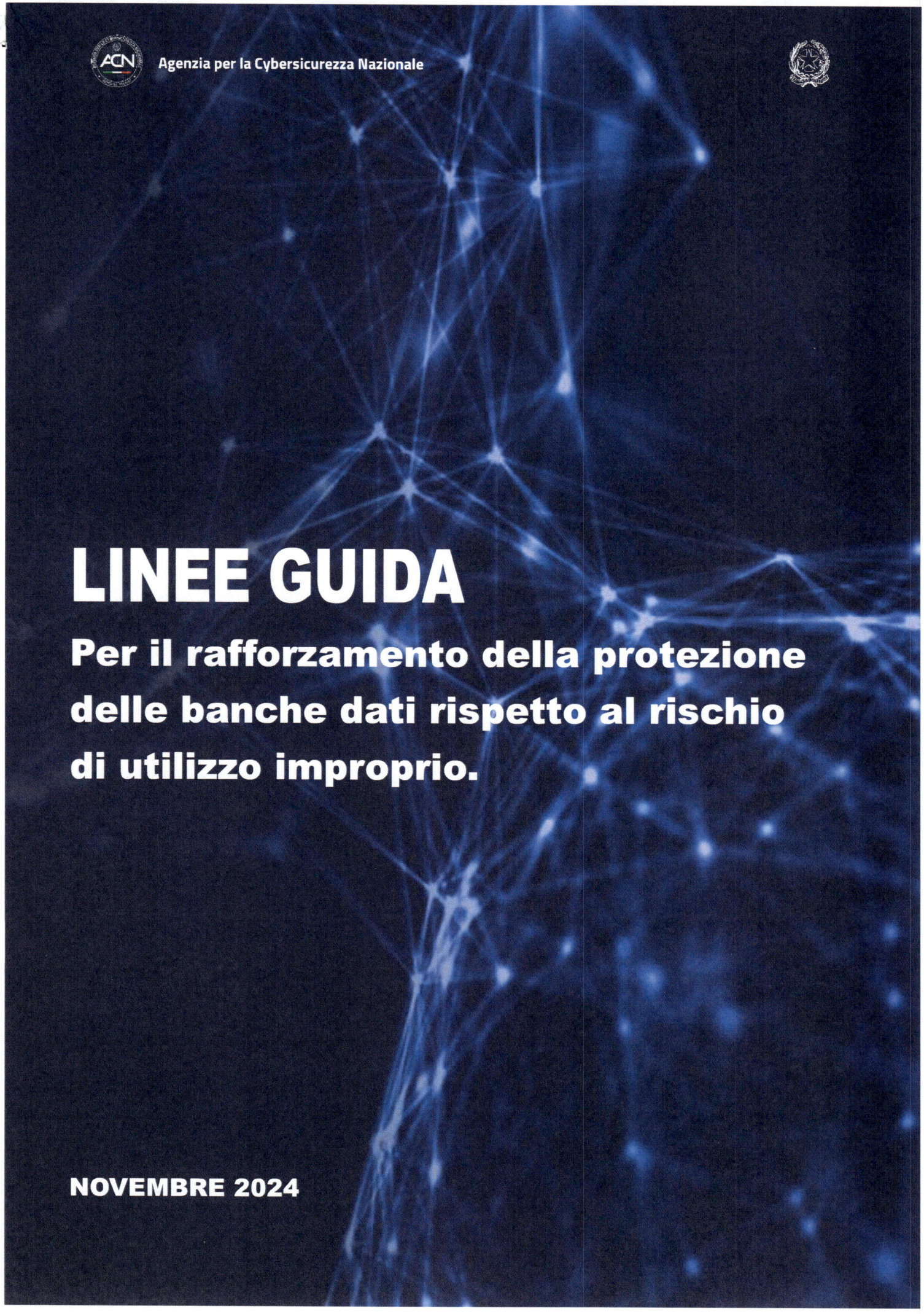
Agenzia per la Cybersicurezza Nazionale
LINEE GUIDA
Per il rafforzamento della protezione delle banche dati rispetto al rischio di utilizzo improprio.
NOVEMBRE 2024

SOMMARIO

1. Analisi del contesto

Negli ultimi mesi sono emersi diversi casi di utilizzo improprio di banche dati di rilevanza nazionale da parte di soggetti o organizzazioni che, con differenti tecniche e finalità, sono riusciti ad ottenere l'accesso alle informazioni in esse contenute senza averne titolo.

Secondo quanto riportato dai media, tali organizzazioni realizzavano, su mandato dei propri clienti o su richiesta di affiliati, report e dossier contenenti le informazioni abusivamente raccolte.

Le tecniche utilizzate per le attività illecite sarebbero sintetizzabili in 3 modalità principali:

- ottenimento di informazioni tramite presunte attività corruttive riferibili a pubblici ufficiali infedeli;
- installazione di software per il controllo remoto (RAT[1]) in particolare di server utilizzati per erogare i servizi verosimilmente in esito alla possibilità di operare sugli stessi, da parte di persone collegate alle aziende coinvolte, in forza di un contratto di manutenzione in essere o similari;
- installazione di software per il controllo remoto (RAT) su postazioni di lavoro aziendali e private con la complicità dei gestori dei sistemi informatici delle aziende clienti.

[1] Remote administration tool.

2. Criticità emerse

L'analisi di tali eventi, seppur in presenza di alcune differenze in termini di "intento", "organizzazione" e "capacità" mostrate dai protagonisti delle singole vicende, consente di identificare alcuni punti di sovrapposizione tra le stesse.

Nello specifico:

- la gran parte delle azioni malevole è stata perpetrata, o quantomeno agevolata, dalla possibilità di accesso alle informazioni grazie a permessi assegnati ai protagonisti delle vicende in esito alle loro specifiche attività lavorative;
- limitato utilizzo delle classiche tecniche di compromissione di infrastrutture informatiche, ad esempio, attraverso lo sfruttamento di vulnerabilità software nei sistemi;
- movimento all'interno delle reti e dei sistemi mediante comportamenti ritenuti leciti dai comuni sistemi di protezione (es. AV, EDR, Firewall, ecc.) che pertanto risultano inefficaci nella fase di rilevamento;
- limitata efficacia dei sistemi di *alerting* predisposti per il rilevamento di comportamenti impropri nell'accesso alle informazioni in particolare in ottica preventiva.

Tali considerazioni consentono di identificare criticità non solo di carattere prettamente tecnico ma legate ad aspetti organizzativi e di governance delle informazioni e nello specifico:

- eccessiva "ampiezza" dei permessi consentiti agli utenti abilitati all'accesso alle informazioni;
- utilizzo di banche dati realizzate anteriormente alla diffusione dei principi di security-by-design, privacy-by-design, zero-trust;
- limitata governance del ciclo di vita dei sistemi e delle applicazioni utilizzate in particolare per la gestione di informazioni sensibili;
- limitata gestione dei processi di sicurezza nella gestione della supply chain;
- ridotta capacità di monitoraggio e auditing di comportamenti impropri da parte di dipendenti infedeli in chiave preventiva;
- limitata disponibilità di personale adeguatamente formato nelle attività di verifica e identificazione di azioni improprie di questa tipologia.

A queste considerazioni si aggiungono quelle relative all'esigenza di specificare con maggiore chiarezza cosa si intende per utilizzo improprio.

Si versa in questa fattispecie allorché:

a) l'utilizzo delle credenziali di accesso legittimamente detenute dall'operatore risulti strumentale al perseguimento di scopi estranei alle necessità funzionali di accesso, quale che sia l'intenzionalità dell'operatore, ivi incluso l'accesso a informazioni che esulano dalla necessità di conoscere ai fini dello svolgimento delle mansioni per le quali tali credenziali sono state assegnate;
b) l'utilizzo delle credenziali di accesso legittimamente detenute è in violazione delle politiche sul loro utilizzo definite dal fornitore del servizio;
c) in tutti i casi di utilizzo illegittimo delle credenziali di accesso da parte di altro operatore (o altri operatori) diverso da quello legittimato, in qualsivoglia modo ne abbia ottenuto la disponibilità e per qualsivoglia scopo (che sia estraneo alle necessità funzionali di accesso).

I casi di utilizzo improprio dipendenti da accesso abusivo da parte di operatori interni sono presidiati dall'articolo 4 del decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81 relativo alle notifiche volontarie degli incidenti. Ciò nelle more di un prossimo aggiornamento che ne stabilirà l'obbligo in caso di superamento delle soglie critiche per la cui descrizione si rinvia a pagina 14.

3. Contesto normativo

A tutela degli assetti digitali del Paese, ivi incluse le banche dati più sensibili e le infrastrutture che le ospitano, insiste un ampio corpus di misure di sicurezza discendenti dalla normativa vigente, oggetto di costante aggiornamento.

Il livello più elevato di protezione per i dati più critici del Paese, connessi alla tutela della sicurezza nazionale, è assicurato dal Perimetro di sicurezza nazionale cibernetica, istituito con decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla legge 18 novembre 2019, n. 133. Questo prevede misure di sicurezza particolarmente stringenti, declinate nell'allegato B del decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, che si applicano alle reti, ai sistemi informativi e ai servizi informatici dei soggetti pubblici e privati da cui dipende l'esercizio di una funzione essenziale dello Stato o la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato dalla cui compromissione possa derivare un pregiudizio per la sicurezza nazionale.

Inoltre, tutte le banche dati della pubblica amministrazione sono soggette alle previsioni del cd. Regolamento Cloud, adottato ai sensi dell'articolo 33-septies del decreto-legge 18 ottobre 2012, n. 179 e recentemente aggiornato da ACN con Decreto Direttoriale n. 21007 del 27 giugno 2024. Ai sensi del citato Regolamento tutte le pubbliche amministrazioni sono chiamate a classificare i propri dati e servizi digitali quali ordinari, critici o strategici, secondo il modello predisposto da ACN.

Tale attività è finalizzata ad assicurare che i dati e i servizi digitali della pubblica amministrazione siano trattati ed erogati attraverso infrastrutture digitali e servizi cloud che rispettano requisiti, ivi inclusi quelli di sicurezza, adeguati ai rischi connessi al relativo livello di classificazione, così come declinati dal Regolamento. L'esercizio di classificazione consente anche di individuare le banche dati considerate strategiche.

Più recentemente la legge 28 giugno 2024, n. 90, ha introdotto obblighi tesi al rafforzamento della resilienza delle pubbliche amministrazioni centrali e di numerose amministrazioni locali, con l'individuazione di un referente e di una struttura responsabili per l'attuazione, ivi inclusa l'adozione delle linee guida per la cybersicurezza che saranno emanate da ACN.

In prospettiva, il decreto legislativo del 4 settembre 2024, n. 138, di recepimento della direttiva (UE) 2022/2555 (cd. direttiva NIS), prevede un ampio catalogo di obblighi, con punti specifici relativi alla sicurezza della catena di approvvigionamento, alla manutenzione dei sistemi informativi e di rete, nonché alla sicurezza e all'affidabilità del personale. Tali obblighi saranno declinati con riguardo ai principi di proporzionalità e gradualità con determinazioni dell'Agenzia ad aprile 2025, definendo una cornice di sicurezza generalizzata per rafforzare ulteriormente la protezione delle banche dati già tutelate dal Perimetro.

4. Possibili azioni di contrasto

La risoluzione delle criticità individuate al capitolo 2 necessita di un approccio strutturato che concili aspetti normativi, procedurali, tecnici, tecnologici e di risorse sia economiche sia in termini di personale.

Si è già avuto modo di richiamare nel paragrafo precedente le misure di sicurezza particolarmente stringenti dettate dal DPCM 81/2021 che i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica (PSNC) sono obbligati a porre in essere a protezione delle funzioni e/o servizi essenziali inseriti nel PSNC.

Con le presenti linee guida si intende fornire un'ulteriore loro declinazione rafforzativa sotto il profilo tecnico, organizzativo e procedurale allo scopo di rafforzare la mitigazione dei rischi connessi alle criticità individuate nel capitolo 2.

In particolare, per ciascun ambito di intervento sono indicate le misure di sicurezza che possono essere considerate come base di riferimento per potenziare le capacità di mitigazione dei rischi promananti anche dall'utilizzo improprio delle credenziali di accesso alle banche dati (riquadro "Misure di sicurezza di riferimento").

L'elenco delle misure di sicurezza selezionate è inoltre riportato in appendice A. Queste sono state opportunamente selezionate dal catalogo di misure di cui al citato allegato B al DPCM 81/2021 e al cd. Regolamento Cloud (Decreto Direttoriale n. 21007 del 27 giugno 2024), a loro volta derivate dal Framework Nazionale per la Cybersecurity e la Data Protection[2]. In aggiunta, per ciascun ambito sono indicate una serie di raccomandazioni specifiche per il contesto in esame.

L'adozione delle misure di sicurezza e delle raccomandazioni di cui al presente documento non esenta, tuttavia, dall'implementazione delle restanti misure previste dal DPCM 81/2021, dal Regolamento Cloud e dalla normativa NIS2, ove queste ultime discipline siano applicabili.

Tali misure di sicurezza e raccomandazioni devono, quindi, essere intese come elementi cui porre particolare attenzione al fine di indirizzare le specifiche criticità riscontrate per il contesto in esame e non possono essere ritenute esaustive di tutte le attività da porre in essere per proteggere i sistemi da tutti i tipi di minacce cui possono essere esposti.

4.1. Controllo degli accessi

Misure di sicurezza di riferimento: PR.AC-1, PR.AC-2, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-7, PR.MA-2.

Strutturare un controllo degli accessi coerente e robusto rappresenta la base per garantire che l'accesso a sistemi e banche dati sia ristretto al personale e alle utenze autorizzati e che ne hanno la necessità in virtù del loro ruolo.

[2] https://www.cybersecurityframework.it/framework2

A tale scopo le identità digitali del personale e le relative credenziali di accesso a sistemi e banche dati devono essere amministrate. Le identità digitali devono essere nominative e individuali, non devono essere, cioè, condivise tra più persone, anche al fine di poter tracciare gli accessi e poter risalire in modo inequivocabile al personale interno ed esterno che effettua gli accessi. Nel caso delle "identità di sistema", per loro natura impersonali in quanto utilizzate da applicativi *software*, è necessario garantirne una gestione sicura, volta a mitigare sia il rischio di utilizzo diretto da parte del personale dell'Amministrazione, sia quello di impossessamento in generale.

A ciascuna identità digitale devono essere assegnati privilegi e autorizzazioni di accesso minimi, strettamente necessari a svolgere i compiti assegnati al relativo ruolo e che rispettano il principio di segregazione delle funzioni.

Le utenze, i relativi privilegi e credenziali sono verificati, aggiornati, revocati e sottoposti a audit periodicamente, secondo una cadenza temporale coerente con l'analisi dei rischi, considerando la criticità dei sistemi e delle banche dati cui possono accedere e il tipo di operazioni che possono effettuare.

Le utenze e le relative credenziali devono essere aggiornate tempestivamente, e senza ingiustificato ritardo, in seguito a variazioni delle utenze (es. trasferimento di personale) e, in particolare, devono essere revocate tempestivamente per il personale cessato.

Deve essere implementato un modello di gestione degli accessi centralizzato. Tutti gli accessi ai sistemi e alle banche dati, anche da remoto, da parte degli utenti devono essere registrati e monitorati. Per gli accessi ai sistemi e alle banche dati devono essere impiegate modalità di autenticazione multifattore.

Le modalità di autenticazione per le diverse utenze devono essere commisurate al rischio connesso ai privilegi delle utenze, alla criticità dei sistemi e delle banche dati cui accedono e alla tipologia di operazioni che possono effettuare sugli stessi.

Le predisposizioni di accesso utilizzate per le applicazioni che consentono l'interrogazione delle banche dati devono essere applicate anche a tutte le componenti utilizzate per l'erogazione del servizio (es. server, database, sistemi di virtualizzazione, VPN, etc.) al fine di prevenire la possibilità di accesso ai dati eludendo i sistemi di monitoraggio in essere.

In virtù della possibilità di accesso al dato anche attraverso modalità diverse da quelle logiche, è necessario predisporre le opportune misure di protezione di natura fisica, sia di tipo preventivo che di monitoraggio. Tali misure devono riguardare primariamente l'area in cui sono presenti i sistemi di elaborazione e memorizzazione relativi alle banche dati, nonché i sistemi per l'interconnessione su rete locale su cui questi insistono. Più in dettaglio, anche in riferimento ai controlli previsti per le Infrastrutture Digitali della PA nel Decreto Direttoriale n. 21007 del 27 giugno 2024, è necessario assicurare la protezione a partire

dai varchi dell'edificio[3], prevedendo l'ausilio aggiuntivo di sistemi di videosorveglianza[4], al fine di garantire il controllo degli accessi fisici. Il presidio del personale di sicurezza fisica deve essere garantito 24h.

Raccomandazioni di contesto

1. Assicurare la completa distinzione tra utenze con ruoli e privilegi differenti alle quali debbono corrispondere credenziali diverse.
2. Prevedere l'autenticazione multifattore per l'accesso ai sistemi e alle banche dati.
3. Prevedere una gestione centralizzata del controllo degli accessi.
4. Prevedere l'utilizzo di strumenti di gestione degli accessi privilegiati (PAM).
5. Adottare meccanismi di gestione e controllo delle utenze privilegiate, in termini di limitazioni di natura temporale e delle funzionalità amministrative disponibili.
6. Nei casi di condivisione del dominio di autenticazione tra sistemi (es: accesso *Single Sign-On* alla banca dati coincidente con quello utilizzato per le postazioni di lavoro), implementare delle misure volte a mitigare il rischio di riuso degli artefatti di autenticazione reperibili su sistemi terzi quali, ad esempio, la contestuale richiesta di verifica del secondo fattore o di ripetizione della password prima di accedere alle funzionalità critiche del sistema (es: interrogazione su banca dati).
7. Considerare l'impiego di sistemi di controllo degli accessi basati su modelli quali *Mandatory Access Control* (*MAC*), *Discretionary Access Control* (*DAC*), *Role-Based Access Control* (*RBAC*), *Rule-Based Access Control* (*RuBAC*) che segnalino allarmi in caso di accessi non autorizzati.

4.2. Applicazione di principi e buone pratiche di sviluppo sicuro dei sistemi e delle applicazioni

Misure di sicurezza di riferimento: PR.IP-1, PR.IP-3, PR.IP-4, PR.DS-1, PR.DS-7, PR.AC-1

La sicurezza dei sistemi e delle applicazioni deve essere garantita sin dalla progettazione (*security by design*) e per impostazione predefinita (*security by default*) adottando le buone pratiche di sviluppo sicuro e assumendo che nessuna connessione, utente o sistema/applicazione possa essere considerata attendibile sino a quando non viene verificata (*zero-trust security*).

In aggiunta devono essere definite, stabilite e mantenute delle pratiche di riferimento (c.d. *baseline*) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (come, ad

[3] Ingresso protetto con porte interbloccate con accesso singolo, unitamente a sistemi anti-scavalcamento e anti-*passback*, sorvegliato attraverso guardiola e bancone di sorveglianza per il controllo delle autorizzazioni, anch'esso adeguatamente protetto (vetro antiproiettile livello 3).

[4] Controllo TVCC su tutti i varchi con controllo d'accesso e di uscita, nonché sulle aree ristrette con accesso tramite porte con badge. Il periodo di conservazione delle registrazioni TVCC è almeno di 30 giorni e la frequenza delle immagini è pari almeno a 20 frame\sec.

esempio, il principio di minima funzionalità) indicando le politiche di sicurezza adottate per lo sviluppo di configurazioni di sistemi IT e di controllo industriale e il dispiegamento delle sole configurazioni adottate, le politiche di sicurezza adottate per l'aggiornamento delle configurazioni dei sistemi e delle applicazioni e per il controllo della modifica delle configurazioni in uso rispetto a quelle previste, l'elenco delle configurazioni dei sistemi e delle applicazioni impiegate e il riferimento alle relative pratiche di riferimento, i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

In particolare, si raccomanda che le cosiddette "pipeline di sviluppo" siano composte da almeno tre ambienti separati, a cui devono essere applicate le opportune segregazioni in termini di accesso e gestione dati:

- **sviluppo**: è l'area in cui opera lo sviluppatore dove avviene la scrittura del codice, quest'area non deve avere accesso ai dati reali gestiti dall'applicazione in particolare se critici;
- **staging**: è l'area che riproduce in maniera esatta l'ambiente di produzione dove vengono effettuati tutti i test approfonditi prima del rilascio nell'area di produzione. Oltre ai test funzionali è in quest'area che devono essere eseguiti i test di sicurezza orientati all'identificazione della presenza nel codice di eventuali vulnerabilità e/o backdoor intenzionali. Anche in questa area non devono essere presenti i dati reali gestiti dall'applicazione;
- **produzione**: è l'area dove l'applicazione viene effettivamente messa a disposizione degli utenti. Considerato che è sempre possibile che alcuni bug e/o vulnerabilità raggiungano l'area di produzione, i meccanismi di rilascio delle patch correttive dovranno sempre seguire le attività di test nell'area staging e mai dovrà essere rilasciato codice direttamente dall'area di sviluppo a quella in produzione.

Raccomandazioni di contesto

1. Minimizzare la superficie d'attacco, ad esempio disinstallando o disabilitando servizi e software non necessari.
2. Integrare le funzionalità di monitoraggio e allarme già dalla fase di progettazione, ivi inclusi gli aspetti di rilevamento.
3. Prevedere strati multipli di controlli di sicurezza (*defense in depth*) per la protezione dei sistemi e delle banche dati.
4. Adozione, per le banche dati e i sistemi ad uso anche interno, di protocolli che garantiscano l'integrità del flusso di rete e la protezione dei dati in transito, con particolare riferimento alla cifratura del canale di comunicazione.
5. Garantire la separazione degli ambienti di sviluppo e test dei sistemi da quelli di produzione, anche in riferimento ai rispettivi meccanismi di autenticazione.
6. Adottare metodologie sicure, di natura tecnica (es: utilizzo di certificati digitali) e\o organizzativa (es: generazione di password casuale estremamente complessa, conservata in cassaforte), per la gestione delle identità di sistema, al fine di mitigare il rischio di accessi non autorizzati ai sistemi di difficile identificazione e attribuzione.

7. Adottare opportune tecniche di protezione (cifratura, limitazione accessi) anche a favore delle copie di backup dei dati dei sistemi.
8. Adottare linee guida (es: OWASP) e misure tecniche/organizzative per lo sviluppo sicuro (requisiti, progettazione, implementazione, test e verifica) e le evoluzioni dei propri sistemi. In caso di sviluppo affidato a terzi, deve esserne assicurata l'applicazione da parte degli stessi.

4.3. Gestione del ciclo di vita dei sistemi e delle applicazioni

Misure di sicurezza di riferimento: PR.MA-1, PR.MA-2, PR.IP-2, PR.IP-12, PR.DS-3, DE.CM-8

La sicurezza dei sistemi e delle applicazioni deve comprendere tutte le fasi del ciclo di vita dei sistemi e delle applicazioni. A tale scopo, deve essere implementato un processo per la gestione del ciclo di vita dei sistemi (*System Development Life Cycle*), che contempli altresì una formale gestione delle vulnerabilità, coerente con ciascuna fase del ciclo.

In aggiunta, la manutenzione e la riparazione dei sistemi e delle applicazioni deve essere eseguita e registrata con strumenti controllati ed autorizzati indicando le politiche di sicurezza adottate per la registrazione della manutenzione e riparazione dei sistemi e delle applicazioni e i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza e predisponendo un registro aggiornato delle manutenzioni e riparazioni eseguite. In base all'analisi del rischio, ogni aggiornamento dei sistemi e delle applicazioni ritenuti critici, fatte salve motivate esigenze di tempestività relative alla sicurezza, dovrà essere verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo e il relativo codice oggetto dovrà essere custodito per almeno 24 mesi.

Inoltre, la manutenzione remota dei sistemi e delle applicazioni deve essere approvata, documentata e svolta in modo da evitare accessi non autorizzati in accordo alle politiche definite per l'accesso remoto ai sistemi e alle applicazioni procedendo, ove applicabile, alla conservazione dei log delle attività svolte.

Tutti gli accessi eseguiti da remoto da personale di terze parti devono essere autorizzati dall'organizzazione e limitati ai soli casi essenziali e devono essere adottati stringenti meccanismi di protezione per l'autenticazione, l'identificazione e per il tracciamento degli eventi e meccanismi di gestione e controllo delle utenze privilegiate, in termini di limitazioni di natura temporale e delle funzionalità amministrative disponibili. Tutti i log relativi alle sessioni di comunicazione remota e alle attività eseguite sui sistemi remoti, devono essere prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze remote.

Raccomandazioni di contesto

1. Garantire che il processo per la gestione del ciclo di vita delle banche dati sia approvato dai vertici dell'organizzazione.

2. Revisionare il processo per la gestione del ciclo di vita delle banche dati al verificarsi di eventi interni (come l'aggiornamento di piani strategici o modifiche organizzative), eventi esterni (come l'evoluzione del conteso normativo e legislativo) o mutamenti dell'esposizione alle minacce e ai relativi rischi.
3. Eseguire, con periodicità connessa al rischio, test di penetrazione sui sistemi, quale complemento alle attività di gestione delle vulnerabilità e verifica dei controlli di sicurezza in essere.
4. Adottare formalmente procedure per la dismissione sicura dei dispositivi di memorizzazione impiegati per la gestione dei dati (es. cancellazione sicura dei dati e/o delle chiavi di cifratura), nonché per il loro smaltimento.
5. Al fine di preservare l'efficacia dei controlli di sicurezza dei sistemi, garantire un ciclo di gestione delle vulnerabilità commisurato al rischio, anche in relazione alle librerie di terze parti eventualmente utilizzate (*Software Component Analysis*).

4.4. Gestione dei rischi e sicurezza della catena di approvvigionamento

Misure di sicurezza di riferimento: ID.SC-1, ID.SC-2, ID.SC-3, ID.SC-4, PR.IP-11

I fornitori e le terze parti, specie se poco maturi dal punto di vista della cybersicurezza, possono rappresentare un punto di vulnerabilità ed esporre i sistemi e le banche dati della propria organizzazione a rischi di attacco ed esfiltrazione di dati. I fornitori e le terze parti stessi possono rappresentare un vettore di attacco qualora compromessi da soggetti malintenzionati.

Per tale motivo è fondamentale integrare nel proprio processo di gestione del rischio cyber la gestione dei rischi connessi alla catena di approvvigionamento, valutando a tal scopo per ogni fornitore e per ogni fornitura i connessi rischi.

Con riferimento alle forniture di beni, sistemi e servizi ICT devono essere adottate misure di sicurezza specifiche per garantire la diversificazione dei fornitori e la possibilità di ricorrere ad altro fornitore, prevedendo a tal fine una seconda linea in caso di caduta della fornitura primaria.

L'affidabilità dei fornitori e delle terze parti deve essere valutata prima di concludere un contratto con gli stessi, anche al fine di verificare l'applicazione da parte degli stessi di pratiche di sicurezza adeguate. In ogni caso i contratti, gli accordi e le convenzioni stipulate con i fornitori e con le terze parti devono definire i requisiti in termini di sicurezza che gli stessi devono applicare nel contesto della fornitura. Le misure di sicurezza adottate dai fornitori e dalle terze parti devono essere tali da minimizzare i rischi cyber connessi alla fornitura e, comunque, coerenti con quelle applicate internamente dall'organizzazione.

È necessario mantenere un inventario aggiornato dei fornitori esterni e delle terze parti, nonché delle relative forniture. I fornitori devono essere classificati in base ai rischi cyber connessi alle forniture.

I fornitori e le terze parti devono essere sottoposti a verifiche e audit periodici. A tale scopo deve essere redatto e mantenuto aggiornato un documento che definisce le modalità e la cadenza delle valutazioni e degli audit dei fornitori e delle terze parti, proporzionate agli esiti dell'analisi del rischio. In accordo a tale

documento viene effettuata una pianificazione e viene mantenuto un registro delle verifiche e degli audit effettuati e della relativa documentazione.

Raccomandazioni di contesto

1. Registrare e monitorare tutte le attività dei fornitori e delle terze parti sui sistemi e sulle banche dati dell'organizzazione.
2. I fornitori e le terze parti devono poter accedere esclusivamente ai sistemi e ai dati cui hanno la necessità di accedere nell'ambito della fornitura, così come definito dai contratti, gli accordi o le convenzioni stipulate. Il relativo personale è identificato, registrato e formalmente autorizzato, prevedendo anche la stipula di accordi di riservatezza.
3. A seguito della cessazione di una fornitura revocare tempestivamente le eventuali utenze e le relative credenziali di accesso ai sistemi e ai dati dell'organizzazione.
4. Adottare, sia in relazione al personale interno che ad eventuali fornitori esterni con accesso privilegiato all'infrastruttura o ai dati dell'organizzazione, l'adozione di procedure per la verifica dell'affidabilità del personale (*vetting process methodology*), sia prima dell'incarico[5] che durante l'effettivo esercizio dei privilegi[6].

4.5. Monitoraggio e auditing

Misure di sicurezza di riferimento: ID.AM-3, PR.AC-7, PR.PT-1, PR.PT-4, DE.AE-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.DP-1

L'adozione di processi e strumenti per monitoraggio e l'auditing è un elemento imprescindibile per la difesa e il contrasto delle minacce alla sicurezza dei sistemi e delle applicazioni.

Deve essere conservato e mantenuto aggiornato un inventario relativo ai flussi informativi approvati. Un flusso informativo è un insieme di dati scambiati in una rete tra una sorgente e un destinatario. Possono essere rappresentati tramite le connessioni, in ingresso o in uscita, e i protocolli tramite i quali avvengono le comunicazioni[7].

Il citato inventario dei flussi informativi approvati deve contenere almeno le seguenti informazioni, se disponibili e presenti: sorgente del flusso, destinatario del flusso, protocolli e servizi di rete abilitati sul flusso, nominativo responsabile gestione, nominativo responsabile per l'autorizzazione alla comunicazione, esito e data del processo di autorizzazione. Deve essere, inoltre, predisposto un processo

[5] Ad esempio, tramite la verifica degli elementi storici a supporto dell'affidabilità del personale, anche in relazione alle precedenti attività svolte in analoghi contesti, oltre ad un necessario approfondito controllo dell'identità.

[6] Procedure di audit rafforzate volte a verificare l'effettiva coerenza tra le azioni compiute e l'incaricato affidato.

[7] Ad esempio, il flusso informativo conseguente alla navigazione Internet è una connessione in uscita su protocollo HTTPS, mentre il flusso informativo conseguente alla ricezione di mail è un flusso informativo in ingresso su protocollo SMTP.

che descriva nel dettaglio le attività previste nell'ambito della gestione dei flussi informativi (a titolo esemplificativo, invio della richiesta di apertura di un nuovo flusso informativo/chiusura di un flusso informativo approvato, approvazione/rigetto della richiesta, aggiornamento dell'inventario dei flussi informativi) e dei connessi ruoli e responsabilità.

Il monitoraggio deve inoltre rilevare la presenza di personale a seguito di accesso fisico o remoto non autorizzato alle risorse (prevedendo sistemi di sorveglianza e controllo di accesso, anche automatizzati), di dispositivi (anche fisici) non approvati (contemplando, salvi documentati limiti tecnici, almeno dei sistemi di controllo di accesso di rete), di software non autorizzato (prevedendo sistemi di controllo per il rilevamento dei software non approvati), di connessioni e flussi informativi dei sistemi e delle applicazioni (anche attraverso sistemi di controllo per il rilevamento delle connessioni non autorizzate).

Deve essere, altresì, previsto un documento recante almeno le politiche di sicurezza adottate per la gestione dei log esistenti, nonché i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza con particolare riguardo all'integrità e alla disponibilità dei log, i quali dovranno essere conservati in modo sicuro, possibilmente centralizzato, per almeno 24 mesi.

Ai fini di rilevare tempestivamente incidenti, è richiesto di dotarsi di strumenti tecnici e procedurali per acquisire le informazioni da più sensori e sorgenti, ottenere tempestivamente eventi occorsi a carico di dipendenze interne o esterne che potrebbero avere impatti sui beni dell'organizzazione, nonché ricevere e raccogliere informazioni inerenti alla sicurezza dei propri asset rese note dal CSIRT Italia, da fonti interne o esterne al soggetto. Sulla scorta delle peculiarità del sistema di gestione o della banca dati, è necessario, sin dalle prime fasi di progettazione ovvero in fase evolutiva qualora già operativi, valutare gli strumenti per il monitoraggio delle attività applicative (eventi) prodotte dalle azioni dei relativi utenti, al fine di predisporre, in maniera granulare ed evolvibile nel tempo, le opportune segnalazioni relative a potenziali comportamenti anomali. Tutti i dati e le informazioni acquisiti devono essere analizzati e correlati per rilevare tempestivamente eventi di interesse e le connesse attività di analisi e correlazione devono essere monitorate e registrate, conservandone la documentazione per almeno 24 mesi. L'organizzazione deve altresì predisporre un documento di dettaglio, da tenere aggiornato, che indichi almeno le politiche applicate per individuare i sensori e le sorgenti, le procedure e gli strumenti tecnici per ottenere le informazioni di cui sopra, le politiche, i processi e gli strumenti tecnici per l'analisi e la correlazione di dati e informazioni e i processi e gli strumenti tecnici per il monitoraggio e la registrazione delle attività di analisi e correlazione.

Devono essere previsti sistemi di rilevamento delle intrusioni (*intrusion detection systems* - IDS) e strumenti per monitorare e correlare tra loro – al fine di identificare eventi di cybersecurity – il traffico in ingresso e uscita, le attività dei sistemi perimetrali (ad esempio, router e firewall), gli eventi amministrativi di rilievo, nonché gli accessi eseguiti o falliti alle risorse di rete e alle postazioni terminali.

Tali strumenti tecnici devono essere aggiornati, mantenuti e ben configurati nel rispetto delle politiche di gestione delle identità, autenticazione e controllo degli accessi, protezione delle informazioni e manutenzione. Deve inoltre essere predisposto un documento aggiornato che descriva almeno le politiche di sicurezza adottate per gli strumenti di cui sopra e i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

Deve essere, inoltre, redatto un documento aggiornato di dettaglio che indichi almeno il personale incaricato, i ruoli, i processi e le responsabilità per le attività propedeutiche al rilevamento di incidenti e la successiva notifica al CSIRT Italia e descriva altresì i processi per la diffusione di tali nomine, ruoli, processi e responsabilità.

Le attività del personale sui sistemi e sulle banche dati devono essere monitorate e sottoposte ad audit periodici con cadenza proporzionata agli esiti dell'analisi del rischio.

Con riferimento alle attività di monitoraggio, devono essere definiti i criteri quantitativi e qualitativi per rilevare casi di utilizzo improprio delle banche dati da parte del personale. A titolo indicativo e non esaustivo, sono riportati di seguito alcuni esempi di tali criteri:

- consultazione di profili sensibili o comunque rilevanti ai fini della tutela della sicurezza nazionale, quali ad esempio i dati di personalità politicamente esposte;
- superamento di una soglia per le interrogazioni da parte di un singolo utente (definita dai rispettivi dirigenti/responsabili);
- variazione sensibile del numero medio di ricerche effettuate da un utente calcolato su un arco temporale definito;
- ricerche effettuate da personale che non ricopre posizioni di impiego tali da necessitare determinate informazioni;
- ricerche effettuate da postazioni di lavoro non comunemente utilizzate dal dipendente o geograficamente non congruenti con la normale posizione di impiego del dipendente;
- inserimento nelle motivazioni della richiesta (es. Nr. Protocollo/pratica/fascicolo) di valori non congruenti con le attività in corso da parte del dipendente.

Con riferimento alle attività di auditing, l'organizzazione deve:

- avvalersi di personale esterno solo qualora, sulla base degli esiti di una valutazione del rischio che consideri anche la sensibilità delle informazioni trattate, il livello di rischio stimato sia considerato accettabile;
- stilare, almeno annualmente, un programma di audit che comprenda elementi minimi quali gli obiettivi del programma di audit, i rischi e le opportunità ad esso associati e le azioni per affrontarli, il campo di applicazione (estensione, confini, siti) di ciascun audit previsto, la programmazione (numero/durata/frequenza) degli audit, i tipi di audit (interni o esterni), i criteri dell'audit, i metodi di audit da impiegare, i criteri per selezionare i membri del gruppo di audit e le informazioni documentate pertinenti;
- disporre di un'apposita struttura interna dedicata allo svolgimento delle attività di audit;
- collocare la suddetta struttura interna alle dipendenze dell'Alta Direzione (a titolo esemplificativo, Presidente, Direttore Generale, Collegio Sindacale) al fine di ridurre al minimo possibili indebite pressioni da parte di altre strutture interne e garantire l'indipendenza funzionale del personale incaricato delle attività di audit;

- limitare l'attribuzione di ulteriori incarichi al di fuori di quelli previsti dal proprio ruolo, in modo da ridurre gli ambiti sui quali l'auditor non potrà svolgere la propria attività di auditor e da non rischiare di comprometterne imparzialità e indipendenza;
- garantire adeguate risorse alla funzione di audit al fine di promuovere un sufficiente grado di indipendenza;
- affidare le attività di audit a personale di comprovata integrità, riservatezza e imparzialità che non si trovi in una situazione di conflitto di interesse, anche solo potenziale;
- assicurare che gli auditor dispongano di adeguata competenza e professionalità nell'ambito oggetto di audit;
- garantire un opportuno livello di formazione agli auditor, individuando i fabbisogni formativi e predisponendo la necessaria programmazione;
- evitare, ove possibile, che il gruppo di audit abbia ad oggetto attività nell'ambito delle quali abbia anche solo contribuito da un punto di vista operativo al fine di evitare che il controllore e il controllato coincidano.

Raccomandazioni di contesto

1. Adottare strumenti per la sicurezza e il monitoraggio dei flussi di rete (*firewall, IPS, IDS*), al fine di mitigare il rischio di intrusioni.
2. Adottare strumenti per la sicurezza e il monitoraggio dei dispositivi di accesso ai sistemi, anche al fine di mitigare il rischio di furto di sessione presso i sistemi e le banche dati in uso.
3. Prevedere uno strumento automatico per l'aggiornamento degli inventari.
4. Prevedere l'utilizzo di un sistema di ticketing per il tracciamento delle attività previste nell'ambito della gestione degli asset censiti (ad esempio, richieste di approvazione, attribuzione delle responsabilità agli utenti coinvolti).
5. Impiegare un sistema centralizzato dei log che ne possa garantire, anche attraverso il backup dei log raccolti, l'integrità e la disponibilità.
6. Prevedere l'impiego di un *SIEM* (*Security information and event management*) per rilevare eventi connessi a potenziali minacce, sia accidentali che intenzionali.

4.6. Formazione del personale

Misure di sicurezza di riferimento: PR.AT-1, PR.AT-2

La formazione del personale e in particolare degli utenti con privilegi (come, ad esempio, gli Amministratori di sistema) è una pre-condizione essenziale e necessaria per garantire resilienza, privacy, correttezza ed affidabilità dei sistemi e delle applicazioni.

A tale scopo devono essere previsti corsi di formazione per tutti gli utenti – compresi gli utenti con privilegi – predisponendo un registro che indichi i contenuti della formazione ricevuta dagli utenti e definendo modalità per la verifica dell'acquisizione dei contenuti stessi.

Tutto il personale deve essere sensibilizzato sul tema della cybersicurezza e sulla consapevolezza dei rischi informatici, nonché sull'adozione delle migliori pratiche di igiene informatica che devono sempre essere applicate sul posto di lavoro.

Raccomandazioni di contesto

1. Prevedere corsi dedicati in materia di cybersecurity agli utenti con privilegi dei sistemi e delle banche dati.
2. Definire modalità di verifica dei contenuti della formazione specifiche per le varie categorie di utenti con privilegi dei sistemi e delle banche dati (amministratori dei sistemi operativi, amministratori di database, utenti con privilegi sulle banche dati, utenti in grado di creare/cancellare e profilare altri utenti).
3. Formare il personale su come sviluppare, mantenere e proteggere banche dati.
4. Prevedere programmi di sensibilizzazione del personale con riguardo alla non divulgazione e alla riservatezza delle informazioni.

A. Elenco delle misure di sicurezza

CODICE	DESCRIZIONE
ID.AM-3	I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati
ID.SC-1	I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione
ID.SC-2	I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber
ID.SC-3	I contratti con i fornitori e i partner terzi sono utilizzati per realizzare appropriate misure progettate per rispettare gli obiettivi del programma di cybersecurity dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento cyber.
ID.SC-4	Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali.
PR.AC-1	Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza.
PR.AC-2	L'accesso fisico alle risorse è protetto e amministrato.
PR.AC-3	L'accesso remoto alle risorse è amministrato.
PR.AC-4	I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni.
PR.AC-5	L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete).
PR.AC-7	Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione).
PR.AT-1	Tutti gli utenti sono informati e addestrati.
PR.AT-2	Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità.
PR.DS-1	I dati e le informazioni memorizzate sono protetti.
PR.DS-3	Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale.
PR.DS-7	Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione.
PR.IP-1	Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità).

PR.IP-2	Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle).
PR.IP-3	Sono attivi processi di controllo della modifica delle configurazioni.
PR.IP-4	I backup delle informazioni sono eseguiti, amministrati e verificati periodicamente
PR.IP-11	Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale.
PR.IP-12	Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle).
PR.MA-1	La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati.
PR.MA-2	La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati.
PR.PT-1	Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi.
PR.PT-4	Le reti di comunicazione e controllo sono protette.
DE.AE-3	Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple.
DE.CM-1	Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity.
DE.CM-4	Il codice malevolo viene rilevato.
DE.CM-7	Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati.
DE.CM-8	Vengono svolte scansioni per l'identificazione di vulnerabilità.
DE.DP-1	Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability.