle informazioni)

I seguenti requisiti in materia di sicurezza delle informazioni sono strutturati secondo un principio «per livelli» e devono essere adattati di conseguenza ai gruppi di utenti per i servizi NOVA.
Se il gestore NOVA classifica l'utente NOVA in diverse categorie, quest'ultimo deve soddisfare il livello con i requisiti più ampi.
Gli utenti con accesso di lettura ai dati personali hanno il diritto di utilizzare i dati dell'ambiente NOVA per le finalità definite nella convenzione d'utilizzo NOVA.

Le seguenti categorie vengono differenziate nei seguenti requisiti e si traducono in un'attuazione completa o ridotta delle misure:

Lettura senza accesso univoco ai dati personali (Lo):
Gli utenti NOVA con diritto di lettura senza accesso ai dati personali trattano in linea di principio solo informazioni pseudonimizzate da NOVA, che consentono di risalire alle persone solo attraverso i reparti autorizzati del gestore NOVA.

Lettura con accesso univoco ai dati personali (Lm):
Le imprese che trattano informazioni con accesso ai dati personali devono sottostare tassativamente a una convenzione d'utilizzo e rispettare le disposizioni sulla protezione dei dati.

Lettura/scrittura (L/S):
Gli utenti NOVA con diritto di lettura/scrittura possono anche modificare i dati all'interno dell'ambiente NOVA.

Glossario

Alliance SwissPass	Organizzazione di settore dei trasporti pubblici formata da 250 imprese di trasporto e 20 comunità, che si impegna a livello nazionale a favore di condizioni tariffarie armonizzate, chiare ed economiche, soluzioni di vendita moderne e allettanti nonché assortimenti e sistemi informativi orientati ai clienti.
API (Application Programming Interface)	Interfaccia di programmazione che consente ai programmi software di comunicare tra loro e di scambiarsi dati.
Attacco DDoS	In un attacco DDoS (Distributed Denial of Service), un aggressore sovraccarica un sito web, un server o una risorsa di rete con un traffico estremamente elevato, con l'obiettivo di farla andare in crash o di limitarne la disponibilità.
CA (Certificate Authority) - Autorità di certificazione	Un'autorità di certificazione, detta anche istanza di certificazione, è un'entità organizzativa nella sicurezza informatica che rilascia certificati digitali all'interno di un'infrastruttura a chiave pubblica (PKI). Esistono autorità di certificazione pubbliche e interne alle aziende.
C500	La Convenzione 500 (C500), il contratto di collaborazione del settore, disciplina le competenze all'interno dell'Alliance SwissPass. Viene aggiornata costantemente.
CISO	Abbreviazione di Chief Information Security Officer, responsabile della sicurezza informatica.
CU NOVA	Condizioni di utilizzo della piattaforma NOVA, allegato 12 della C500
Diritti privilegiati	Gli account con diritti privilegiati sono tipicamente account di amministratori IT o altri account utente con privilegi che comportano un impatto significativo sull'attività aziendale. Hanno spesso accesso a funzioni critiche del sistema e possono apportare modifiche rilevanti allo stato operativo, alle configurazioni e ai dati dei sistemi. Sono soggetti a requisiti di sicurezza specifici, che devono essere rispettati senza eccezioni.
FIRST	FIRST sta per «Forum for Incident Response and Security Teams» (www.first.org) e funge da amministratore delle specifiche CVSS.
Fornitore di servizi	Il fornitore di servizi è la persona o l'impresa che eroga la prestazione. Può essere una persona fisica, vale a dire una persona con capacità giuridica o una persona giuridica (impresa, organizzazione ecc.).
Framework	Framework è un altro termine per indicare il quadro riferimento o la struttura di base.
Gestore NOVA	Mandatario incaricato dall'Alliance SwissPass per la gestione dei sistemi e delle infrastrutture NOVA.
Intermediario	Organizzazione che vende assortimenti NOVA in rappresentanza di una o più imprese di trasporto incaricata/e della fornitura di servizi. In questa categoria rientrano le imprese di trasporto titolari di una concessione dell'UFT, i gestori di un'infrastruttura ferroviaria, le comunità tariffarie e dei trasporti svizzere e i terzi collegati a NOVA.
Livello CIS 1	CIS sta per Center for Internet Security, un'organizzazione di utilità pubblica che ha per scopo la promozione della cibersicurezza. Il livello 1 rappresenta una configurazione di sicurezza di base che viene considerata come standard minimo di sicurezza. I controlli al livello 1 hanno la funzione di schermare i maggiori vettori di minaccia e proteggere il sistema dagli attacchi più comuni. Le direttive al livello 1 sono meno restrittive e offrono un approccio equilibrato tra sicurezza e funzionalità del sistema. Il livello 1 è adatto alla maggior parte degli ambienti ed è consigliato per garantire un livello di sicurezza di base.

Livello CVSS 7	«Common Vulnerability Scoring System» è uno standard industriale sviluppato da FIRST per valutare il grado di gravità delle vulnerabilità potenziali o effettive nei sistemi informatici. Le misure o i livelli menzionati qui fanno riferimento alle specifiche della versione 3 (CVSS v3).
Malware	Termine collettivo per indicare qualsiasi tipo di software dannoso sviluppato per infiltrarsi nei dispositivi senza essere individuato, causare danni e interruzioni o rubare dati. Adware, spyware, virus, botnet, cavalli di Troia, worm, rootkit e ransomware rientrano tutti in questo termine collettivo.
Metodi di crittografia	I metodi di crittografia si distinguono in crittografia di archiviazione e di trasporto. Esistono anche diverse funzioni basate su crittografia, firma o checksum per poter verificare l'integrità delle informazioni tecniche. - AES 256 bit: Advanced Encryption Standard (AES) è un algoritmo di crittografia simmetrico che utilizza una chiave a 256 bit per convertire il testo in chiaro o i dati in un testo cifrato. - RSA: è un metodo di crittografia asimmetrico che può essere utilizzato sia per la crittografia che per la firma digitale. - Funzione hash crittografica: viene impiegata per verificare l'integrità di file o messaggi e con un valore crittografico aggiunto (hash) svela se ha avuto luogo un cambiamento. Viene utilizzata anche nelle firme digitali e per le verifiche delle password. - SHA2 / SHA3: sta per Secure Hash Algorithm, esiste in diverse versioni e mette a disposizione funzioni hash per determinare valori di test univoci di dati digitali. - Scambio di chiave Diffie-Hellman: è un protocollo per il contratto di chiave. Consente a due interlocutori di concordare, attraverso una linea pubblica e intercettabile, una chiave segreta condivisa sotto forma di numero, che solo loro conoscono e che un potenziale eavesdropper non può calcolare. - Suite di cifratura TLS: il protocollo Transport Layer Security (TLS) e il suo predecessore obsoleto Secure Socket Layer (SSL). Le suite di cifratura sono una serie di algoritmi utilizzati per proteggere le connessioni di rete tra client e server. I protocolli TLS/SSL vengono utilizzati per esempio per creare HTTPS, FTPS, POP3, SMTPS e altri. - L'RC4 (Rivest Cipher 4) è una cosiddetta crittografia di flusso che crittografa i messaggi byte per byte utilizzando un algoritmo. - Il Data Encryption Standard (DES; italiano «Standard di crittografia dei dati») è un algoritmo di crittografia simmetrico ampiamente diffuso. - L'IDEA (International Data Encryption Algorithm) è una crittografia a blocchi simmetrica. -L'ECB (Electronic Code Book Mode) è una modalità operativa per crittografie a blocchi. - HMAC: è un codice di autenticazione dei messaggi ottenuto con l'esecuzione di una funzione hash crittografica (come MD5, SHA1 e SHA256) tramite i dati da autenticare e una chiave segreta condivisa.
NIST	Il framework di cybersicurezza del National Institute of Standards and Technology (NIST) degli Stati Uniti (www.nist.gov) fornisce linee guida complete e buone pratiche che aiutano le aziende a migliorare la gestione dei rischi legati alla sicurezza delle informazioni e alla cybersicurezza.
Oggetto da proteggere	Sono considerati oggetti da proteggere tutte le applicazioni, i sistemi, le reti, le raccolte di dati, le infrastrutture e i prodotti che trattano dati NOVA.
Piattaforma NOVA	Piattaforma nazionale per la vendita di titoli di trasporto. Dal termine tedesco « Netzweite ÖV-Anbindung »
PKI	L'infrastruttura a chiave pubblica (Public Key Infrastructure – PKI) è un sistema gerarchico per l'emissione, la distribuzione e la verifica dei certificati

	digitali. Questi certificati digitali consentono un'associazione affidabile tra entità e le loro chiavi pubbliche.
Principio «per livelli»	Gli utenti NOVA che vengono classificati dal gestore NOVA in più/diverse categorie devono soddisfare il livello «categoria» con i requisiti più ampi.
Protezione contro i ciber-rischi	Misure per proteggere computer, server, dispositivi mobili, sistemi elettronici, reti e dati da attacchi intenzionali dal ciberspazio.
Segretariato dell'Alliance SwissPass	Il segretariato gestisce le attività dell'Alliance SwissPass secondo le disposizioni della Convenzione 500.
Sistema di rilevamento delle intrusioni	Il sistema di rilevamento delle intrusioni o sistema di rilevamento degli attacchi serve a riconoscere gli attacchi contro un sistema informatico o una rete di computer.
Standard minimo per le TIC	Standard minimo per migliorare la resilienza delle TIC
Standard OWASP TOP 10	Open Web Application Security Project è un'organizzazione internazionale no-profit dedicata alla sicurezza delle applicazioni web. L'OWASP TOP 10 è un rapporto aggiornato regolarmente che descrive i problemi di sicurezza delle applicazioni web, concentrandosi sui 10 rischi più critici.
Stateful Firewalling, Stateful Packet Inspection	Per Stateful Packet Inspection s'intende una tecnica dinamica di filtraggio dei pacchetti in cui ogni pacchetto di dati viene attribuito a una determinata sessione attiva. I pacchetti di dati vengono analizzati e lo stato della connessione viene incluso nella decisione.
TCP/IP	Il Transmission Control Protocol/Internet Protocol (TCP/IP) è un gruppo di protocolli di rete. Si tratta sostanzialmente dell'Internet Protocol (IP), del Transmission Control Protocol (TCP), dello User Datagram Protocol (UDP) e dell'Internet Control Message Protocol (ICMP). In senso più ampio, anche l'intera famiglia di protocolli Internet viene designata come TCP/IP.
Terzi	Organizzazioni che si collegano alla piattaforma NOVA e utilizzano l'assortimento NOVA, ma che non sono né imprese di trasporto concessionate dall'UFT, né gestori di infrastrutture ferroviarie, né comunità tariffarie e/o di trasporto svizzere.
Titolare della tariffa	L'istanza che esercita il controllo sulla tariffa (Servizio diretto nazionale [SDN], comunità, imprese di trasporto).
tp	Trasporti pubblici
UFT	Ufficio federale dei trasporti
Utenti NOVA	Intermediari, vettori, titolari della tariffa e fornitori di servizi.
Vendita	Per vendita s'intende l'intero processo di vendita di titoli di trasporto dei trasporti pubblici che inizia con l'informazione/consulenza alla clientela e continua con la vera e propria procedura di vendita, incluso il pagamento. Seguono il controllo dei titoli di trasporto e il servizio dopo vendita (cambio, annullamento, rimborso, reclami della clientela).
Verifica dell'integrità	Garanzia e tracciabilità dell'integrità e della completezza delle informazioni tramite il "logging" e il salvataggio immutabile dei dati.
Vettori	Agli offerenti che realizzano trasporti fisici come cosiddetti vettori (ad es. imprese dei tp o taxi) o che possiedono e mettono a disposizione un'infrastruttura o veicoli come gestori (ad es. Mobility) si uniscono sempre più spesso intermediari che non offrono direttamente mobilità, ma distribuiscono le offerte corrispondenti e in parte le combinano (ad es. Whim, moovel).

Web Application Filtering	Mediante un software di filtraggio web e delle applicazioni viene limitato l'accesso ad applicazioni, siti web e contenuti potenzialmente pericolosi.
Zero-day	Zero-day è un termine generico che designa le nuove vulnerabilità di sicurezza scoperte con cui gli hacker possono attaccare i sistemi. Il termine inglese «zero-day» si riferisce al fatto che un produttore o uno sviluppatore è appena venuto a conoscenza dell'errore e quindi ha «zero giorni» per correggerlo. Si parla di un attacco zero-day quando gli hacker possono sfruttare la vulnerabilità prima che gli sviluppatori siano in grado di eliminarla.
Zona demilitarizzata (DMZ)	Una zona demilitarizzata è una rete di computer con accesso sicuro ai server ad essa collegati. I sistemi installati nella DMZ sono protetti contro altre reti da uno o più firewall e da ulteriori misure tecniche di sicurezza.

Requisiti minimi sulla base dello standard minimo per le TIC (std. min. TIC UFAE)

<table>
<tr><th>Lo</th><th>Lm</th><th>L/S</th><th>Requisito</th><th>Std. min. TIC</th></tr>
<tr><td>X</td><td>X</td><td>X</td><td>1. Inventario degli oggetti da proteggere

Gli oggetti da proteggere e i rispettivi singoli componenti vanno riportati in maniera completa in un inventario.
Le modifiche agli oggetti da proteggere devono essere integrate nello stesso. Inoltre, ogni anno è necessario verificare le voci dell’inventario per assicurare che siano aggiornate.
Gli oggetti da proteggere che non sono più necessari o operativi devono essere rimossi dall’inventario.</td><td>ID.AM-1
PR.DS-3</td></tr>
<tr><td>X</td><td>X</td><td>X</td><td>2. Analisi delle esigenze di protezione

Per ogni oggetto da proteggere è necessario realizzare un’analisi delle esigenze di protezione. I criteri confidenzialità, integrità e disponibilità devono essere valutati almeno in tre livelli.
<table>
<tr><th></th><th>Confidenzialità</th><th>Integrità</th><th>Disponibilità</th></tr>
<tr><td>Nessun requisito</td><td>Pubblico</td><td>Nessun requisito</td><td>Sotto la responsabilità dell’utente NOVA</td></tr>
<tr><td>Requisiti standard</td><td>Interno</td><td>Verificabile</td><td>Sotto la responsabilità dell’utente NOVA</td></tr>
<tr><td>Maggiori requisiti</td><td>Confidenziale</td><td>Dimostrabile</td><td>Sotto la responsabilità dell’utente NOVA</td></tr>
</table>
Le disponibilità del gestore NOVA non fanno parte di questo allegato.</td><td>ID.AM-5
ID.BE-4</td></tr>
<tr><td>X</td><td>X</td><td>X</td><td>3. Matrice di comunicazione

Per ogni oggetto da proteggere collegatoa NOVA, devono essere documentati i flussi di comunicazione e di dati.
La relazione di comunicazione crea trasparenza e fornisce una visione d’insieme:

• da quali sistemi/applicazioni/utenti
• con quali log
• attraverso quali porte

si accede ad altri sistemi/applicazioni.</td><td>ID.AM-3
ID.AM-4</td></tr>
<tr><td></td><td>X</td><td>X</td><td>4. Sicurezza fisica

I sistemi IT e le infrastrutture devono essere protetti con misure strutturali/fisiche conformemente alle loro esigenze di protezione. In particolare, si deve garantire che solo le persone autorizzate abbiano accesso fisico o accesso al rispettivo oggetto da proteggere.</td><td>PR.AC-2</td></tr>
</table>

X	X	X	**5. Account utente – login degli utenti NOVA** Gli accessi utente ("login") assegnati direttamente in NOVA o nei sistemi collegati per l'utilizzo di oggetti da proteggere devono soddisfare i seguenti requisiti: • Gli utenti NOVA sono tenuti a creare un account personale per ogni personale che necessita dell'accesso a NOVA. Gli account di gruppo condivisi non sono ammessi. • Gli utenti di NOVA vigilano affinchégli account personali non vengano utilizzati da altre persone. • Gli utenti di NOVA tengono un elenco di tutti gli account e garantiscono l'identificazione del rispettivo titolare di ciascun account. • Gli utenti di NOVA sono tenuti, su richiesta, a comunicare al gestore di NOVA quale persona fisica utilizza un account e quali ruoli (amministratore/acesso tecnico, ecc.) le sono stati assegnati. • Sono stati stabiliti processi e misure tecniche per la concessione, la gestione e la revoca delle autorizzazioni per gli utenti e i dispositivi. • Le autorizzazioni comprendono tutti i tipi di accesso, in particolare anche gli accessi fisici, di sistema e remoti. • L'accesso deve avvenire tramite autenticazione a più fattori (MFA). • Gli utenti di NOVA con diritti privilegiati devono verificare almeno una volta l'identità del personale sulla base di un di un documento ufficiale d'identità valido, come un passaporto o una carta d'identità, e controllarne periodicamente l'integrità tramite estratti ufficiali aggiornati del casellario giudiziale o dell'ufficio esecuzioni.	PR.AC-1 PR.AC-6
X	X	X	**6. Account di sistema – login tecnici** I login tecnici dei sistemi collegati a NOVA devono soddisfare i seguenti requisiti: • Gli account devono essere unici e assegnati esclusivamente a una funzione tecnica o a un servizio. • Gli account devono essere attribuiti in modo univoco a una persona fisica responsabile come utente di NOVA. • Gli user devono avere solo i privilegi necessari per la funzione tecnica o il servizio richiesto. • La password deve essere cambiata ad ogni aggiornamento principale della versione, almeno una volta all'anno..	PR.AC-1 PR.AC-2 PR.AC-4 PR.AC-6

X	X	X	**7. Gestione delle password** Gli oggetti da proteggere devono richiedere dal sistema password complesse: • Un requisito minimo per la password (cfr. requisito 8) è impostato a livello di sistema e impone automaticamente i seguenti criteri: • Le password non possono essere riutilizzate. • Archiviazione crittografata o con hash delle password. • È vietata l'archiviazione di password in chiaro. • Nessuna trasmissione di password. Inoltre, a livello di sistema deve essere garantito che le password iniziali/di default siano tassativamente modificate quando si accede per la prima volta. Per reimpostare password dimenticate, scadute o bloccate, per ogni oggetto da proteggere deve essere presente un processo attuato e documentato.	PR.IP-1
X	X	X	**8. Requisiti delle password£éà** Nel caso degli oggetti da proteggere devono essere soddisfatti i seguenti requisiti delle password: • Lunghezza minima della password: 12 caratteri • Composizione della password: alfanumerica incl. caratteri maiuscoli/minuscoli • Nessun termine dai dizionari	PR.IP-1
		X	**9. Accesso remoto** Gli accessi agli oggetti da proteggere per la manutenzione dei dati NOVA da reti non NOVA devono soddisfare i requisiti standard del mandatario per NOVA. L'accesso temporaneo viene concesso a terzi. Gli accessi e i relativi diritti di accesso devono essere documentati, verificati regolarmente e limitati al minimo indispensabile (principio dei privilegi minimi). I subappaltatori si assumono l'obbligo di rispettare i requisiti. Per la manutenzione da remoto devono essere creati account utente personalizzati. Questi devono essere monitorati, protetti (MFA) e il loro utilizzo deve essere documentato in modo tracciabile (logging).	PR.AC-3 PR.MA-2

X	X	X	**10. Registrazione di oggetti da proteggere** La registrazione e la relativa entità devono essere definite per ogni oggetto da proteggere insieme all'incaricato della sicurezza delle informazioni/CISO. In linea di principio, le seguenti attività devono essere registrate e monitorate in forma pseudonimizzata per gli oggetti protetti, per uno scopo specifico e in modo comprensibile: • avvio e spegnimento del sistema: • procedure di accesso; • accessi remoti; • accessi falliti agli oggetti; • assegnazione e modifica dei privilegi; • tutte le azioni che richiedono privilegi elevati; • modifiche del sistema. I dati di log devono essere analizzati, archiviati centralmente, conservati per sei mesi e valutati. I file di log devono essere protetti da successive manipolazioni.	PR.MA-1 PR.MA-2 PR.PT-1 DE.AE-1 DE.AE-5 DE.CM-1 DE.CM-2 PR.DS-5
X	X	X	**11. Log di traffico dei ponti di rete** Tutti i log di traffico (file di log e log proxy) dei ponti di rete (firewall e gateway) in relazione a NOVA devono essere conservati per 6 mesi e analizzati conformemente alle regole. I log devono essere protetti da ulteriori manipolazioni. Quando si utilizzano i servizi NOVA nello stato di contratto L/S, tutti i dati del traffico devono essere controllati attivamente tramite monitoring e, in caso di anomalie, trasferiti a un processo di analisi.	PR.MA-1 PR.MA-2 PR.PT-1
X	X	X	**12. Crittografia dell'accesso** Tutti gli accessi agli oggetti da proteggere devono essere crittografati durante la trasmissione. La crittografia deve essere effettuata in conformità allo stato attuale della tecnica (cfr. clausola 13).	PR.DS-2

X	X	X	**13. Metodi di crittografia** Se è richiesta la crittografia, per gli oggetti protetti e le password possono essere utilizzati solo metodi di crittografia riconosciuti e controllati con generazione di chiavi sicure. Deve essere rispettata una lunghezza minima della chiave, come descritto di seguito. Attualmente sono ammessi i metodi seguenti: • Crittografia simmetrica: AES 256 bit. • Crittografia asimmetrica: RSA con una lunghezza in bit pari ameno a 2048 bit o metodi analoghi. • Funzione hash crittografica: SHA2 o SHA3 con almeno 256 bit. • Scambio di chiave: Diffie-Hellman con almeno 2048 bit o metodi analoghi. Quando si utilizzano le suite di cifratura TLS, le suite di cifratura offerte devono essere limitate ad algoritmi sicuri. Non sono più considerati sicuri: • Algoritmi di crittografia: RC4, DES, IDEA • Metodi di crittografia: ECB • Funzioni hash: MD4, MD5, SHA-1 (eccetto HMAC) • Lunghezze della chiave inferiore a XZ<128 bit in caso di algoritmi simmetrici Questi requisiti si applicano all'archiviazione come anche alla trasmissione di dati.	PR.DS-2
X	X	X	**14. Impiego di certificati** Gli accessi web agli oggetti da proteggere devono essere effettuati utilizzando una crittografia del traffico TLS. Si applicano le regole seguenti: • Gli accessi web di terzi agli oggetti da proteggere devono avvenire mediante un certificato TLS pubblico valido. • Gli accessi agli oggetti da proteggere che sono disponibili solo per un gruppo chiaramente definito di persone, possono avvenire tramite un certificato emesso dalla CA interna. I certificati TLS devono essere ottenuti daun'autorità di certificazione (CA) pubblica riconosciuta, secondo un processo definito. Se un oggetto da proteggere si basa su certificati client (ad esempio per l'autenticazione di dispositivi mobili), questi devono essere firmati dalla CA interna e, all'occorrenza, creati da essa. I certificati possono avere un periodo di validità massimo di due anni.	PR.DS-2
	X	X	**15. Eliminazione dei dati e delle informazioni** Se gli oggetti da proteggere o parti di essi vengono dismessi, sostituiti o messi fuori servizio, tutti i dati relativi ai servizi NOVA (in particolare i dischi rigidi) devono essere eliminati in modo completo e irreversibile oppure distrutti fisicamente in modo da non poter essere recuperati.	PR.IP-6 PR.DS-3

	X	X	**16. Scansione delle vulnerabilità** Tutti gli oggetti da proteggere devono essere sottoposti a una scansione delle vulnerabilità prima del rollout produttivo e in caso di tutte modifiche importanti (cfr. requisito n. 22). Le vulnerabilità riconosciute devono essere segnalate ai responsabili interni (ad es. responsabili della sicurezza delle informazioni – ISO, CISO, ecc.) e trattate immediatamente. Come regola generale : Critico, 9.0 - 10.0 --> immediatamente/prima del GoLive • - Le vulnerabilità con un livello CVSS v3 compreso tra 9.0 e 10.0 e un potenziale di danno critico devono essere corrette immediatamente o prima del GoLive. Alto, 7.0 - 8.9 --> Entro 6 settimane/prima del GoLive • Le vulnerabilità con un livello CVSS v3 compreso tra 7.0 e 8.9 e un potenziale di danno elevato devono essere corrette entro 6 settimane o prima del GoLive.	PR.IP-12 DE.CM-8
	X	X	**17. Test di penetrazione** Gli oggetti da proteggere accessibili da Internet devono essere sottoposti a un test di penetrazione per verificare la presenza di vulnerabilità prima della messa in servizio e in caso di modifiche o aggiornamenti importanti (cfr. requisito n. 22). Il controllo dovrebbe essere effettuato da un ente indipendente. Secondo lo standard OWASP TOP 10, in seguito i servizi web non dovrebbero più presentare vulnerabilità con un livello di severità elevato (high) o addirittura critico (critical). Gli oggetti da proteggere con diritti di lettura e scrittura devono essere controllati mediante test di penetrazione prima dell'implementazione e in caso di modifiche e aggiornamenti importanti (cfr. requisito n. 22). Il controllo deve essere effettuato da un ente indipendente.	DE.CM-8
	X	X	**18. Modifiche agli oggetti da proteggere** Le modifiche agli oggetti da proteggere devono essere documentate in modo tracciabile e gestite tramite un processo di gestione delle modifiche (change management). In tale contesto, le funzioni critiche e importanti ai fini della sicurezza devono essere controllate per verificare il loro funzionamento e, se necessario, adattate immediatamente.	PR.IP-3 PR.DS-6
X	X	X	**19. Considerazione della baseline di sicurezza al momento della stipula del contratto** I requisiti minimi di questo documento devono essere presi in considerazione già al momento della stipula del contratto, il che corrisponde qui all'accettazione dell'allegato 12 della c500 e del contratto standard NOVA.	ID.SC-3

	X	X	**20. Separazione tra ambiente operativo e ambiente di test** Per lo sviluppo e il test degli oggetti da proteggere, gli ambienti produttivi e non produttivi (staging, testing,…) devono essere separati in modo tale che non vi siano restrizioni nell'ambiente produttivo durante il test e lo sviluppo.	PR.DS-7
	X	X	**21. Considerazione degli standard di sviluppo software sicuri** Nello sviluppo delle applicazioni devono essere utilizzati standard di sicurezza riconosciuti (ad es. OWASP TOP 10 per lo sviluppo web o NIST SP 800-218 per lo sviluppo di software).	PR.IP-1
	X	X	**22. Utilizzo di dati di test fittizi** Per i test nell'ambito dello sviluppo e dell'approntamento di applicazioni vengono utilizzati esclusivamente dati fittizi.	PR.DS-7
	X	X	**23. Interfacce utente e API** Se nell'ambito degli oggetti da proteggere vengono implementate interfacce utente, per tutte le interfacce si applica quanto segue: • l'input e l'output devono essere convalidati; • sono ammessi solo i valori esplicitamente consentiti (whitelisting); • devono essere convalidati anche i parametri nascosti, come variabili, valori di intestazione e informazioni sui cookie; • la convalida comprende tutti i tipi di input e output, in particolare i dati binari.	PR.IP-1
	X	X	**24. Creazione di configurazioni standard e protezione avanzata del sistema** Per ogni oggetto da proteggere, nell'ambito dell'implementazione devono essere create configurazioni standard. Le misure di protezione avanzata devono soddisfare il livello CIS 1. Si tratta tra le altre delle misure specifiche seguenti: • i servizi non necessari o non esplicitamente richiesti devono essere disattivati e, se possibile, eliminati o disinstallati; • gli account non necessari devono essere disattivati o eliminati; • i file temporanei vengono eliminati automaticamente al momento della disconnessione; • Le impostazioni di sicurezza devono essere gestite a livello centrale; • le condivisioni standard sono disattivate.	PR.IP-1
	X	X	**25. Crittografia dei backup dei dati** I backup dei dati devono essere criptati.	PR.IP-4

X	X	X	**26. Protezione da malware** Ogni oggetto da proteggere deve essere protetto da malware. Tutti gli oggetti da proteggere con interazione diretta con l'utente devono disporre di una soluzione malware aggiornata ed efficace. I subappaltatori si assumono l'obbligo di rispettare i requisiti.	DE.CM-4 DE.CM-5 PR.DS-6
	X	X	**27. Verifica dell'integrità** La verifica dell'integrità delle transazioni degli oggetti da proteggere NOVA e delle informazioni di login deve essere eseguita in modo continuativo per individuare tempestivamente modifiche non autorizzate, scostamenti e possibili vulnerabilità. Il controllo può essere fornito dai registri di audit e delle transazioni. Quando si trasmettono i dati, è necessario utilizzare procedure per prevenire la modifica dei dati durante la trasmissione, controllando i valori di hash (ad esempio, utilizzando le procedure TLS).	PR.DS-6
	X	X	**28. Installazione di patch e aggiornamenti** Per ogni oggetto da proteggere gestito per i servizi NOVA deve essere documentata la gestione delle patch e degli aggiornamenti al fine di garantirne l'aggiornamento continuo. Gli aggiornamenti o le patch critici per la sicurezza devono essere installati immediatamente, e comunque entro 30 giorni dalla loro pubblicazione. L'incaricato della sicurezza delle informazioni (ISO) o il CISO della mandataria può ordinare la distribuzione di patch entro 48 ore in caso di emergenze giustificate (zero-day) e d'intesa con l'appaltatore.	PR.IP-2
	X	X	**29. Ora di sistema** L'ora di sistema degli oggetti da proteggere deve essere sincronizzata a livello centrale.	PR.IP-1
	X	X	**30. Manutenzione remota da parte di terzi** La manutenzione remota degli oggetti da proteggere da parte di terzi deve avvenire in modo controllato. Si applicano le stesse regole di gestione degli utenti e dei diritti di accesso previste per gli altri utenti.	PR.AC-3 PR.MA-2

	X	X	**31. Concetto di zona** Per il funzionamento degli oggetti da proteggere è necessario sviluppare un concetto di zona di sicurezza e assicurarne la manutenzione. Il concetto di zona deve tenere conto dei seguenti principi: • A ogni zona deve essere assegnato il proprio posto nel concetto di zona in base alla criticità e alla sensibilità dei relativi oggetti da proteggere. • I passaggi di zona devono essere limitati con misure adeguate per esempio Stateful Firewalling/Intrusion detection/Web Application Filtering ecc. in modo da evitare la diffusione laterale indesiderata. • Possono essere utilizzati solo protocolli standardizzati dalla suite TCP/IP. • Il traffico da reti non sicure (ad es. Internet) deve essere inoltre protetto da attacchi DDoS e da metodi di attacco noti mediante un sistema di rilevamento delle intrusioni. Il traffico da e verso reti non sicure deve essere inoltre programmato in una zona DMZ (interruzione del protocollo). • Considerando le esigenze di protezione, ogni oggetto da proteggere deve essere posizionato in una zona di sicurezza adeguata. Il posizionamento deve essere collaudato dal responsabile del concetto di zona o dal responsabile della sicurezza delle informazioni (ISO)..	PR.AC-5 PR.PT-4
	X	X	**32. Verifica del software** Tutti i software utilizzati nell'ambito degli oggetti da proteggere per i servizi NOVA devono essere verificati e possono essere acquistati solo direttamente dall'offerente ufficiale o da uno dei suoi partner certificati. Devono essere garantite l'affidabilità delle fonti e la protezione contro qualsiasi modifica non autorizzata del software. • L'autenticità e l'integrità del software utilizzato per gli oggetti da proteggere devono essere garantite in maniera automatizzata mediante procedure crittografiche (firme, verifica degli hash). • Il software che non può essere testato in maniera automatizzata per verificarne l'autenticità deve essere controllato manualmente (query dei valori hash sul sito web dello sviluppatore). • I software open source devono provenire da fonti ufficiali e affidabili e disporre di una licenza open source di un'organizzazione riconosciuta, come GPL, MIT, BSD, ASF, MPL, ecc.	PR.DS-6
	X	X	**33. Comunicazione software a livello di reti** La comunicazione a livello di rete deve avvenire tramite porte server fisse (TCP/IP). Non è consentito l'utilizzo di intervalli di porte server dinamici.	PR.AC-5

X	X	X	**34. Acquisizione di funzionalità rilevanti per la sicurezza** La sicurezza della piattaforma NOVA viene continuamente migliorata. Gli utenti NOVA si impegnano ad aggiornare e a implementare le funzionalità rilevanti per la sicurezza tempestivamente, ma non oltre 3 mesi dalla loro disponibilità nell'ambiente produttivo. Per le release altamente critiche o eccezionalmente ampie, in singoli casi il gestore NOVA può stabilire una scadenza vincolante diversa.	PR.IP-2