Controlli di sicurezza

Allegato B alla

POLITICA DELLA SICUREZZA DEI SISTEMI INFORMATICI DELLA GIUSTIZIA (art. 15, Allegato ex art. 1 del DM 27-4-2009)

Controlli di sicurezza
Parte I – Livello M0

Function	Category	Subcategory	Priorità	POLICY	POLICY PER CONTROLLO	Livello M0	RUOLO	CONTESTO	RIFERIMENTI NORMATIVI
IDENTIFY (ID)	**Asset Management (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi di business e con la strategia di rischio dell'organizzazione**	**ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione**	Critica	**PLC-001; PLC-062**	**PLC-001; PLC-062**	**CTR-M0-ID.AM-1-01** (ABSC 1.1.1): Tutti i sistemi e gli apparati fisici in uso (dispositivi connessi alla rete a cui è associato un indirizzo IP) vengono catalogati.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 1.1.1) DM 27.4.2009
					PLC-001; PLC-062	**CTR-M0-ID.AM-1-02** (ABSC 1.1.1): Per i sistemi e gli apparati fisici in uso (risorse attive comprese di IP) catalogati si tiene traccia delle loro configurazioni attuali (versioni del software/firmware).	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 1.1.1)
					PLC-001	**CTR-M0-ID.AM-1-03** (ABSC 1.1.1): Per i sistemi e gli apparati fisici in uso (risorse attive comprese di IP) catalogati si tiene traccia dei rispettivi cambiamenti storici nella configurazione.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 1.1.1)
					PLC-001	**CTR-M0-ID.AM-1-04** (ABSC 1.3.1): L'inventario viene aggiornato quando nuovi dispositivi approvati vengono collegati in rete.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 1.3.1) DM 27.4.2009
					PLC-001	**CTR-M0-ID.AM-1-05** (ABSC 1.4.1): L'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi viene gestito registrando almeno indirizzo IP.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 1.4.1)

		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	**Critica**	**PLC-002; PLC-003; PLC-004; PLC-062; PLC-080**	**PLC-002; PLC-062**	**CTR-M0-ID.AM-2-01** (ABSC 2.1.1): Esiste un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema (PC, laptop, workstation, server ...).	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 2.1.1) DM 27.4.2009
					PLC-002	**CTR-M0-ID.AM-2-02** (ABSC 2.1.1): Non viene consentita l'installazione di software non compreso nell'elenco di cui al controllo precedente (**CTR-M0-ID.AM-2-01**).	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 2.1.1)
					PLC-002; PLC-080	**CTR-M0-ID.AM-2-03** (ABSC 2.3.1): Vengono eseguite regolari scansioni sui sistemi (PC, laptop, workstation, server) al fine di rilevare la presenza di software non autorizzato (cioè non nell'elenco individuato al controllo di cui **CTR-M0-ID.AM-2-01**).	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 2.3.1)
					PLC-003	**CTR-M0-ID.AM-2-04** (DPCM 1/4/2008): Esiste un elenco di applicativi e strumenti di video-conferenza accessibili dalle singole postazioni di lavoro (PdL) o da apposite postazioni condivise per la comunicazione e la collaborazione in tempo reale ed in modalità interattiva fra diversi utenti dislocati remotamente in altre PPAA.			CAD DPCM 1/4/2008

					PLC-004	**CTR-M0-ID.AM-2-05** (DPCM 1/4/2008): Esiste un elenco delle applicazioni telematiche multicanale che favoriscono la comunicazione asincrona con altre PPAA e con cittadini ed imprese.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	CAD DPCM 1/4/2008
		ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati.	**Critica**	**PLC-005; PLC-006; PLC-062; PLC-072**	**PLC-005**	**CTR-M0-ID.AM-3-01** (DPCM 1/4/2008): I servizi applicativi, di ambito SPC, offerti dall'ufficio giudiziario e i relativi Accordi di Servizio e di Cooperazione vengono pubblicati mediante i Servizi Infrastrutturali di Cooperazione Applicativa (SICA) nel Registro SICA.	DGSIA	Uffici centrali DGSIA	CAD DPCM 1/4/2008
					PLC-005	**CTR-M0-ID.AM-3-02** (DPCM 1/4/2008): Esiste un elenco degli indirizzi di posta elettronica utilizzati per lo scambio di semplici email, email firmate o email cifrate verso altre PPAA.	DGSIA	Uffici centrali DGSIA	CAD DPCM 1/4/2008
					PLC-005	**CTR-M0-ID.AM-3-03** (DPCM 1/4/2008): Esiste un elenco degli indirizzi di posta elettronica certificata (con riferimento al registro iPA) utilizzati per lo scambio di email certificate verso altre PPAA.	DGSIA	Uffici centrali DGSIA	CAD DPCM 1/4/2008

		ID.AM-4: I sistemi informativi esterni all'organizzazione sono catalogati	**Critica**	**PLC-005; PLC-007; PLC-072**	**PLC-005**	**CTR-M0-ID.AM-4-01** (DPCM 1/4/2008): I servizi applicativi, di ambito SCP, offerti da altre PPAA e utilizzati dall'ufficio giudiziario per espletare i propri compiti istituzionali devono essere pubblicati nel Registro SICA.	DGSIA	Uffici centrali DGSIA	CAD DPCM 1/4/2008
		ID.AM-5: Le risorse (es: hardware, dispositivi, dati e software) sono prioritizzati in base alla loro classificazione (e.g. confidenzialità,	**Critica**	**PLC-008; PLC-009; PLC-010; PLC-011; PLC-012; PLC-036**	**PLC-008; PLC-009**	**CTR-M0-ID.AM-5-01** (ABSC 13.1.1): Viene effettuata un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica.	DGSIA	Uffici centrali DGSIA	AgID (ABSC 13.1.1) GDPR

		integrità, disponibilità), criticità e valore per il business dell'organizzazione		**PLC-008; PLC-009**	**CTR-M0-ID.AM-5-02**: La prioritizzazione delle risorse dell'ufficio giudiziario tiene conto della classificazione dei dati, delle informazioni e dei documenti informatici secondo il sistema di classificazione previsto per la Direzione Nazionale Antimafia e Antiterrorismo, organizzato su 5 livelli e il DPCM n.5/2015 che rende la classificazione delle informazioni conforme agli standard internazionali (di seguito i livelli): **livello 1.** *Divulgabile*: dato/informazione/documento può essere distribuito a chiunque e pubblicato su mezzi che ne consentono la divulgazione, quali i siti Internet istituzionali; **livello 2.** *Pubblico* (riservato): dato/informazione/documento può essere fornito a chiunque ne faccia richiesta avendone titolo, previa identificazione del soggetto richiedente; **livello 3.** *Circolazione limitata* (riservatissimo): dato/informazione/documento può essere distribuito solo a soggetti facenti parte di specifici ambiti che devono essere chiaramente indicati nel documento stesso; un ambito	DGSIA	Tutti gli UUGG e Data Center	

					può corrispondere ad una determinata organizzazione (ad es. una Direzione o una Società) o a più organizzazioni accomunate da una particolare caratteristica (ad es. direzioni tecniche); **livello 4.** *Circolazione ristretta* (segreto): dato/informazione/documento può essere distribuito solo a specifici uffici o a specifiche persone che devono essere chiaramente indicati nel documento stesso; **livello 5.** *Altamente riservato* (segretissimo): dato/informazione/documento può essere reso ostensibile solo a specifiche persone che devono essere chiaramente indicate nel documento stesso.			

		ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	Alta	PLC-106; PLC-107; PLC-108		
	Business Environment (ID.BE): La mission dell'organizzazione, gli obiettivi, le attività e gli attori coinvolti sono	ID.BE-1:Il ruolo dell'organizzazione all'interno della filiera produttiva è identificato e reso noto	Non selezionata			

	compresi e valutate in termini di priorità. Tali informazioni influenzano i ruoli, le responsabilità di cybersecurity e le decisioni in materia di gestione del rischio.	ID.BE-2: Il ruolo dell'organizzazione come infrastruttura critica e nel settore industriale di riferimento è identificato e reso noto	Non selezionata			
		ID.BE-3: Sono definite e rese note delle priorità per quanto riguarda la missione, gli obiettivi e le attività dell'organizzazione.	Non selezionata			
		ID.BE-4: Sono identificate e rese note interdipendenze e funzioni fondamentali per la fornitura di servizi critici	Non selezionata			

		ID.BE-5: Sono identificati e resi noti i requisiti di resilienza a supporto della fornitura di servizi critici	**Alta**	**PLC-109; PLC-122**					
	Governance (ID.GV): Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-1: E' indetificata e resa nota una policy di sicurezza delle informazioni**	**Critica**	**PLC-110; PLC-111; PLC-112; PLC-113; PLC-114; PLC-115**	**PLC-110; PLC-111**	**CTR-M0-ID.GV-1-01**: Il trattamento del dato e delle informazioni è coerente con il D.Lgs. 196/2003 relativamente al trattamento di dati giudiziari.	DGSIA	Uffici centrali DGSIA	D.Lgs 196/2003
					PLC-112	**CTR-M0-ID.GV-1-02** (DPCM 3/12/2013): Esiste un responsabile della conservazione delle informazioni/dati/documenti dell'ufficio giudiziario.	DGSIA/CISIA	Tutti gli UUGG e Data Center	CAD DPCM 3/12/2013
					PLC-113	**CTR-M0-ID.GV-1-03** (DPCM 3/12/2013): Il Piano della Sicurezza include il piano della sicurezza del sistema di conservazione (rif. art.12 DPCM 3/12/2013).	DGSIA	Tutti gli UUGG e Data Center	CAD DPCM 3/12/2013

					PLC-115	**CTR-M0-ID.GV-1-04:** È stata effettuata la compilazione del "MODULO DI IMPLEMENTAZIONE DELLE MISURE MINIME DI SICUREZZA PER LE PUBBLICHE AMMINISTRAZIONI", allegato 2 GU n.79 del 4-4-2017 (obbligatoria entro il 31/12/2017, firmata digitalmente con Marca Temporale)	DGSIA/CISIA	Tutti gli UUGG e Data Center	AgID Circ. n. 2/2017
					PLC-114	**CTR-M0-ID.GV-1-05** (DPCM 3/12/2013): Esiste un processo di conservazione dei documenti informatici conforme al DPCM 3/12/2013 in materia di conservazione dei documenti informatici.	DGSIA/CISIA	Tutti gli UUGG e Data Center	CAD DPCM 3/12/2013
		ID.GV-2: Ruoli e responsabilità inerenti la sicurezza delle informazioni sono coordinati ed allineati con i ruoli interni ed i partner esterni	**Alta**	**PLC-116**					

		ID.GV-3: I requisiti legali in materia di cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti	**Alta**	**PLC-110; PLC-117**		
		ID.GV-4: La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity				
	Risk Assessment (ID.RA): L'impresa comprende il rischio di cybersecurity inerente l' operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-1: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate**	**Alta**	**PLC-118; PLC-119; PLC-122**		

		ID.RA-2: L'organizzazione riceve informazioni su minacce e vulnerabilità da fonti esterne (e.g. CERT, fonti aperte, forum di information sharing)	Critica	PLC-120		
		ID.RA-3: Le minacce, sia interne che esterne, sono identificate e documentate	Alta	PLC-120		

	ID.RA-4: Sono identificati i potenziali impatti sul business e le relative probabilità di accadimento	**Alta**	**PLC-121; PLC-122**					
	ID.RA-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio	**Critica**	**PLC-122**	**PLC-122**	**CTR-M0-ID.RA-5-01** (ABSC 4.8.1): Esiste un piano di gestione dei rischi.	CISIA/Assistenza tecnica (esterna)	Sala Server Ufficio Giudiziario	AgID (ABSC 4.8.1)
				PLC-122	**CTR-M0-ID.RA-5-02** (ABSC 4.8.1): Il piano di gestione dei rischi di cui al controllo precedente (**CTR-M0-ID.RA-5-01**) tiene conto della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.)	CISIA/Assistenza tecnica (esterna)	Sala Server Ufficio Giudiziario	AgID (ABSC 4.8.1)
				PLC-122	**CTR-M0-ID.RA-5-03** (ABSC 4.8.1): Il piano di gestione dei rischi di cui al controllo **CTR-M0-ID.RA-5-01** tiene conto dei livelli di gravità delle vulnerabilità e del potenziale impatto.	CISIA/Assistenza tecnica (esterna)	Sala Server Ufficio Giudiziario	AgID (ABSC 4.8.1)
	ID.RA-6: Sono identificate e prioritizzate le risposte al rischio	**Media**	**PLC-123; PLC-124**					

	Risk Management Strategy (ID.RM): Le priorità e i requisiti dell'organizzazione e la tolleranza al rischio sono definiti e utilizzati per supportare le decisioni sul rischio operazionale.	ID.RM-1: I processi di risk management sono stabiliti, gestiti e concordati tra i responsabili dell'organizzazione (c.d. stakeholder)	Alta	PLC-123; PLC-129		
		ID.RM-2: Il rischio tollerato dall'organizzazione è identificato ed espresso chiaramente	Non selezionata			
		ID.RM-3: Il rischio tollerato è determinato tenendo conto del ruolo dell'organizzazione come infrastruttura critica e dei rischi specifici presenti nel settore industriale di appartenenza	Non selezionata			

	Supply Chain Risk Management (ID.SC): Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione vengono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio della fornitura Cyber. L'organizzazione ha in essere i processi per identificare, valutare e gestire i rischi della catena di approvvigionamento dei sistemi e dei servizi informatici.	ID.SC-1: I processi di gestione del rischio inerenti la catena della fornitura Cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione	Alta	PLC-124; PLC-130		
		ID.SC-2: Identificare, prioritizzare e valutare i fornitori e i partner di sistemi informatici, componenti e servizi critici, utilizzando un processo di valutazione del rischio inerente la fornitura Cyber	Media	PLC-124		
		ID.SC-3: Fornitori e partner sono tenuti per contratto ad attuare misure appropriate volte a conseguire gli obiettivi del programma di sicurezza delle informazioni o Piano di gestione	Alta	PLC-125; PLC-128		

		del rischio della catena di fornitura Cyber				
		ID.SC-4: Fornitori e partner sono monitorati per verificare che essi adempiano ai loro obblighi, come richiesto. Revisione degli audit, sintesi dei risultati dei test o di altre valutazioni equivalenti dei fornitori sono condotte.	**Alta**	**PLC-126; PLC-128; PLC-063**		
		ID.SC-5: La pianificazione e la verifica della risposta e del ripristino sono condotti con i fornitori critici	**Alta**	**PLC-122; PLC-127**		

PROTECT (PR)	**Access Control (PR.AC): L'accesso agli asset ed alle relative risorse è limitato al personale, ai processi, ai dispositivi, alle attività ed alle transazioni effettivamente autorizzate**	**PR.AC-1: Le identità digitali e le credenziali di accesso per gli utenti e per i dispositivi autorizzati sono amministrate**	**Critica**	**PLC-017; PLC-018; PLC-019; PLC-020; PLC-021; PLC-023; PLC-024; PLC-025; PLC-026; PLC-047**	**PLC-017; PLC-018; PLC-047**	**CTR-M0-PR.AC-1-01** (ABSC 5.7.1, 5.7.2): Si utilizzano, per le utenze amministrative, credenziali di elevata robustezza (cioè, almeno 14 caratteri) qualora l'autenticazione a più fattori non è supportata per tali categorie di utenze.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	AgID (ABSC 5.7.1, 5.7.2)
					PLC-017; PLC-018	**CTR-M0-PR.AC-1-02** (ABSC 5.7.3): Le credenziali delle utenze amministrative vengono sostituite con sufficiente frequenza (password aging).	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	AgID (ABSC 5.7.3)
					PLC-017; PLC-018	**CTR-M0-PR.AC-1-03** (ABSC 5.7.4): Si impedisce che credenziali già utilizzate vengano riutilizzate a breve distanza di tempo (password history).	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	AgID (ABSC 5.7.4)
					PLC-017; PLC-018	**CTR-M0-PR.AC-1-04** (ABSC 5.11.1): Le credenziali amministrative vengono conservate e gestite con modalità che ne garantiscono disponibilità e riservatezza.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	AgID (ABSC 5.11.1) D.Lgs. 196/2003 GDPR
					PLC-025	**CTR-M0-PR.AC-1-05**(ABSC 5.11.2): Se per l'autenticazione si utilizzano certificati digitali, le chiavi private vengono adeguatamente protette.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	AgID (ABSC 5.11.2) D.Lgs. 196/2003 GDPR

PLC-023	**CTR-M0-PR.AC-1-06** (CAD Art. 64): Esiste un sistema di gestione delle identità digitali per gli utenti esterni integrato con il Sistema Pubblico per la gestione delle Identità Digitali (SPID), per l'accesso ai servizi telematici offerti dall'ufficio giudiziario.	DGSIA	Ufficio Infrastrutture e reti	CAD
PLC-019	**CTR-M0-PR.AC-1-07** (ABSC 5.2.1): Viene mantenuto l'inventario delle utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	AgID (ABSC 5.2.1) DM 27.4.2009
PLC-020	**CTR-M0-PR.AC-1-08** (196/2003): Le credenziali di autenticazione per gli utenti che hanno accesso a dati personali consistono in un identificativo e una password riservata (conosciuta solamente dall'utente), oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'utente (es. smart card), oppure in una caratteristica biometrica dell'utente.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	D.Lgs. 196/2003
PLC-020	**CTR-M0-PR.AC-1-09** (196/2003): Per le utenze che possono trattare dati personali, la password (se prevista dal sistema di autenticazione) è composta da almeno otto caratteri, oppure, se lo strumento elettronico non lo permette, da un numero di caratteri pari al massimo	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	D.Lgs. 196/2003

	consentito.			
PLC-024	**CTR-M0-PR.AC-1-10** (196/2003): Se la creazione di una nuova utenza comporta l'assegnazione automatica di una password da parte del sistema, la password non contiene riferimenti riconducibili all'utente ed inoltre la modifica della stessa è imposta all'utente contestualmente alla prima autenticazione.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	D.Lgs. 196/2003
PLC-020	**CTR-M0-PR.AC-1-11** (196/2003): Agli utenti che possono trattare dati personali è imposto di cambiare password almeno ogni 6 mesi. Almeno ogni 3 mesi nel caso il trattamento riguardi dati sensibili o giudiziari.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	D.Lgs. 196/2003
PLC-021	**CTR-M0-PR.AC-1-12** (196/2003): Per le utenze che possono trattare dati personali, lo stesso codice identificativo usato per l'autenticazione (es. login name, nickname, etc.) non viene mai assegnato a due utenti diversi, nemmeno in tempi diversi.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	D.Lgs. 196/2003

PLC-019; PLC-021	**CTR-M0-PR.AC-1-13** (196/2003): Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	D.Lgs. 196/2003
PLC-024	**CTR-M0-PR.AC-1-14** (196/2003): Se un utente perde il ruolo che gli consente l'accesso ai dati personali le relative credenziali vengono disattivate.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	D.Lgs. 196/2003
PLC-024	**CTR-M0-PR.AC-1-15** (196/2003): I profili di autorizzazione degli utenti sono gestiti tramite un sistema o uno strumento automatico.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	D.Lgs. 196/2003
PLC-021	**CTR-M0-PR.AC-1-16** (196/2003): In caso di prolungata assenza o impedimento dell'incaricato del trattamento di dati personali, sono impartite idonee e preventive disposizioni scritte volte ad individuare le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	D.Lgs. 196/2003
PLC-021	**CTR-M0-PR.AC-1-17** (196/2003): Nel caso di cui al controllo precedente, la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	D.Lgs. 196/2003

					PLC-021	**CTR-M0-PR.AC-1-18** (196/2003): I soggetti incaricari della custodia delle copie delle credenziali informano tempestivamente l'incaricato dopo ogni intervento effettuato con le sue credenziali.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	D.Lgs. 196/2003
		PR.AC-2: L'accesso fisico alle risorse è protetto e amministrato	**Alta**	**PLC-013; PLC-014; PLC-015; PLC-016**					

		PR.AC-3: L'accesso remoto alle risorse è amministrato	**Critica**	**PLC-031; PLC-055; PLC-056**	**PLC-031; PLC-055; PLC-056**	**CTR-M0-PR.AC-3-01** (ABSC 3.4.1): Tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature si eseguono per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	AgID (ABSC 3.4.1)
		PR.AC-4: Gli accessi alle risorse sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	**Critica**	**PLC-027; PLC-028; PLC-029; PLC-030**	**PLC-027**	**CTR-M0-PR.AC-4-01** (ABSC 5.1.2): Le utenze amministrative vengono utilizzate solo per effettuare operazioni che ne richiedano i privilegi.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	AgID (ABSC 5.1.2)
					PLC-029	**CTR-M0-PR.AC-4-02** (ABSC 5.1.2): Vengono registrati tutti gli accessi effettuati dalle utenze amministrative.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	AgID (ABSC 5.1.2)
					PLC-030	**CTR-M0-PR.AC-4-03** (196/2003): Relativamente al trattamento di dati personali, le credenziali di autenticazione assegnate ad un utente gli garantiscono accesso esclusivamente ad un trattamento o un insieme di trattamenti di dati personali, in coerenza con il suo profilo di autorizzazione.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	D.Lgs. 196/2003

					PLC-030	**CTR-M0-PR.AC-4-04** (196/2003): Relativamente al trattamento di dati personali, i profili di autorizzazione, per ciascun incaricato (singolo utente) o per classi di incaricati (es. ruoli), sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	D.Lgs. 196/2003
					PLC-030	**CTR-M0-PR.AC-4-05** (196/2003): Relativamente al trattamento di dati personali, periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	D.Lgs. 196/2003
					PLC-027	**CTR-M0-PR.AC-4-06** (ABSC 5.1.1): Vengono attribuiti i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 5.1.1)
		PR.AC-5: L'integrità di rete è protetta, anche applicando la segregazione di rete dove appropriata	**Alta**	**PLC-032; PLC-033; PLC-034**					

		PR.AC-6: Le identità digitali sono comprovabili, associate a credenziali e, qualora richiesto, possono essere asserite durante le interazioni	**Critica**	**PLC-021; PLC-023; PLC-024; PLC-027; PLC-047**	**PLC-027**	**CTR-M0-PR.AC-6-01** (ABSC 5.10.3): Le utenze amministrative anonime (es. "root" su UNIX o "Administrator" su Windows) vengono utilizzate solo per le situazioni di emergenza e le relative credenziali devono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	AgID (ABSC 5.10.3)
					PLC-021	**CTR-M0-PR.AC-6-02** (196/2003): Relativamente al trattamento di dati personali, ad ogni incaricato del trattamento è associato un utente individuale con proprie credenziali di autenticazione. In altre parole non si utilizzano utenze condivise tra più incaricati.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	D.Lgs. 196/2003
					PLC-023	**CTR-M0-PR.AC-6-03** (CAD art. 64): Le identità digitali delle utenze esterne vengono comprovate mediante il sistema SPID.	DGSIA	Ufficio centrale Infrastrutture e reti	CAD (art. 64)
					PLC-023	**CTR-M0-PR.AC-6-04** (DPCM 01/04/2008): Esiste un sistema di gestione delle identità digitali predisposto per l'accesso ai servizi applicativi erogati dall'ufficio giudiziario.	DGSIA	Ufficio centrale Infrastrutture e reti	CAD DPCM 01/04/2008

				PLC-023	**CTR-M0-PR.AC-6-05** (DPCM 01/04/2008): Il sistema di gestione delle identità e degli accessi dell'ufficio giudiziario utilizzato in ambito SPC permette di gestire gli accessi a (lista esaustiva): 1. servizi che non richiedono alcuna identificazione o autenticazione; 2. servizi che richiedono l'autenticazione in rete da parte di un'autorità di autenticazione; 3. servizi che richiedono, per le persone fisiche, l'identificazione in rete da parte di un'autorità di identificazione; 4. servizi che richiedono per gli utenti, oltre all'identificazione, l'attestazione di attributi e/o ruoli, che ne qualifichino ulteriormente le funzioni e/o i poteri.	DGSIA	Uffici centrali DGSIA	CAD DPCM 01/04/2008
				PLC-023	**CTR-M0-PR.AC-6-06** (DPCM 01/04/2008): Il sistema d'identificazione per un servizio applicativo avviene mediante le modalità previste dal sistema SPID;	DGSIA	Uffici centrali DGSIA	CAD DPCM 01/04/2008

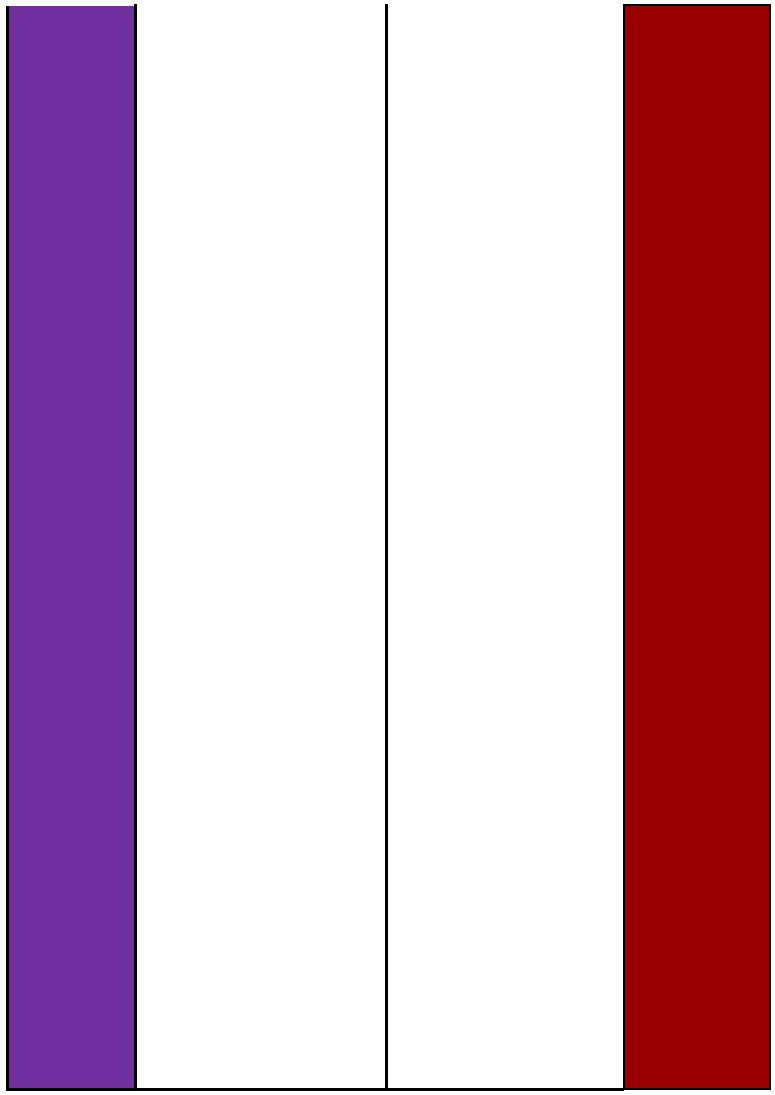
	Awareness and Training (PR.AT): Il personale e le terze sono sensibilizzate e formate in materia di cybersecurity e ricevono adeguata preparazione, coerente con le politiche, le procedure e gli accordi esistenti, per svolgere correttamente i compiti e le responsabilità legate alla sicurezza delle informazioni	**PR.AT-1: Tutti gli utenti sono informati e addestrati**	**Critica**	**PLC-021; PLC-022; PLC-026**	**PLC-021; PLC-022**	**CTR-M0-PR.AT-1-01** (196/2003): A tutto il personale che ha accesso e può trattare dati personali sono impartite istruzioni circa l'adottare le necessarie cautele per assicurare la segretezza delle credenziali di accesso e la diligente custodia dei dispositivi utilizzati per il trattamento.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	D.Lgs. 196/2003
					PLC-021; PLC-022	**CTR-M0-PR.AT-1-02** (196/2003): A tutto il personale che possiede credenziali di accesso a dati personali sono impartite istruzioni di non lasciare incustodito e accessibile lo strumento elettronico usato per il trattamento dei dati durante una sessione di trattamento.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	D.Lgs. 196/2003
		PR.AT-2: Gli utenti privilegiati (e.g. Amministratori di Sistema) comprendono ruoli e responsabilità	**Critica**	**PLC-019**	**PLC-019**	**CTR-M0-PR.AT-2-01** (ABSC 5.10.1): Viene assicurata la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali corrispondono credenziali diverse.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	AgID (ABSC 5.10.1)
					PLC-019	**CTR-M0-PR.AT-2-02** (ABSC 5.10.2): Le utenze amministrative sono nominative e riconducibili ad una sola persona.	CISIA/Assistenza tecnica (esterna)	Sala Server Uffici Giudiziari	AgID (ABSC 5.10.2)

		PR.AT-3: Tutte le terze parti (es. fornitori, clienti, partner) comprendono ruoli e responsabilità	**Critica**	**PLC-125**	**PLC-125**	**CTR-M0-PR.AT-3-01** (196/2003): Nel caso in cui per garantire le misure minime di sicurezza di cui all'allegato B del D. Lgs. 30 giugno 2003, n. 196, ci si avvale di soggetti esterni, viene ricevuta dal fornitore esterno una descrizione scritta degli interventi effettuati che ne attesta la conformità alle disposizioni del disciplinare tecnico di cui all'allegato B del D. Lgs. 30 giugno 2003, n. 196.	DGISIA	Uffici centrali DGSIA	D.Lgs. 196/2003
		PR.AT-4: I dirigenti ed i vertici aziendali comprendono ruoli e responsabilità	**Alta**	**PLC-116**					
		PR.AT-5: Il personale addetto alla sicurezza fisica e delle informazioni comprende i ruoli e le responsabilità	**Alta**	**PLC-116**					

	Data Security (PR.DS): I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1: I dati e le informazioni memorizzate sono protette**	**Alta**	**PLC-025; PLC-037; PLC-038; PLC-045**					
		PR.DS-2: I dati sono protetti durante la trasmissione	**Critica**	**PLC-066; PLC-067; PLC-068; PLC-086**	**PLC-066**	**CTR-M0-PR.DS-2-01** (DPCM 01/04/2008): Gli scambi dei dati/informazioini/documenti tra PPAA avvegono mediante porta di dominio o, alternativamente, con protocollo HTTPS.	DGSIA	Ufficio centrale Infrastruttura e reti	CAD DPCM 01/04/2008
					PLC-066	**CTR-M0-PR.DS-2-02** (DPCM 01/04/2008): Lo scambio di messaggi di posta elettronica crittografati e firmati digitalmente verso e da altre PPAA avviene sulla base dello standard MIME S/MIME.	DGSIA	Ufficio centrale Infrastruttura e reti	CAD DPCM 01/04/2008

					PLC-086	**CTR-M0-PR.DS-2-03** (DPCM 01/04/2008): Al fine di consentire il monitoraggio dei servizi SPC, esiste un sistema in grado di interfacciarsi al Centro di Gestione SPC (CG-SPC) o ad ogni altra componente preposta al monitoraggio o alla gestione di risorse condivise in ambito nazionale, per consentire lo scambio di dati relativi ai parametri di qualità dei servizi, di fault, di provisioning, di informazioni di configurazione o di ogni altra informazione rilevante per la misura degli indicatori di qualità e di sicurezza del servizio. Le modalità di invio di tali dati si basano su protocolli standard (mail, FTP, etc.), che includono meccanismi per la protezione di dati confidenziali (IPSEC, SSL, SSH).	DGSIA	Ufficio centrale Infrastruttura e reti	CAD DPCM 01/04/2008
		PR.DS-3:Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale	**Alta**	**PLC-060; PLC-073**					

		PR.DS-4: I sistemi hanno adeguate risorse a disposione per poter garantire la disponibilità	**Alta**	**PLC-059; PLC-087**				
		PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).	**Critica**	**PLC-024; PLC-030; PLC-036; PLC-037; PLC-039; PLC-040; PLC-045; PLC-046; PLC-048; PLC-069**	**PLC-030; PLC-046**	**CTR-M0-PR.DS-5-01** (196/2003): I dati personali, i dati sensibili o giudiziari sono protetti contro il rischio di accesso abusivo e compromissione mediante idonei strumenti automatici.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	D.Lgs. 196/2003
					PLC-024; PLC-046	**CTR-M0-PR.DS-5-02** (196/2003): Gli strumenti automatici di cui al controllo precedente (**CTR-M0-PR.DS-5-02**) sono aggiornati con cadenza almeno semestrale.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	D.Lgs. 196/2003
					PLC-069	**CTR-M0-PR.DS-5-03** (DPCM 03/12/2013): Il sistema di protocollo informatico dell'ufficio giudiziario assicura l'univoca identificazione ed autenticazione degli utenti e la protezione delle informazioni relative a ciascun utente nei confronti degli altri.	DGSIA	Ufficio giudiziario Sala Server	CAD DPCM 03/12/2013



PLC-069	**CTR-M0-PR.DS-5-04** (DPCM 03/12/2013): Il sistema di protocollo informatico dell'ufficio giudiziario assicura la garanzia di accesso alle risorse esclusivamente agli utenti abilitati.	DGSIA	Ufficio giudiziario Sala Server	CAD DPCM 03/12/2013
PLC-069	**CTR-M0-PR.DS-5-05** (DPCM 03/12/2013): Il sistema di protocollo informatico dell'ufficio giudiziario permette la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione.	DGSIA	Ufficio giudiziario Sala Server	CAD DPCM 03/12/2013
PLC-069	**CTR-M0-PR.DS-5-06** (DPCM 03/12/2013): Il sistema di protocollo informatico consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti.	DGSIA	Ufficio giudiziario Sala Server	CAD DPCM 03/12/2013
PLC-069	**CTR-M0-PR.DS-5-07** (DPCM 03/12/2013): Il sistema di protocollo informatico consente il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni vengono protette da modifiche non autorizzate.	DGSIA	Ufficio giudiziario Sala Server	CAD DPCM 03/12/2013

					PLC-069	**CTR-M0-PR.DS-5-08** (DPCM 03/12/2013): Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	CAD DPCM 03/12/2013
					PLC-069	**CTR-M0-PR.DS-5-09** (DPCM 03/12/2013): Il sistema di protocollo rispetta le misure di sicurezza previste dagli articoli da 31 a 36 e dal disciplinare tecnico di cui all'allegato B del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.	DGSIA	Ufficio giudiziario Sala Server	CAD DPCM 03/12/2013
		PR.DS-6: Vengono implementate tecniche di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni	**Critica**	**PLC-041; PLC-042; PLC-049; PLC-050; PLC-061; PLC-070; PLC-071; PLC-077**	**PLC-041; PLC-042; PLC-049; PLC-050; PLC-061**	**CTR-M0-PR.DS-6-01** (ABSC 10.3.1): È assicurata la riservatezza delle informazioni contenute nelle copie di sicurezza (backup) mediante adeguata protezione fisica dei supporti e/o mediante cifratura.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 10.3.1) DM 27.4.2009
					PLC-041; PLC-042; PLC-049; PLC-050; PLC-061	**CTR-M0-PR.DS-6-02** (ABSC 10.3.1): Nel caso i backup vengano remotizzati su piattaforme cloud, ne viene effettuata la cifratura prima della trasmissione.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 10.3.1) DM 27.4.2009

					PLC-070	**CTR-M0-PR.DS-6-03** (DM 2/11/2005): Il sistema di gestione delle PEC è conforme alle regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata.	DGSIA	Uffici centrali DGSIA	CAD DM 2/11/2005
					PLC-071	**CTR-M0-PR.DS-6-04** (DPCM 01/04/2008): Esiste un sistema di generazione di riferimenti temporali relativo ai messaggi (busta E-gov) scambiati nell'ambito dell'interazione tra servizi applicativi SPC che garantisce stabilmente uno scarto non superiore al decimo di minuto secondo rispetto alla scala di tempo universale coordinato (UTC), determinata ai sensi dell'art. 3, comma 1, della legge 11 agosto 1991, n. 273.	DGSIA	Uffici centrali DGSIA	CAD DPCM 01/04/2008
		PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	**Alta**	**PLC-035; PLC-065**					

		PR.DS-8: Meccanismi per il controllo dell'integrità sono utilizzati per verificare l'integrità hardware.	**Non Selezionata**						
	Information Protection Processes and Procedures (PR.IP): Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli assets.	**PR.IP-1: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale**	**Critica**	**PLC-051; PLC-057; PLC-065; PLC-080**	**PLC-051; PLC-057**	**CTR-M0-PR.IP-1-01** (ABSC 3.1.1): Si implementano configurazioni sicure standard per la protezione dei sistemi operativi.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 3.1.1)
					PLC-051; PLC-057	**CTR-M0-PR.IP-1-02** (ABSC 5.3.1): Prima di collegare alla rete un nuovo dispositivo le credenziali dell'amministratore predefinito vengono sostituite con valori coerenti con quelli delle utenze amministrative in uso.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 5.3.1)
					PLC-051; PLC-057	**CTR-M0-PR.IP-1-03** (ABSC 3.3.1): Le immagini d'installazione devono essere memorizzate offline.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 3.3.1)
					PLC-057	**CTR-M0-PR.IP-1-04** (ABSC 3.2.1): Sono definite e utilizzate configurazioni standard per workstation, server e gli altri tipi di sistemi usati.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 3.2.1)

		PR.IP-2: Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle).	**Non selezionata**						
		PR.IP-3: Sono attivi processi di controllo della modifica delle configurazioni	**Alta**	**PLC-052; PLC-058**					
		PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati periodicamente	**Critica**	**PLC-059**	**PLC-059**	**CTR-M0-PR.IP-4-01** (ABSC 10.1.1): Si effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 10.1.1)
					PLC-059	**CTR-M0-PR.IP-4-02** (ABSC 10.4.1): I supporti contenenti almeno una delle copie non sono permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 10.4.1)
					PLC-059	**CTR-M0-PR.IP-4-03** (196/2003): I backup dei dati personali sono eseguiti almeno settimanalmente.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	D.Lgs. 196/2003

		PR.IP-5: Sono rispettate le policy ed i regolamenti relativi agli ambienti fisici in cui operano le risorse dell'organizzazione	**Alta**	**PLC-015; PLC-074; PLC-099**					
		PR.IP-6: I dati sono distrutti in conformità con le policy	**Critica**	**PLC-060 - PLC-073**	**PLC-073**	**CTR-M0-PR.IP-6-01** (196/2003): I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili. Se riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, le informazioni precedentemente in essi contenute sono rese non intelligibili e non ricostruibili in alcun modo.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	D.Lgs. 196/2003
		PR.IP-7: I processi di protezione sono migliorati in maniera continuativa	**Bassa**	**PLC-131**					
		PR.IP-8: L'efficacia delle tecnologie di protezione è condivisa con i referenti appropriati	**Alta**	**PLC-082; PLC-131**					

		PR.IP-9: Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	**Alta**	**PLC-097; PLC-100; PLC-122**					
		PR.IP-10: I piani di risposta e recupero a seguito di incidenti/disastri sono verificati nel tempo	**Media**	**PLC-097; PLC-100**					
		PR.IP-11: Le problematiche inerenti la cybersecurity sono incluse nei processi di gestione del personale (es: screening, licenziamenti)	**Alta**	**PLC-116**					
		PR.IP-12:Viene sviluppato e implementato un piano di gestione delle vulnerabilità	**Critica**	**PLC-064; PLC-065; PLC-118**	**PLC-118**	**CTR-M0-PR.IP-12-01** (ABSC 4.8.2): Viene attribuito alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 4.8.2)

					PLC-118; PLC-065	**CTR-M0-PR.IP-12-02** (ABSC 4.7.1): Vengono verificate che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 4.7.1)
					PLC-064	**CTR-M0-PR.IP-12-03** (196/2003): L'aggiornamento periodico degli strumenti elettronici che trattano dati personali è effettuato almeno annualmente. In caso di trattamento di dati sensibili e giudiziari l'aggiornamento viene effettuato almeno ogni 6 mesi.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	D.Lgs. 196/2003
	Maintenance (PR.MA): La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:La manutenzione e la riparazione delle risorse e dei sistemi è svolta e registrata in modo tempestivo e portata a termine attraverso l'utilizzo di strumenti controllati ed autorizzati**	**Critica**	**PLC-053; PLC-054; PLC-058; PLC-065**	**PLC-053; PLC-054**	**CTR-M0-PR.MA-1-01** (ABSC 4.5.1): Le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni vengono installate automaticamente per le PdL.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario	AgID (ABSC 4.5.1)
					PLC-065; PLC-058; PLC-053; PLC-054	**CTR-M0-PR.MA-1-02** (ABSC 4.5.2): Esistono aggiornamenti specifci per i sistemi separati dalla rete, in particolare di quelli air-gapped, e si adottano misure adeguate al loro livello di criticità.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 4.5.2)

					PLC-058; PLC-053; PLC-054	**CTR-M0-PR.MA-1-03** (196/2003): Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati personali in caso di danneggiamento degli stessi o degli strumenti elettronici usati per accedervi, in tempi certi compatibili con i diritti degli interessati e comunque non superiori a sette giorni.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	D.Lgs. 196/2003
		PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	**Alta**	**PLC-031; PLC-053; PLC-054; PLC-055; PLC-056**					
	Protective Technology (PR.PT): Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-1: Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi**	**Alta**	**PLC-053; PLC-054; PLC-058; PLC-091; PLC-092; PLC-096**					
		PR.PT-2: I supporti di memorizzazione removibili sono protetti ed il loro uso è ristretto in accordo alle policy	**Critica**	**PLC-043; PLC-048; PLC-057**	**PLC-043**	**CTR-M0-PR.PT-2-01** (ABSC 8.7.1): L'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili è disabilitata.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 8.7.1)
					PLC-048; PLC-057	**CTR-M0-PR.PT-2-02** (ABSC 8.3.1): L'uso dei dispositivi esterni è limitato a quelli necessari alle attività preposte	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 8.3.1)

					PLC-057	**CTR-M0-PR.PT-2-03** (196/2003): Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati dati personali al fine di evitare accessi non autorizzati e trattamenti non consentiti.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	D.Lgs. 196/2003
		PR.PT-3: L'accesso alle risorse e ai sistemi è limitato secondo il principio di minima funzionalità	**Non selezionata**						
		PR.PT-4: Le reti di comunicazione e controllo sono protette	**Critica**	**PLC-057; PLC-089; PLC-090**	**PLC-089**	**CTR-M0-PR.PT-4-01** (DPCM 01/04/2008): I collegamenti fra le sedi di una o più Amministrazioni (ambito Intranet/Infranet) sono generalmente realizzati in Virtual Private Network (VPN) o con meccanismi equivalenti dal punto di vista della sicurezza.	DGSIA	Uffici centrali DGSIA/ Data center Napoli	CAD DPCM 01/04/2008

		PR.PT-5: I sistemi operano in stati funzionali predefiniti per ottenere la disponibilità (ad esempio sotto costrizione, sotto attacco, durante il recupero, normale funzionalità).	**Media**	**PLC-098**		

DETECT (DE)	**Anomalies and Events (DE.AE): Le attività anomale sono rilevate tempestivamente e il loro impatto potenziale viene analizzato.**	**DE.AE-1: sono definite, rese note e gestite delle pratiche di riferimento (c.d. baseline) inerenti l'utilizzo della rete ed i flussi informativi attesi per utenti e sistemi**	**Media**	**PLC-072; PLC-075**		
		DE.AE-2: Gli eventi rilevati vengono analizzati per comprendere gli obiettivi e le metodologie dell'attacco	**Alta**	**PLC-093; PLC-094**		
		DE.AE-3: Le informazioni relative agli eventi sono aggregate e correlate da sensori e sorgenti multiple	**Alta**	**PLC-072; PLC-075; PLC-094**		

		DE.AE-4: Viene determinato l'impatto di un evento	**Media**	**PLC-093**					
		DE.AE-5: Vengono definite delle soglie di allerta per gli incidenti	**Media**	**PLC-093**					
	Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati periodicamente per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity**	**Critica**	**PLC-076; PLC-077**	**PLC-076; PLC-077**	**CTR-M0-DE.CM-1-01** (ABSC 8.9.1): Il contenuto dei messaggi di posta viene filtrato prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	DGSIA	Ufficio centrale DGSIA / Centro Firewall Napoli	AgID (ABSC 8.9.1)
					PLC-076	**CTR-M0-DE.CM-1-02** (ABSC 8.9.2): Il contenuto del traffico web viene filtrato.	DGSIA	Ufficio centrale DGSIA / Centro Firewall Napoli	AgID (ABSC 8.9.2)
					PLC-076	**CTR-M0-DE.CM-1-03** (ABSC 8.9.3): Vengono bloccati nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (es. ".cab").	DGSIA	Ufficio centrale DGSIA / Centro Firewall Napoli	AgID (ABSC 8.9.3)
					PLC-076	**CTR-M0-DE.CM-1-04** (ABSC 13.8.1, ABSC 8.6.1): Viene bloccato il traffico da e verso url presenti in una blacklist, o comunque è previsto un meccanismo basato su blacklist o	DGSIA	Ufficio centrale DGSIA / Centro Firewall Napoli	AgID (ABSC 13.8.1, 8.6.1)

						whitelist.			
		DE.CM-2: Viene svolto il monitoraggio degli spazi fisici per rilevare potenziali eventi di cybersecurity	**Alta**	**PLC-016; PLC-078**					

		DE.CM-3: Viene svolto il monitoraggio del personale per rilevare potenziali eventi di cybersecurity	**Alta**	**PLC-088; PLC-092**					
		DE.CM-4: Il codice malevolo viene rilevato	**Critica**	**PLC-043; PLC-055; PLC-056; PLC-075; PLC-077**	**PLC-077; PLC-043**	**CTR-M0-DE.CM-4-01** (ABSC 8.1.1): Su tutti i sistemi connessi alla rete locale sono installati strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (anti-malware locali).	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 8.1.1)
					PLC-077; PLC-043	**CTR-M0-DE.CM-4-02** (ABSC 8.1.1): Gli strumenti di cui al controllo precedente (**CTR-M0-DE.CM-4-01**) sono mantenuti aggiornati in modo automatico.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 8.1.1)
					PLC-077; PLC-043	**CTR-M0-DE.CM-4-03** (ABSC 8.8.1): I sistemi sono configurati in modo che venga eseguita una scansione anti-malware dei supporti removibili al momento	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 8.8.1)

						della loro connessione.			
					PLC-077; PLC-043	**CTR-M0-DE.CM-4-04** (ABSC 8.7.2): È disattivata su tutti i sistemi l'esecuzione automatica dei contenuti dinamici (es. macro) presenti nei file.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 8.7.2)
					PLC-077; PLC-043	**CTR-M0-DE.CM-4-05** (ABSC 8.7.3): È disattivata su tutti i sistemi l'apertura automatica dei messaggi di posta elettronica.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario	AgID (ABSC 8.7.3)
					PLC-077; PLC-043	**CTR-M0-DE.CM-4-06** (ABSC 8.7.4): È disattivata su tutti i sistemi l'anteprima automatica dei contenuti dei file.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario	AgID (ABSC 8.7.4)
		DE.CM-5: Il codice non autorizzato su dispositivi mobili viene rilevato	**Alta**	**PLC-043; PLC-055; PLC-056**					
		DE.CM-6: Viene svolto il monitoraggio delle attività dei service provider esterni per rilevare potenziali eventi di cybersecurity	**Non selezionata**						

		DE.CM-7: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati.	**Critica**	**PLC-044; PLC-079; PLC-081; PLC-094**	**PLC-044; PLC-079**	**CTR-M0-DE.CM-7-01** (ABSC 8.1.2): Su tutti i dispositivi che lo consentono sono installati firewall personali.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 8.1.2)
					PLC-044; PLC-079	**CTR-M0-DE.CM-7-02** (ABSC 8.1.2): Su tutti i dispositivi che lo consentono sono installati IPS host-based.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 8.1.2)
		DE.CM-8: Vengono svolte scansioni per l'identificazione di vulnerabilità	**Critica**	**PLC-082**	**PLC-082**	**CTR-M0-DE.CM-8-01** (ABSC 4.1.1): È prevista, dopo ogni modifica significativa della configurazione, l'esecuzione di strumenti automatici di scansione delle vulnerabilità su tutti i sistemi in rete che fornisca a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche rilevate.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 4.1.1)
					PLC-082	**CTR-M0-DE.CM-8-02** (ABSC 4.4.1): I tool di scansione delle vulnerabilità vengono aggiornati regolarmente con tutte le più rilevanti vulnerabilità di sicurezza.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 4.4.1)

	Detection Processes (DE.DP): Sono adottati, mantenuti e verificati nel tempo i processi e le procedure di monitoraggio per assicurare una tempestiva e adeguata comprensione degli eventi di sicurezza	DE.DP-1: Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability	Alta	PLC-072; PLC-079; PLC-083		
		DE.DP-2: Le attività di monitoraggio soddisfano tutti i requisiti applicabili	Non selezionata			
		DE.DP-3: I processi di monitoraggio vengono testati	Alta	PLC-075; PLC-082; PLC-095		

		DE.DP-4: L'informazione relativa agli eventi rilevati è comunicata a tutte le parti interessate	**Alta**	**PLC-084; PLC-085**		
		DE.DP-5: I processi di monitoraggio sono oggetto di periodici miglioramenti e perfezionamenti	**Alta**	**PLC-083; PLC-094**		

RESPOND (RS)	Response Planning (RS.RP): Procedure e processi di risposa sono eseguiti e mantenuti per assicurare la tempestiva risposta agli eventi di cybersecurity rilevati.	RC.RP-1: Esiste un piano di ripristino (recovery plan) e questo viene eseguito durante o dopo un incidente	Alta	PLC-084; PLC-100		
	Communications (RS.CO): Le attività di risposta sono coordinate con le parti interne ed esterne, per includere eventuale supporto da parte degli organi di legge o dalle forze dell'ordine.	RS.CO-1: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	Alta	PLC-100; PLC-106		
		RS.CO-2: Sono stabiliti dei criteri per documentare gli incidenti/eventi	Alta	PLC-084; PLC-096; PLC-100		

		RS.CO-3: Le informazioni sono condivise in maniera coerente con il piano di risposta	**Non selezionata**			
		RS.CO-4: Il coordinamento con le parti interessate dell'organizzazione avviene in coerenza con i piani di risposta	**Alta**	**PLC-084; PLC-100**		

		RS.CO-5: E' attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awareness)	Alta	PLC-096; PLC-101; PLC-120		
	Analysis (RS.AN): Vengono condotte analisi per assicurare un'adeguata riposta e supporto alle attività di ripristino	RS.AN-1: Le notifiche provenienti dai sistemi di monitoraggio vengono sempre visionate e analizzate	Alta	PLC-075; PLC-084		
		RS.AN-2: Viene compreso l'impatto di ogni incidente	Alta	PLC-084; PLC-101		

		RS.AN-3: A seguito di un incidente viene svolta un'analisi forense	**Alta**	**PLC-094; PLC-101**					
		RS.AN-4: Gli incidenti sono categorizzati in maniera coerente con i piani di risposta	**Non selezionata**						
	Mitigation (RS.MI): Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i sui effetti e per rimuovere l'incidente.	**RS.MI-1: In caso di incidente vengono messe in atto procedure atte a contenerne l'impatto**	**Alta**	**PLC-084; PLC-100**					
		RS.MI-2: In caso di incidente vengono messe in atto procedure atte a mitigarne gli effetti	**Non selezionata**						
		RS.MI-3: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato	**Critica**	**PLC-118; PLC-120**	**PLC-118-PLC-120**	**CTR-M0-RS.MI-3-01 (ABSC 4.7.1):** Le nuove vulnerabilità scoperte vengono risolte per mezzo di patch o implementando opportune contromisure, oppure documentando e accettando un ragionevole rischio.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 4.7.1)

	Improvements (RS.IM): Le attività di risposta sono migliorate incorporando le "lesson learned" da attività precedenti di monitoraggio e risposta.	**RS.IM-1: I piani di risposta agli incidenti tengono in considerazione le esperienze passate (lesson learned)**	**Alta**	**PLC-059; PLC-100; PLC-101; PLC-102**					
		RS.IM-2: Le strategie di risposta agli incidenti sono aggiornate	**Alta**	**PLC-059; PLC-100**					
RECOVER (RC)	**Recovery Planning (RC.RP): I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un tempestivo recupero dei sistemi o asset coinvolti da un evento di cybersecurity.**	**RC.RP-1: Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un evento** **RC.IM-1: I piani di riprisitino tengono in considerazione le esperienze passate (lesson learned)**	**Critica**	**PLC-102; PLC-103; PLC-048**	**PLC-103**	**CTR-M0-RC.RP-1-01** (ABSC 3.2.2): Eventuali sistemi in esercizio che vengono compromessi sono ripristinati usando la configurazione standard.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	AgID (ABSC 3.2.2)
					PLC-048; PLC-102	**CTR-M1-RC.RP-1-01**: Esiste un piano di ripristino.	CISIA/Assistenza tecnica (esterna)	Ufficio giudiziario Sala Server	

	Improvements (RC.IM): I piani di ripristino ed i relativi processi sono migliorati tenendo conto delle "lesson learned" per le attività future.		Alta	PLC-059; PLC-102		
		RC.IM-2: Le strategie di recupero sono aggiornate	Alta	PLC-059; PLC-102		
	Communications (RC.CO): Le attività di ripristino a seguito di un incidente sono coordinate con le parti interne ed esterne, come ad esempio, le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT.	RC.CO-1: A seguito di un incidente vengono gestite le pubbliche relazioni	Alta	PLC-084; PLC-105		
		RC.CO-2: A seguito di un incidente viene ripristinata la reputazione	Non selezionata			
		RC.CO-3: Le attività di recupero condotte a seguito di un incidente vengono comunicate alle parti interessate interne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione	Alta	PLC-059; PLC-104		

Controlli di sicurezza
Parte II – Livello M1

Function	Category	Subcategory	Priorità	Policy / subcategory	Policy / controlli	Livello M1	RUOLO	CONTESTO	RIFERIMENTI NORMATIVI
IDENTIFY (ID)	**Asset Management (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi di business e con la strategia di rischio dell'organizzazione**	**ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione**	**Critica**	**PLC-001; PLC-062**	**PLC-001**	**CTR-M1-ID.AM-1-01**: Per ogni sistema e apparato fisico in uso è identificato un responsabile.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data center	
					PLC-001	**CTR-M1-ID.AM-1-02**: Esiste una procedura interna documentata che gestisce e controlla l'inventario dei sistemi e apparati di cui al controllo precedente.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data center	

		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	**Critica**	**PLC-002; PLC-003; PLC-004; PLC-062; PLC-080**	**PLC-002; PLC-062**	**CTR-M1-ID.AM-2-01**: Tutti i software, anche non espressamente autorizzati, in uso sui sistemi (PC, laptop,workstation,server, ...) vengono catalogati.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data center	
					PLC-002	**CTR-M1-ID.AM-2-02**: Vengono mantenuti, mediante opportuni strumenti informatici, tutte le configurazioni e i cambiamenti storici dei software di cui al controllo **CTR-M1-ID.AM-2-01**.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data center	
					PLC-002; PLC-080	**CTR-M1-ID.AM-2-03**: Per ogni software in uso è identificato un responsabile.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data center	
					PLC-003; PLC-004	**CTR-M1-ID.AM-2-04**: Esiste una procedura interna documentata che governa la gestione e il controllo dell'inventario dei software.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data center	

		ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati.	**Crittica**	**PLC-005; PLC-006; PLC-062; PLC-072**	**PLC-006; PLC-072**	**CTR-M1-ID.AM-3-01**: Tutti i flussi di dati e le comunicazioni/notificazioni in ingresso, in uscita, e interni sono censiti e documentati.	DGSIA/CISIA/Assistenza tecnica	Tutti gli UUGG e sale server	
					PLC-006	**CTR-M1-ID.AM-3-02**: Per ogni flusso e comunicazione/notificazione sono identificati e descritti i dati coinvolti e i ruoli dei mittenti e destinatari.	DGSIA/CISIA/Assistenza tecnica	Tutti gli UUGG e sale server	
					PLC-006; PLC-062; PLC-072	**CTR-M1-ID.AM-3-03**: Per i flussi e le comunicazioni/notificazioni di una certa rilevanza per l'organizzazione, i dati coinvolti vengono catalogati sulla base di livelli di confidenzialità, integrità e disponibilità.	DGSIA/CISIA/Assistenza tecnica	Tutti gli UUGG e sale server	
		ID.AM-4: I sistemi informativi esterni all'organizzazione sono catalogati	**Critica**	**PLC-005 ; PLC-007; PLC-072**	**PLC-007; PLC-072**	**CTR-M1-ID.AM-4-01**: Tutti i sistemi informatici esterni (inclusi portali di altre PPAA, provider di posta esterni, provider di data storing esterni, ecc.), con cui i sistemi interni scambiano informazioni/dati (compresi Web browser, client di posta o specifici client di scambio informazioni/dati - es., Dropbox client, GDrive, ecc.), vengono catalogati, comprese le loro configurazioni necessarie per l'interazione con essi (protocolli, interfacce applicative, indirizzi di rete, politiche di sicurezza,...).	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data center	

					PLC-007	**CTR-M1-ID.AM-4-02**: Relativamente ai sistemi del controllo precedente, esiste una procedura interna documentata che governa la gestione e il controllo dell'inventario.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data center	
					PLC-007	**CTR-M1-ID.AM-4-03**: Esiste ed è identificato un responsabile interno per ogni sistema esterno identificato nell'inventario.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data center	
		ID.AM-5: Le risorse (es: hardware, dispositivi, dati e software) sono prioritizzati in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione	**Critica**	**PLC-008; PLC-009; PLC-010; PLC-011; PLC-012; PLC-036**	**PLC-010; PLC-011**	**CTR-M1-ID.AM-5-01**: Tutte le risorse logiche e fisiche (hardware, dispositivi, reti, dati, software) censite vengono prioritizzate sulla base del livello di criticità attribuita all'informazione trattata.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data center	
					PLC-010; PLC-011; PLC-036	**CTR-M1-ID.AM-5-02**: Le modalità di prioritizzazione sono ben identificate e documentate; tali modalità tengono conto del livello di classificazione dell'informazione trattata rispetto ai parametri di: confidenzialità, disponibilità, integrità, autenticità e controllo degli accessi.	DGSIA/CISIA/Assistenza Tecnica	Tutti gli UUGG e Data center	
					PLC-012	**CTR-M1-ID.AM-5-03**: Esiste ed è identificato un responsabile interno che controlla i processi di prioritizzazione delle risorse fisiche e logiche.	CISIA	Tutti gli UUGG e Data center	
					PLC-012	**CTR-M1-ID.AM-5-04**: Esiste una procedura interna documentata che governa le modalità di prioritizzazione.	DGSIA/CISIA	Tutti gli UUGG e Data center	

		ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	**Alta**	**PLC-106; PLC-107; PLC-108**	**PLC-106**	**CTR-M1-ID.AM-6-01**: Esiste una normativa interna documentata che identifica ed elenca i ruoli e le responsabilità inerenti la Cybersecurity, nonché le attività in carico a ciascun ruolo.	DGSIA/CISIA	Tutti gli UUGG e Data center	
					PLC-107	**CTR-M1-ID.AM-6-02**: Esiste una normativa interna documentata che disciplina l'utilizzo e il trattamento delle informazioni e degli strumenti informatici da parte di tutto il personale (es. fornitori, consulenti, ecc.).	DGSIA/CISIA	Tutti gli UUGG e Data center	
					PLC-108	**CTR-M1-ID.AM-6-03**: Esiste una normativa interna documentata che disciplina l'utilizzo e il trattamento delle informazioni e degli strumenti informatici da parte di terze parti (es. fornitori, consulenti, ecc.).	DGSIA/CISIA	Tutti gli UUGG e Data center	
	Business Environment (ID.BE): La mission dell'organizzazione, gli obiettivi, le attività e gli attori coinvolti sono compresi e valutate in termini di priorità.	**ID.BE-1:Il ruolo dell'organizzazione all'interno della filiera produttiva è identificato e reso noto**							

	Tali informazioni influenzano i ruoli, le responsabilità di cybersecurity e le decisioni in materia di gestione del rischio.	**ID.BE-2: Il ruolo dell'organizzazione come infrastruttura critica e nel settore industriale di riferimento è identificato e reso noto**				
		ID.BE-3: Sono definite e rese note delle priorità per quanto riguarda la missione, gli obiettivi e le attività dell'organizzazione.				
		ID.BE-4: Sono identificate e rese note interdipendenze e funzioni fondamentali per la fornitura di servizi critici				

		ID.BE-5: Sono identificati e resi noti i requisiti di resilienza a supporto della fornitura di servizi critici	**Alta**	**PLC-109**; **PLC-122**	**PLC109**	**CTR-M1-ID.BE-5-01**: Esiste ed è gestito un elenco di servizi critici che l'ufficio giudiziario offre come propria funzione istituzionale a tutti coloro che ne fanno uso (es., altri uffici giudiziari, altre PPAA, avvocatura, cittadini, ecc.).	DGSIA/CISIA	Tutti gli UUGG e Data center	
					PLC-109	**CTR-M1-ID.BE-5-02**: Esiste ed è gestito un elenco di requisiti di resilienza per la fornitura dei servizi critici di cui al controllo **CTR-M1-ID.BE-5-01**.	DGSIA/CISIA	Tutti gli UUGG e Data center	CAD
	Governance (ID.GV): Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono	**ID.GV-1: E' indetificata e resa nota una policy di sicurezza delle informazioni**	**Critica**	**PLC-110; PLC-111; PLC-112; PLC-113; PLC-114; PLC-115**	**PLC-110**	**CTR-M1-ID.GV-1-01**: Esiste una policy documentata di sicurezza delle informazioni.	DGSIA/CISIA/Assistenza Tecnica	Uffici centrali DGSIA UU.GG. e sale server	
					PLC-111	**CTR-M1-ID.GV-1-02**: Esiste un responsabile che controlla e garantisce l'applicazione delle policy di sicurezza delle informazioni.	DGSIA/CISIA	Uffici centrali DGSIA UU.GG. e sale server	

	compresi e utilizzati nella gestione del rischio di cybersecurity.								
		ID.GV-2: Ruoli e responsabilità inerenti la sicurezza delle informazioni sono coordinati ed allineati con i ruoli interni ed i partner esterni	**Alta**	**PLC-116**	**PLC-116**	**CTR-M1-ID.GV-2-01**(DPO - Data Processing Officer): Esiste una normativa interna documentata che identifica ed elenca i ruoli e le responsabilità inerenti la sicurezza delle informazioni; tali ruoli vengono mappati sui ruoli istituzionali interni all'ufficio giudiziario e su quelli delle parti esterne (es., fornitori, consulenti, personale di altro ufficio giudiziario, ecc.).	DGSIA/CISIA	Uffici centrali DGSIA e UU.GG.	GDPR
					PLC-116	**CTR-M1-ID.GV-2-02**: Esiste un responsabile del processo di gestione dei ruoli e delle relative responsabilità inerenti la sicurezza delle informazioni.	DGSIA/CISIA	Uffici centrali DGSIA e UU.GG.	GDPR

		ID.GV-3: I requisiti legali in materia di cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti	**Alta**	**PLC-110; PLC-117**	**PLC-110; PLC-117**	**CTR-M1-ID.GV-3-01**: Esiste una normativa interna documentata che identifica ed elenca i requisiti legali in materia di Cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili.	DGSIA	Uffici centrali DGSIA	
					PLC-117	**CTR-M1-ID.GV-3-02**: Esiste una procedura interna documentata che disciplina il processo di comunicazione dei requisiti legali in materia di sicurezza ed obblighi di privacy alle parti interessate (es. personale dell'ufficio giudiziario, fornitori, consulenti, ecc.).	DGSIA/CISIA	Uffici centrali DGSIA e UU.GG.	
		ID.GV-4: La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity				**CTR-M1-ID.GV-4-01**: Esiste un piano della sicurezza che tiene conto dei rischi legati alla cybersecurity.	DGSIA/CISIA	Uffici centrali DGSIA, UU.GG e sale server	
	Risk Assessment (ID.RA): L'impresa comprende il rischio di cybersecurity inerente l' operatività dell'organizzazione	**ID.RA-1: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizz**	**Alta**	**PLC-118; PLC-119; PLC-122**	**PLC-118**	**CTR-M1-ID.RA-1-01**: Esiste un disciplinare tecnico interno documentato che regola le modalità con cui le ricerche di vulnerabilità devono essere eseguite, identifica gli eventi che scatenano tali ricerche e gli intervalli di tempo di ripetizione delle suddette.	CISIA/Assistenza tecnica (esterna)	Tutti gli UUGG e Data center	

	(incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**azione sono identificate e documentate**			**PLC-119; PLC-122**	**CTR-M1-ID.RA-1-02**: Esiste un inventario delle vulnerabilità conosciute, organizzato per tipologia di risorsa (sistema, dispositivo, applicativo, ecc.).	CISIA/Assistenza tecnica (esterna)	Tutti gli UUGG e Data center	
					PLC-119	**CTR-M1-ID.RA-1-03**: Ogni vulnerabilità viene identifica mediante un codice univoco e opportunamente documentata.	CISIA/Assistenza tecnica (esterna)	Tutti gli UUGG e Data center	
		ID.RA-2: L'organizzazione riceve informazioni su minacce e vulnerabilità da fonti esterne (e.g. CERT, fonti aperte, forum di information sharing)	**Critica**	**PLC-120**	**PLC-120**	**CTR-M1-ID.RA-2-01**: Esiste un centro di riferimento interno per la raccolta di informazioni inerenti minacce e vulnerabilità di cybersecurity.	DGSIA	Uffici centrali DGSIA	
					PLC-120	**CTR-M1-ID.RA-2-02**: Il personale del centro di riferimento interno per la ricezione e la raccolta di informazioni inerenti minacce e vulnerabilità di cybersecurity è ben identificato.	DGSIA	Uffici centrali DGSIA	
					PLC-120	**CTR-M1-ID.RA-2-03**: Esiste un elenco ufficiale delle fonti esterne attendibili e fidate per la raccolta delle informazioni inerenti minacce e vulnerabilità di Cybersecurity.	DGSIA	Uffici centrali DGSIA	
					PLC-120	**CTR-M1-ID.RA-2-04**: Il responsabile della gestione e manutenzione dell'elenco ufficiale delle fonti esterne attendibili e fidate è ben identificato.	DGSIA	Uffici centrali DGSIA	
		ID.RA-3: Le minacce, sia interne che esterne,	**Alta**	**PLC-119; PLC-120**	**PLC-119**	**CTR-M1-ID.RA-3-01**: Sono identificate e documentate le minacce (es. attacchi) conosciute a cui si è esposti.	DGSIA/CISIA	Uffici centrali DGSIA e UU.GG. e sale server	

		sono identificate e documentate			**PLC-119**	**CTR-M1-ID.RA-3-02**: È identificato un responsabile della gestione del processo di identificazione e documentazione delle minacce.	DGSIA/CISIA	Uffici centrali DGSIA e UU.GG. e sale server	
					PLC-120	**CTR-M1-ID.RA-3-03** (ABSC 4.4.2): Si utilizza un servizio fidato e attendibile che fornisce tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Tali informazioni vengono utilizzate per aggiornare le attività di scansione.	DGSIA/CISIA/Assistenza tecnica (esterna)	Tutti gli UUGG e Data center	
		ID.RA-4: Sono identificati i potenziali impatti sul business e le relative probabilità di accadimento	**Alta**	**PLC-121; PLC-122**	**PLC-121; PLC-122**	**CTR-M1-ID.RA-4-01**: Viene regolarmente effettuato un processo di impatto delle vulnerabilità e minacce sul business (Business Impact Analysis)	DGSIA/CISIA	Uffici centrali DGSIA Tutti gli UUGG e Data center	
		ID.RA-5: Le minacce, le vulnerabilità, le relative probabilità	**Critica**	**PLC-122**	**PLC-122**	**CTR-M1-ID.RA-5-01**: Nel determinare il rischio vengono presi in considerazione le minacce, le vulnerabilità e le relative probabilità di accadimento.	DGSIA/CISIA	Uffici centrali DGSIA Tutti gli UUGG e Data center	

		di accadimento e conseguenti impatti sono utilizzati per determinare il rischio							
		ID.RA-6: Sono identificate e prioritizzate le risposte al rischio	**Media**	**PLC-123; PLC-124**	**PLC-123; PLC-124**	**CTR-M1-ID.RA-6-01**: Le modalità d'identificazione e prioritizzazione delle risposte al rischio e la loro gestione sono documentate.	DGSIA/CISIA	Uffici centrali DGSIA, UU.GG. e sale server	
					PLC-123; PLC-124	**CTR-M1-ID.RA-6-02**: Esiste un responsabile della gestione delle risposte al rischio.	DGSIA/CISIA	Uffici centrali DGSIA, UU.GG. e sale server	
	Risk Management Strategy (ID.RM): Le priorità e i requisiti dell'organizzazione e la tolleranza al rischio sono definiti e utilizzati per supportare le decisioni sul rischio operazionale.	**ID.RM-1: I processi di risk management sono stabiliti, gestiti e concordati tra i responsabili dell'organizzazione (c.d. stakeholder)**	**Alta**	**PLC-123; PLC-129**	**PLC-123; PLC-129**	**CTR-M1-ID.RM-1-01**: La gestione del rischio è disciplinata da opportuni processi documentati che ne stabiliscono attività, ruoli e responsabilità, modalità di gestione e controllo.	DGSIA/CISIA	Uffici centrali DGSIA Tutti gli UUGG e Data center	

		ID.RM-2: Il rischio tollerato dall'organizzazione è identificato ed espresso chiaramente	**Non Selezionata**			
		ID.RM-3: Il rischio tollerato è determinato tenendo conto del ruolo dell'organizzazione come infrastruttura critica e dei rischi specifici presenti nel settore industriale di appartenenza	**Non Selezionata**			

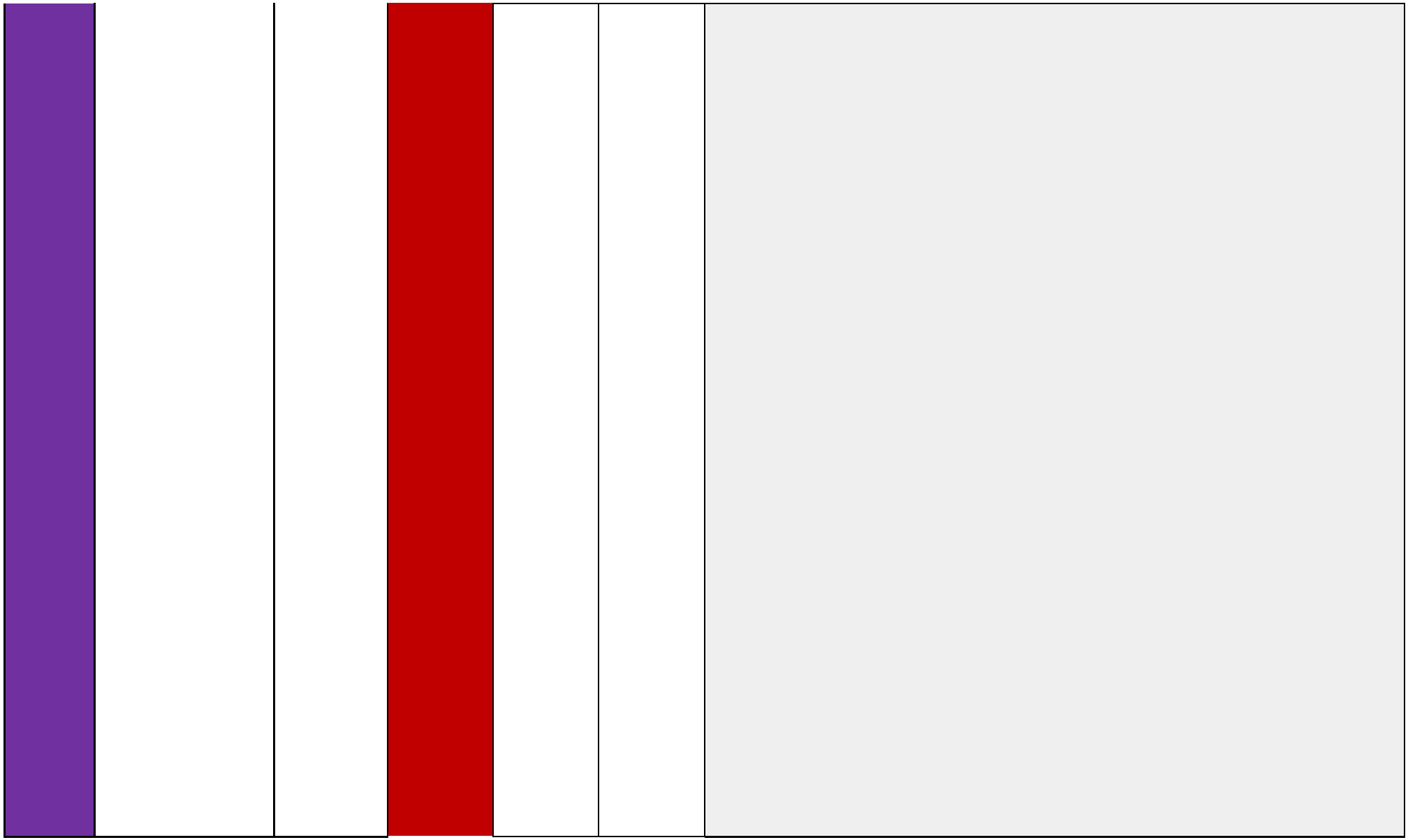
	Supply Chain Risk Management (ID.SC): Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione vengono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio della fornitura Cyber. L'organizzazione ha in essere i processi per identificare, valutare e gestire i rischi della catena di approvvigionamento dei sistemi e dei servizi informatici.	**ID.SC-1: I processi di gestione del rischio inerenti la catena della fornitura Cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione**	**Alta**	**PLC-124; PLC-130**	**PLC-124; PLC-130**	**CTR-M1-ID.SC-1-01:** Il rischio cyber associato alla fornitura di sistemi e servizi esterni è opportunamente valutato e documentato	DGSIA/CISIA	Uffici centrali DGSIA Tutti gli UUGG e Data center	
		ID.SC-2: Identificare, prioritizzare e valutare i fornitori e i partner di sistemi informatici, componenti e servizi critici, utilizzando un processo di valutazione del rischio inerente la fornitura Cyber	**Media**	**PLC-124; PLC-128**	**PLC-124**	**CTR-M1-ID.SC-2-01:** I fornitori dei sistemi, dei componenti e dei servizi informatici vengono priorizzati sulla base delle priorità/criticità associate ai sistemi e servizi informatici da essi forniti e/o erogati.	DGSIA	Uffici centrali DGSIA	
					PLC-128	**CTR-M1-ID.SC-2-02:** Esiste un processo documentato che disciplina la priorizzazione dei fornitori.	DGSIA	Uffici centrali DGSIA	
					PLC-128	**CTR-M1-ID.SC-2-03:** Esiste un responsabile del processo di priorizzazione dei fornitori.	DGSIA	Uffici centrali DGSIA	

		ID.SC-3: Fornitori e partner sono tenuti per contratto ad attuare misure appropriate volte a conseguire gli obiettivi del programma di sicurezza delle informazioni o Piano di gestione del rischio della catena di fornitura Cyber	**Alta**	**PLC-125; PLC-128**	**PLC-125; PLC-128**	**CTR-M1-ID.SC-3-01:** Il contratto di fornitura di prodotti/servizi sottoscritto da ogni fornitore impegna quest'ultimo ad attuare misure appropriate volte a garantire i livelli di cybersecurity minimi per servizi e prodotti.	DGSIA/CISIA	Uffici centrali DGSIA, UU.GG. e sale server	
		ID.SC-4: Fornitori e partner sono monitorati per verificare che essi adempiano ai loro obblighi, come richiesto. Revisione degli audit,	**Alta**	**PLC-126; PLC-128; PLC-063**	**PLC-126; PLC-063; PLC-128**	**CTR-M1-ID.SC-4-01:** Esistono delle procedure e modalità documentate di monitoraggio delle attività e dei comportamenti condotti dai fornitori nell'espletamento dei loro obblighi contrattuali.	DGSIA/CISIA	Uffici centrali DGSIA, UU.GG. e sale server	
					PLC-126	**CTR-M1-ID.SC-4-02:** Le procedure e le modalità di monitoraggio sono specializzate per tipologia di sistema/servizio fornito/erogato dal fornitore sulla base della prioritizzazione del sistema/servizio.	DGSIA/CISIA	Uffici centrali DGSIA, UU.GG. e sale server	

		sintesi dei risultati dei test o di altre valutazioni equivalenti dei fornitori sono condotte.							
		ID.SC-5: La pianificazione e la verifica della risposta e del ripristino sono condotti con i fornitori critici	**Alta**	**PLC-122; PLC-127**	**PLC-122; PLC-127**	**CTR-M1-ID.SC-5-01:** I piani di risposta e ripristino vengono progettati e verificati in cooperazione e coordinamento con i fornitori dei sistemi e servizi a criticità alta.	DGSIA/CISIA	Uffici centrali DGSIA, UU.GG. e sale server	
PROTECT (PR)	**Access Control (PR.AC): L'accesso agli asset ed alle relative risorse è limitato al personale, ai processi, ai dispositivi, alle attività ed alle transazioni effettivamente autorizzate**	**PR.AC-1: Le identità digitali e le credenziali di accesso per gli utenti e per i dispositivi autorizzati sono amministrat**	**Critica**	**PLC-017; PLC-018; PLC-019; PLC-020; PLC-021; PLC-023; PLC-024; PLC-025; PLC-026; PLC-047**	**PLC-024**	**CTR-M1-PR.AC-1-01**: Esiste un sistema di gestione delle identità digitali e delle credenziali di accesso per gli utenti, le applicazioni e i dispositivi (server, PC, laptop, ecc.).	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data center	
					PLC-026	**CTR-M1-PR.AC-1-02**: Esiste una procedura interna documentata che disciplina la gestione delle utenze, dei ruoli e delle responsabilità.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data center	

		e			**PLC-026**	**CTR-M1-PR.AC-1-03**: Esiste un processo documentato conforme alla procedura di cui **CTR-M1-PR.AC-1-02** per la registrazione e la de-registrazione delle utenze (personale, applicazioni e dispositivi) che abilita le stesse alla fase di attribuzione o revoca dei diritti d'accesso ai sistemi e ai servizi.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data center	
					PLC-026	**CTR-M1-PR.AC-1-04**: Esiste un processo documentato conforme alla procedura di cui **CTR-M1-PR.AC-1-02** per l'attribuzione e la revoca dei diritti d'accesso alle utenze (personale, applicazioni e dispositivi) ai sistemi e ai servizi.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data center	
					PLC-026	**CTR-M1-PR.AC-1-05**: Esiste una procedura interna documentata che disciplina le modalità e la gestione dell'assegnazione dell'informazione segreta (es. password) necessaria all'autenticazione delle utenze.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data center	
					PLC-026	**CTR-M1-PR.AC-1-06**: Esiste una politica interna documentata che identifica una serie di pratiche per la conservazione dell'informazione segreta per l'autenticazione.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data center	
					PLC-024	**CTR-M1-PR.AC-1-07**: È in uso un sistema automatico per la gestione dello aging e history delle password.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

					PLC-019	**CTR-M1-PR.AC-1-08:** Esiste un inventario di tutte le utenze di amministrazione e, per ognuna di esse, la formale (documentata) autorizzazione ad operare.	CISIA/Assistenza tecnica (esterna)	Tutti gli UUGG e Data Center	

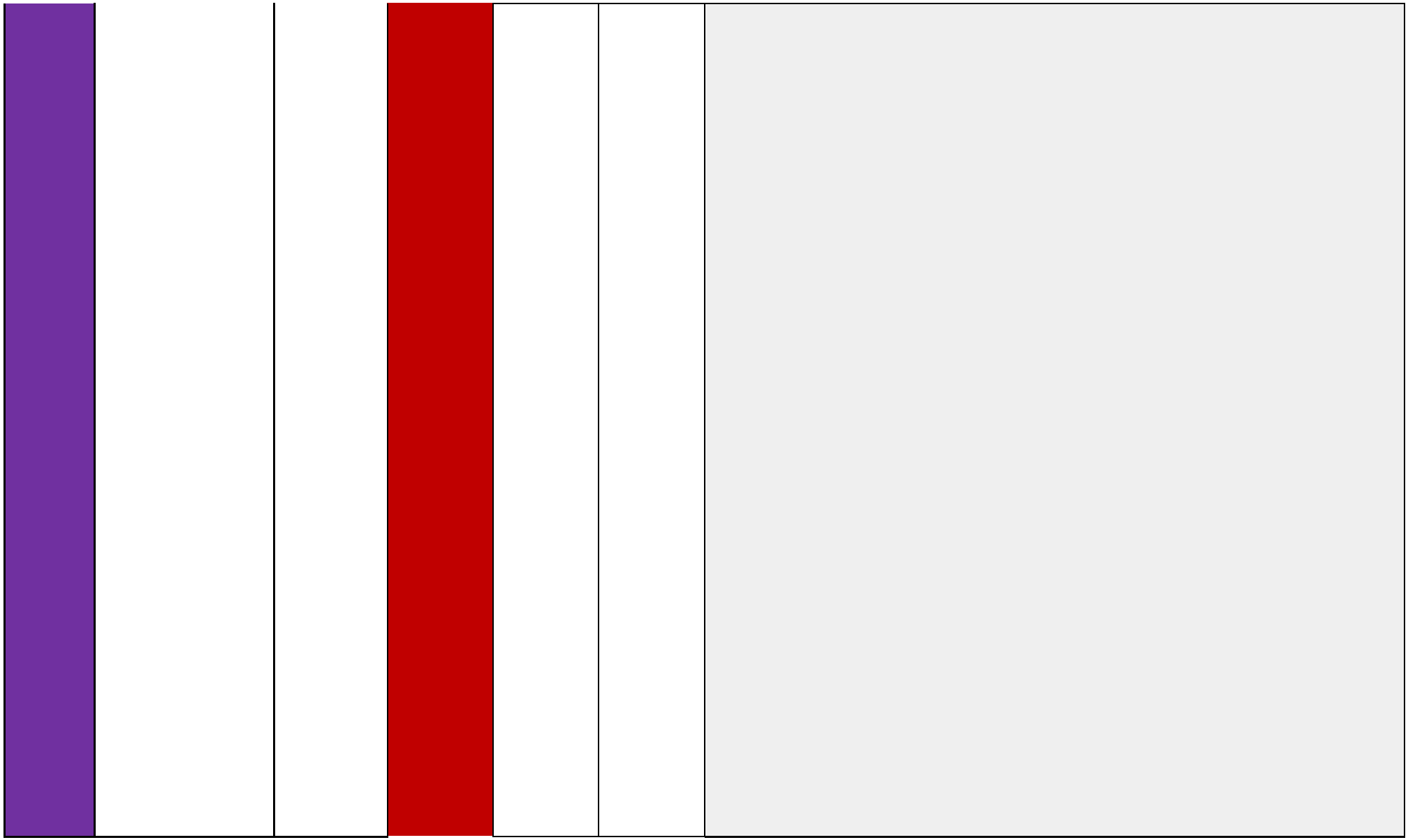


		PR.AC-2: L'accesso fisico alle risorse è protetto e amministrato	**Alta**	**PLC-013; PLC-014; PLC-015; PLC-016**	**PLC-015**	**CTR-M1-PR.AC-2-01**: Sono definiti, mediante opportuna documentazione tecnica, i perimetri dei locali in cui si trovano sistemi informatici (sale server, locali con PDL, ...)	DGSIA/CISIA	Tutti gli UUGG e Data Center	
					PLC-015; PLC-016	**CTR-M1-PR.AC-2-02**: I locali in cui si trovano sistemi informatici (sale server, locali con PDL, ...) sono protetti da adeguati controlli di ingresso. I controlli garantiscono che solo il personale autorizzato ha l'accesso.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-013; PLC-014	**CTR-M1-PR.AC-2-03**: Esiste una procedura interna documentata che disciplina la gestione e il controllo degli accessi fisici del personale autorizzato alla sala server e a specifiche aree dell'ufficio giudiziario.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-015	**CTR-M1-PR.AC-2-04**: I punti di accesso per le consegne e le aree di carico/scarico e altri punti in cui persone non autorizzate possono entrare nei locali sono controllati e, possibilmente, isolati dalla sala server e dalle aree di sicurezza dell'ufficio giudiziario per evitare l'accesso non autorizzato.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		PR.AC-3: L'accesso remoto alle risorse è amministrato	**Critica**	**PLC-031; PLC-055; PLC-056**	**PLC-031**	**CTR-M1-PR.AC-3-01** : Esiste una politica documentata di controllo degli accessi da remoto alle risorse e ai dati.	DGSIA/CISIA/Assistenza tecnica	Tutti gli UUGG e Data Center	

		PR.AC-4: Gli accessi alle risorse sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	**Critica**	**PLC-027; PLC-028; PLC-029; PLC-030**	**PLC-030**	**CTR-M1-PR.AC-4-01**: Gli utenti possono accedere esclusivamente alla rete e ai servizi ai quali sono stati formalmente autorizzati ad accedere.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-030	**CTR-M1-PR.AC-4-02**: Gli accessi ai dati, alle applicazioni e ai sistemi da parte delle utenze dell'ufficio giudiziario sono gestiti e controllati sulla base della separazione delle funzioni istituzionali e delle aree di responsabilità individuate all'interno dell'ufficio.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-028	**CTR-M1-PR.AC-4-03**: Esiste una policy documentata che disciplina l'assegnazione dei diritti di accesso privilegiati.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-027	**CTR-M1-PR.AC-4-04 (ABSC 5.1.3):** Si assegnano a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 5.1.3)

		PR.AC-5: L'integrità di rete è protetta, anche applicando la segregazione di rete dove appropriata	**Alta**	**PLC-032; PLC-033; PLC-034**	**PLC-032; PLC-033; PLC-034**	**CTR-M1-PR.AC-5-01**: Esistono delle policy documentate per la protezione della rete, dei sistemi connessi e dei dati in transito.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-032; PLC-033; PLC-034	**CTR-M1-PR.AC-5-02**: Esiste una procedura documentata che disciplina la segregazione della rete.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-032; PLC-033; PLC-034	**CTR-M1-PR.AC-5-03:** Viene segmentata la rete in base al livello di sicurezza e di classificazione delle informazioni memorizzate su server e PdL. Tutte le informazioni sensibili sono confinate su segmenti separati, utilizzando firewall per filtrare il traffico tra i segmenti in modo che il traffico consentito sia soltanto quello indispensabile all'espletamento delle funzioni.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

		PR.AC-6: Le identità digitali sono comprovabili, associate a credenziali e, qualora richiesto, possono essere asserite durante le interazioni	**Critica**	**PLC-021; PLC-023; PLC-024; PLC-027; PLC-047**	**PLC-024; PLC-047**	**CTR-M1-PR.AC-6-01**: Viene utilizzato esclusivamente ADN per la gestione delle identità digitali, delle credenziali e degli accessi alle PdL, workstation, server, laptop e altri dispositivi per le utenze dell'ufficio giudiziario.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-024; PLC-047	**CTR-M1-PR.AC-6-02**: Viene utilizzato esclusivamente ADN per l'accesso ai sistemi applicativi (SICP, SIPPI, TIAP, ecc.) dell'ufficio giudiziario.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	



	Awareness and Training (PR.AT): Il personale e le terze sono sensibilizzate e formate in materia di cybersecurity e ricevono adeguata preparazione, coerente con le politiche, le procedure e gli accordi esistenti, per svolgere correttamente i compiti e le responsabilità legate alla sicurezza delle informazioni	**PR.AT-1: Tutti gli utenti sono informati e addestrati**	**Critica**	**PLC-021; PLC-022; PLC-026**	**PLC-026**	**CTR-M1-PR.AT-1-01:** Esiste un piano interno di formazione e aggiornamento documentato su aspetti di cybersecurity per il personale non di amministrazione. I percorsi formativi sono organizzati per funzione di lavoro (ruoli e responsabilità) e indirizzano addrestramenti mirati su politiche, procedure organizzative e tecniche specifiche per la cybersecurity.	DGSIA	Uffici centrali DGSIA	
		PR.AT-2: Gli utenti privilegiati (e.g. Amministratori di Sistema) comprendono ruoli e responsabilità	**Critica**	**PLC-019**	**PLC-019**	**CTR-M1-PR.AT-2-01**: Esiste un piano interno di formazione e aggiornmento documentato su aspetti di Cybersecurity per il personale di amministrazione dei sistemi, dei dispositivi e delle reti.	DGSIA	Uffici centrali DGSIA	

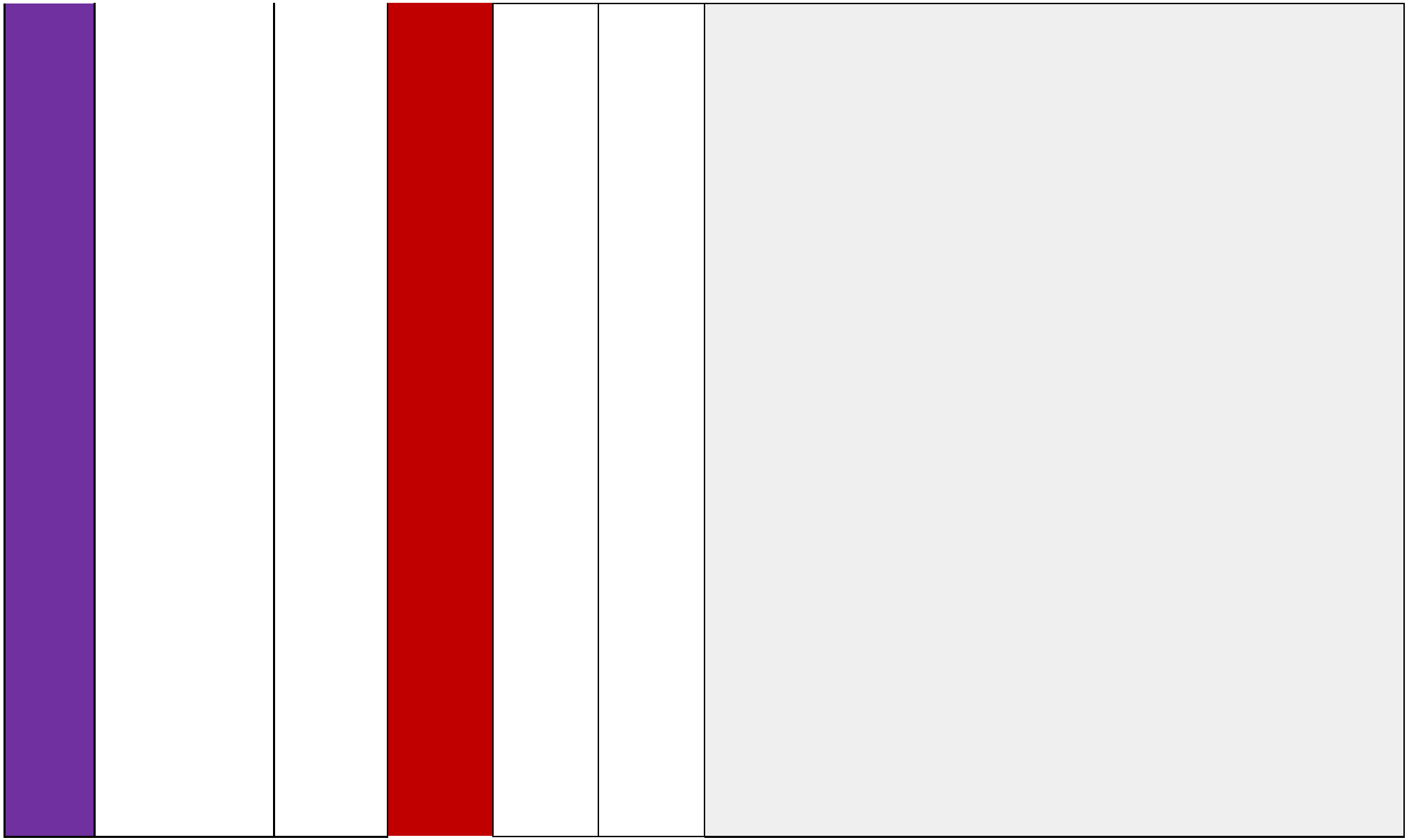
		PR.AT-3: Tutte le terze parti (es. fornitori, clienti, partner) comprendono ruoli e responsabilità	**Critica**	**PLC-125**	**PLC-125**	**CTR-M1-PR.AT-3-01**: Esiste una normativa interna documentata che identifica e formalizza ruoli e responsabilità inerenti la cybersecurity per le terze parti.	DGSIA/CISIA	Tutti gli UUGG e Data Center	
					PLC-125	**CTR-M1-PR.AT-3-02**: Esiste una procedura documentata per la pubblicizzazione/divulgazione alle terze parti del documento di cui al controllo precedente (**CTR-M1-PR.AT-3-01**) .	DGSIA/CISIA	Tutti gli UUGG e Data Center	
		PR.AT-4: I dirigenti ed i vertici aziendali comprendono ruoli e responsabilità	**Alta**	**PLC-116**	**PLC-116**	**CTR-M1-PR.AT-4-01**: Esiste una normativa interna documentata che istituisce e formalizza ruoli e responsabilità inerenti la cybersecurity per il personale dirigenziale.	DGSIA/CISIA	Tutti gli UUGG e Data Center	
					PLC-116	**CTR-M1-PR.AT-4-02**: Esiste un piano di formazione e aggiornamento su tematiche di cybersecurity Risk Management per il personale dirigenziale.	DGSIA/CISIA	Tutti gli UUGG e Data Center	
		PR.AT-5: Il personale addetto alla sicurezza fisica e delle	**Alta**	**PLC-116**	**PLC-116**	**CTR-M1-PR.AT-5-01**: Esiste una normativa interna documentata che istituisce e disciplina i ruoli e le responsabilità per il personale che tratta la sicurezza fisica dei sistemi e dei dati.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

		informazioni comprende i ruoli e le responsabilità			**PLC-116**	**CTR-M1-PR.AT-5-02**: Esiste un piano di formazione e aggiornamento su tematiche di cybersecurity per il personale addetto alla sicurezza fisica dei sistemi e dei dati.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
	Data Security (PR.DS): I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1: I dati e le informazioni memorizzate sono protette**	**Alta**	**PLC-025; PLC-037; PLC-038; PLC-045**	**PLC-038**	**CTR-M1-PR.DS-1-01**: Si applicano tecniche di cifratura per la protezione dei dati elaborati e mantenuti dai sistemi applicativi (SICP, SIPPI, TIAP, ecc.).	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-045; PLC-037	**CTR-M1-PR.DS-1-02**: Si applicano tecniche di cifratura per la protezione dei dati elaborati e mantenuti all'interno di PdL, workstation, laptop, server e altri dispositivi.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-025	**CTR-M1-PR.DS-1-03**: Si applicano tecniche di cifratura per la protezione delle credenziali memorizzate in tutti i sistemi IAA.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	DM 27.4.2009
					PLC-025	**CTR-M1-PR.DS-1-04**: Si utilizzano dispositivi HSM (Hardware Security Module) per la memorizzazione delle chiavi digitali utilizzate per le operazioni di cifratura e firma digitale delle credenziali memorizzate nel sistema ADN.	DGSIA	Tutti gli UUGG e Data Center	
					PLC-025	**CTR-M1-PR.DS-1-05**: Si utilizzano Smartcard (o dispositivi USB) per la memorizzazione delle chiavi digitali utilizzate per le operazioni di cifratura e firma digitale dall'utenze.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		PR.DS-2: I dati sono protetti durante la trasmissione	**Critica**	**PLC-066; PLC-067; PLC-068; PLC-086**	**PLC-067; PLC-068**	**CTR-M1-PR.DS-2-01**: Esiste una policy di sicurezza documentata per la trasmissione sicura (protocolli sicuri, cifratura) dei dati.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

					PLC-067; PLC-068	**CTR-M1-PR.DS-2-02**: Esiste una policy che prevede diversi livelli di protezione dei dati durante la trasmissione sulla base delle differenti tipologie del dato (riservato, riservatissimo, segreto, segretissimo).	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		PR.DS-3:Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazi	**Alta**	**PLC-060; PLC-073**	**PLC-073; PLC-060**	**CTR-M1-PR.DS-3-01**: Esiste una procedura interna documentata che disciplina il trasferimento fisico, la rimozione e la distruzione dei dispositivi fisici atti al trattamento e alla memorizzazione di dati.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-073	**CTR-M1-PR.DS-3-02**: Esiste una policy di dismissione dei dispositivi fisici che tiene conto della tipologia del dato trattato e memorizzato.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

		one di dati sono gestiti attraverso un processo formale							
		PR.DS-4: I sistemi hanno adeguate risorse a disposione per poter garantire la disponibilità	**Alta**	**PLC-059; PLC-087**	**PLC-059; PLC-087**	**CTR-M1-PR.DS-4-01**: Esiste una procedura interna documentata atta a verificare che le risorse a disposizione dei sistemi siano adeguate a garantire la disponibilità dei servizi e dei dati.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	CAD
		PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).	**Critica**	**PLC-024; PLC-030; PLC-036; PLC-037; PLC-039; PLC-040; PLC-045; PLC-046; PLC-048; PLC-069**	**PLC-039; PLC-036**	**CTR-M1-PR.DS-5-01** (ABSC 13.9.1): Si applicano tecniche atte ad assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 13.9.1)
					PLC-048; PLC-040	**CTR-M1-PR.DS-5-02** (ABSC 13.5.1): Nei casi in cui non è strettamente necessario l'utilizzo di dispositivi esterni (es., HD esterni, drive USB, etc.), si impiegano sistemi/configurazioni che impediscono la scrittura di dati su tali supporti.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 13.5.1)

					PLC-045; PLC-037	**CTR-M1-PR.DS-5-03** (ABSC 13.2.1): Si utilizzano sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 13.2.1)



		PR.DS-6: Vengono implementate tecniche di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni	**Critica**	**PLC-041; PLC-042; PLC-049; PLC-050; PLC-061; PLC-070; PLC-071; PLC-077**	**PLC-077**	**CTR-M1-PR.DS-6-01** (ABSC 3.5.1): Si implementano tecniche di controllo dell'integrità di file per verificare che il software e i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 3.5.1)
		PR.DS-7: Gli ambienti di sviluppo e test sono separati	**Alta**	**PLC-035; PLC-065**	**PLC-065; PLC-035**	**CTR-M1-PR.DS-7-01**: Esiste una procedura interna documentata per la gestione degli ambienti di sviluppo, test e produzione (es. modalità di separazione, ecc.).	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

		dall'ambiente di produzione			**PLC-035**	**CTR-M1-PR.DS-7-02**: È individuato un responsabile per ciascuno dei tre ambienti: sviluppo, test e produzione	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		PR.DS-8: Meccanismi per il controllo dell'integrità sono utilizzati per verificare l'integrità hardware.	**Non Selezionata**						
	Information Protection Processes and Procedures (PR.IP): Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative),	**PR.IP-1: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale**	**Critica**	**PLC-051; PLC-057; PLC-065; PLC-080**	**PLC-051; PLC-057**	**CTR-M1-PR.IP-1-01**: Esistono delle pratiche di riferimento documentate per la configurazione dei sistemi.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-065; PLC-051; PLC-057; PLC-080	**CTR-M1-PR.IP-1-02** (ABSC 3.1.2): Le configurazioni sicure standard utilizzate per proteggere i sistemi operativi e le applicazioni hanno subito adeguate operazioni di "hardening". Es.: eliminazione degli account non necessari, disattivazione o eliminazione dei servizi non necessari, configurazioni di stack e head non eseguibili, applicazione di patch, chiusura delle porte di rete non utilizzate, etc.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 3.1.2)
					PLC-051; PLC-057	**CTR-M1-PR.IP-1-03** (ABSC 3.3.2): Le immagini di installazione sono conservate in modo da garantirne l'integrità e la disponibilità solo agli utenti autorizzati.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 3.3.2)

	processi e procedure per gestire la protezione dei sistemi informativi e degli assets.								
		PR.IP-2: Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle).	**Non Selezionata**						
		PR.IP-3: Sono attivi processi di controllo della modifica delle configurazioni	**Alta**	**PLC-052; PLC-058**	**PLC-058; PLC-052**	**CTR-M1-PR.IP-3-01**: Esiste una procedura interna documentata che disciplina la gestione delle configurazioni dei sistemi.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		PR.IP-4: I backup delle informazioni sono eseguiti,	**Critica**	**PLC-059**	**PLC-059**	**CTR-M1-PR.IP-4-01** (ABSC 10.2.1): Viene verificata periodicamente l'utilizzabilità delle copie di backup mediante ripristino di prova.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 10.2.1)

		amministrati e verificati periodicame nte							
		PR.IP-5: Sono rispettate le policy ed i regolamenti relativi agli ambienti fisici in cui operano le risorse dell'organizz azione	**Alta**	**PLC-015; PLC-074; PLC-099**	**PLC-015; PLC-074; PLC-099**	**CTR-M1-PR.IP-5-01**: L'ufficio giudiziario e la sua sala server sono messi in protezione fisica contro le calamità naturali, attacchi o incidenti fisici.	DGSIA/CISIA/Assi stenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		PR.IP-6: I dati sono distrutti in conformità con le policy	**Critica**	**PLC-060 - PLC-073**	**PLC-073; PLC-060**	**CTR-M1-PR.IP-6-01**: Esiste una politica interna documentata che disciplina le modalità di distruzione dei dati, che tiene conto dei diversi livelli di riservatezza (riservato, riservatissimo, segreto, segretissimo).	DGSIA/CISIA/Assi stenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

		PR.IP-7: I processi di protezione sono migliorati in maniera continuativa	**Bassa**	**PLC-131**	**PLC-131**	**CTR-M1-PR.IP-7-01**: Esiste un processo documentato volto al miglioramento continuo dei processi di protezione dei dati e dei sistemi (assessment, aggiornamento, miglioramento, etc.)	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		PR.IP-8: L'efficacia delle tecnologie di protezione è condivisa con i referenti appropriati	**Alta**	**PLC-082; PLC-131**	**PLC-131; PLC-082**	**CTR-M1-PR.IP-8-01**: Sono previste delle procedure di assessment periodiche, relativamente all'analisi dell'efficacia delle tecnologie e dei processi adottati a protezione dei dati e dei sistemi. Tali attività vengono eseguite in collaborazione con esperti nazionali e internazionali in materia di protezione e sicurezza dei dati e dei sistemi.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		PR.IP-9: Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	**Alta**	**PLC-097; PLC-100; PLC-122**	**PLC-122; PLC-097**	**CTR-M1-PR.IP-9-01**: Esiste un piano di business continuity.	DGSIA/CISIA	Tutti gli UUGG e Data Center	
					PLC-122; PLC-100	**CTR-M1-PR.IP-9-02**: Esiste un piano di disaster recovery.	DGSIA/CISIA	Tutti gli UUGG e Data Center	

		PR.IP-10: I piani di risposta e recupero a seguito di incidenti/disastri sono verificati nel tempo	**Media**	**PLC-097; PLC-100**	**PLC-097**	**CTR-M1-PR.IP-10-01**: Esiste un processo documentato di verifica periodica del piano di business continuity.	DGSIA/CISIA	Tutti gli UUGG e Data Center	
					PLC-100	**CTR-M1-PR.IP-10-02**: Esiste un processo documentato di verifica periodica del piano di disaster recovery.	DGSIA/CISIA	Tutti gli UUGG e Data Center	
		PR.IP-11: Le problematiche inerenti la cybersecurity sono incluse nei processi di gestione del personale (es: screening, licenziamenti)	**Alta**	**PLC-116**	**PLC-116**	**CTR-M1-PR.IP-11-01**: Esiste un codice deontologico in materia di cybersecurity sottoscritto dal personale.	DGSIA/CISIA	Tutti gli UUGG e Data Center	
		PR.IP-12:Viene sviluppato e implementato un piano di gestione delle	**Critica**	**PLC-064; PLC-065; PLC-118**	**PLC-064**	**CTR-M1-PR.IP-12-01** (ABSC 4.10.1): Si valutano, nell'ambiente di test, le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 4.10.1)

		vulnerabilità							
	Maintenance (PR.MA): La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:La manutenzione e la riparazione delle risorse e dei sistemi è svolta e registrata in modo tempestivo e portata a termine attraverso l'utilizzo di strumenti controllati ed autorizzati**	**Critica**	**PLC-053; PLC-054; PLC-058; PLC-065**	**PLC-058; PLC-053; PLC-054**	**CTR-M1-PR.MA-1-01**: Esiste una procedura interna documentata che disciplina la manutenzione e la riparazione dei sistemi e dei dispositivi.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

		PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	**Alta**	**PLC-031; PLC-053; PLC-054; PLC-055; PLC-056**	**PLC-031; PLC-053; PLC-054; PLC-055; PLC-056**	**CTR-M1-PR.MA-2-01**: Esiste una procedura interna documentata che disciplina la gestione e il controllo della manutenzione remota dei sistemi e dei dispositivi.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
	Protective Technology (PR.PT): Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-1: Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi**	**Alta**	**PLC-053; PLC-054; PLC-058; PLC-091; PLC-092; PLC-096**	**PLC-058; PLC-053; PLC-054; PLC-096; PLC-091; PLC-092**	**CTR-M1-PR.PT-1-01**: Esiste una procedura interna documentata che disciplina la gestione e il controllo dei log dei sistemi.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		PR.PT-2: I supporti di memorizzazione	**Critica**	**PLC-043; PLC-048; PLC-057**	**PLC-057**	**CTR-M1-PR.PT-2-01**: Esiste una politica di sicurezza documentata che regola la protezione e l'utilizzo dei supporti di memorizzazione removibili.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

		removibili sono protetti ed il loro uso è ristretto in accordo alle policy				
		PR.PT-3: L'accesso alle risorse e ai sistemi è limitato secondo il principio di minima funzionalità	**Non Selezionata**			

		PR.PT-4: Le reti di comunicazione e controllo sono protette	**Critica**	**PLC-057; PLC-089; PLC-090**	**PLC-090**	**CTR-M1-PR.PT-4-01**: Le reti sono classificate sulla base del livello di segretezza del dato trattato dai sistemi presenti nella rete o trasportato dalla stessa.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-090	**CTR-M1-PR.PT-4-02**: Si implementano meccanismi (hardware o software) di cifratura dell'informazione trasmessa da e verso reti interne classificate al più alto livello di segretezza.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-090	**CTR-M1-PR.PT-4-03**: Esistono dispositivi firewall, opportunamente configurati, che controllano il traffico tra le diverse tipologie di rete (si veda **CTR-M1-PR.PT-4-01**).	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-057	**CTR-M1-PR.PT-4-04** (CIS CSC 9.2): I firewall installati sugli host sono configurati in modo da scartare per default tutto il traffico di rete eccetto quello associato a porte e servizi esplicitamente autorizzati.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

		PR.PT-5: I sistemi operano in stati funzionali predefiniti per ottenere la disponibilità (ad esempio sotto costrizione, sotto attacco, durante il recupero, normale funzionalità).	**Media**	**PLC-098**	**PLC-098**	**CTR-M1-PR.PT-5-01**: I sistemi vengono progettati e messi in opera con diversi stati funzionali predefiniti, di modo da garantirne la disponibilità in situazioni critiche, quali: sotto attacco e durante un ripristino.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
DETECT (DE)	**Anomalies and Events (DE.AE): Le attività anomale sono rilevate tempestivamente e il loro impatto potenziale viene analizzato.**	**DE.AE-1: sono definite, rese note e gestite delle pratiche di riferimento (c.d. baseline) inerenti l'utilizzo della rete ed i flussi informativi attesi per utenti e sistemi**	**Media**	**PLC-072; PLC-075**	**PLC-072; PLC-075**	**CTR-M1-DE.AE-1-01** (ABSC 13.3.1): Sono impiegati sul perimetro della rete strumenti automatici che monitorano tentativi di esfiltrare informazioni sensibili ed eventualmente bloccano il trasferimento di tali informazioni fuori dal perimetro della rete e segnalano l'incidente al personale di sicurezza.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 13.3.1)
					PLC-075	**CTR-M1-DE.AE-1-02** (ABSC 13.7.1): Il traffico uscente dal perimetro della rete viene monitorato per bloccare ogni impiego non previsto e non autorizzato di crittografia (gli attacchi spesso sfruttano canali cifrati per non essere rilevati dai dispositivi di sicurezza di rete).	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 13.7.1)

		DE.AE-2: Gli eventi rilevati vengono analizzati per comprendere gli obiettivi e le metodologie dell'attacco	**Alta**	**PLC-093; PLC-094**	**PLC-093; PLC-094**	**CTR-M1-DE.AE-2-01** (ABSC 8.1.3): Gli eventi rilevati dagli strumenti firewall ed IPS installati sono inviati ad un repository centrale (es. syslog) dove sono stabilmente archiviati.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 8.1.3) DM 27.4.2009
					PLC-093	**CTR-M1-DE.AE-2-02 (NIST SI-4 (24)):** Gli eventi rilevati vengono analizzati per determinare, raccogliere ed eventualmente distribuire indicatori di compromissione (IOC).	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		DE.AE-3: Le informazioni relative agli eventi sono aggregate e correlate da sensori e sorgenti multiple	**Alta**	**PLC-072; PLC-075; PLC-094**	**PLC-072; PLC-075; PLC-094**	**CTR-M1-DE.AE-3-01** (CIS CSC 6.6): È presente un SIEM (Security Information and Event Management) che monitora, aggrega e correla gli eventi provenienti da molteplici sorgenti, quali host (macchine fisiche e virtuali), apparati di rete (router, switch, ecc.), firewall, IDS e IPS.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		DE.AE-4: Viene determinato l'impatto di un evento	**Media**	**PLC-093**	**PLC-093**	**CTR-M1-DE.AE-4-01**: Gli eventi rilevati sono analizzati al fine di determinarne l'impatto.	DGSIA/CISIA	Tutti gli UUGG e Data Center	
		DE.AE-5: Vengono definite delle soglie di allerta per gli incidenti	**Media**	**PLC-093**	**PLC-093**	**CTR-M1-DE.AE-5-01**: Sono definite delle soglie sugli eventi rilevati che se superate scatenano degli alert e riportano l'incidente al team di risposta agli incidenti.	DGSIA/CISIA	Tutti gli UUGG e Data Center	

	Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati periodicamente per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity**	**Critica**	**PLC-076; PLC-077**	**PLC-076**	**CTR-M1-DE.CM-1-01** (CIS CSC 12.3): Vengono impiegati IDS (Intrusion Detection System) network-based (oltre agli eventuali host-based) per rilevare eventi di cybersecurity monitorando la rete.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-076	**CTR-M1-DE.CM-1-02**: In caso di utilizzo di blacklist, esiste una procedura documentata che disciplina i ruoli e le responsabilità dei gestori della blacklist di url e le modalità di gestione della stessa.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		DE.CM-2: Viene svolto il monitoraggio degli spazi fisici per rilevare	**Alta**	**PLC-016; PLC-078**	**PLC-016; PLC-078**	**CTR-M1-DE.CM-2-01** (NIST PE-6): I punti di accesso fisico ai locali dove risiedono i sistemi informatici vengono monitorati 24 ore su 24 e 7 giorni su 7 da personale di sicurezza e/o attraverso apparati di sorveglianza e allarmi.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

		potenziali eventi di cybersecurity			**PLC-016; PLC-078**	**CTR-M1-DE.CM-2-02** (NIST PE-6 PE-8): Gli accessi fisici del personale ed eventuali visitatori ai locali dove risiedono i sistemi informatici vengono monitorati e registrati in appositi log.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		DE.CM-3: Viene svolto il monitoraggio del personale per rilevare potenziali eventi di cybersecurity	**Alta**	**PLC-088; PLC-092**	**PLC-088; PLC-092**	**CTR-M1-DE.CM-3-01** (ABSC 5.5.1): I tentativi falliti di accesso con un'utenza amministrativa sono tracciati nei log.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 5.5.1) DM 27.4.2009
					PLC-088	**CTR-M1-DE.CM-3-02** (CIS CSC 16.4): Gli account utente vengono regolarmente monitorati e viene effettuato il log-off automatico degli utenti dopo un determinato tempo di inattività.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-088	**CTR-M1-DE.CM-3-03**: I tentativi falliti di accesso delle utenze del personale sono tracciati nei log.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-088	**CTR-M1-DE.CM-3-04** (CIS CSC 16.6): Viene effettuato il monitoraggio degli account del personale al fine di rilevare quegli account che sono inattivi per un lungo periodo. Tali utenze vengono segnalate al personale di amministrazione che provvede prontamente a disabilitarle se non più necessarie.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		DE.CM-4: Il codice malevolo viene rilevato	**Critica**	**PLC-043; PLC-055; PLC-056; PLC-075; PLC-077**	**PLC-075; PLC-055 PLC-056**	**CTR-M1-DE.CM-4-01** (ABSC 8.5.1): Vengono impiegati strumenti anti-malware network-based che operano sull'intero traffico di rete per rilevare e filtrare il codice malevolo prima che raggiunga gli host.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 8.5.1)

		DE.CM-5: Il codice non autorizzato su dispositivi mobili viene rilevato	**Alta**	**PLC-043; PLC-055; PLC-056**	**PLC-043; PLC-055; PLC-056**	**CTR-M1-DE.CM-5-01** (CIS CSC 8.1): Su tutti i dispositivi mobili (laptop o smartphone) sono installati strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali).	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-043	**CTR-M1-DE.CM-5-02**: Gli strumenti di cui al controllo precedente sono mantenuti aggiornati in modo automatico.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		DE.CM-6: Viene svolto il monitoraggio delle attività dei	**Non Selezionata**						

		service provider esterni per rilevare potenziali eventi di cybersecurity							
		DE.CM-7: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati.	**Critica**	**PLC-044; PLC-079; PLC-081; PLC-094**	**PLC-081**	**CTR-M1-DE.CM-7-01** (ABSC 8.3.2): L'uso e i tentativi di utilizzo di dispositivi esterni non autorizzati sono monitorati.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 8.3.2)
					PLC-081	**CTR-M1-DE.CM-7-02:** Viene rilevato e impedito l'accesso alla rete ai dispositivi (anche quelli wireless) non autorizzati.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-094	**CTR-M1-DE.CM-7-03 (CIS CSC 6.2):** Per ogni software installato viene verificato che la configurazione del processo di logging sia tale che tutte le informazioni rilevanti e utili a rilevare eventi di cybersecurity vengano registrate.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		DE.CM-8: Vengono svolte scansioni per l'identificazione di vulnerabilità	**Critica**	**PLC-082**	**PLC-082**	**CTR-M1-DE.CM-8-01** (ABSC 4.1.2): La ricerca delle vulnerabilità tramite gli strumenti di scansione delle vulnerabilità viene effettuata su base periodica (settimanale, o più frequente, e comunque commisurata alla complessità dell'infrastruttura).	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 4.1.2)

					PLC-082	**CTR-M1-DE.CM-8-02** (ABSC 4.3.1): Gli strumenti di scansione delle vulnerabilità vengono eseguiti, sia da locale sia da remoto, in modalità privilegiata da un account dedicato che non viene utilizzato per nessun altra attività di amministrazione.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 4.3.1)
	Detection Processes (DE.DP): Sono adottati, mantenuti e verificati nel tempo i processi e le procedure di monitoraggio per assicurare una tempestiva e adeguata comprensione degli eventi di sicurezza	**DE.DP-1: Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability**	**Alta**	**PLC-072; PLC-079; PLC-083**	**PLC-072; PLC-083**	**CTR-M1-DE.DP-1-01**: È nominato un responsabile per i processi di monitoraggio della rete e dei sistemi, analisi degli eventi e reporting.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-079	**CTR-M1-DE.DP-1-02** (ABSC 8.2.1): Tutti gli strumenti di monitoraggio, come firewall personali, anti-virus, anti-spyware e IPS host-based, sono gestiti centralmente e non è consentito agli utenti normali alterarne la configurazione.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	AgID (ABSC 8.2.1)
		DE.DP-2: Le attività di monitoraggio soddisfano tutti i requisiti applicabili	**Non selezionata**						
		DE.DP-3: I processi di monitoraggio vengono testati	**Alta**	**PLC-075; PLC-082; PLC-095**	**PLC-095**	**CTR-M1-DE.DP-3-01** (CIS CSC 6.3): Viene verificato periodicamente che tutti i sistemi abbiano sufficiente spazio di storage per i log.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-075; PLC-082	**CTR-M1-DE.DP-3-02** (NIST SI-4): Tutti gli strumenti e i sistemi di monitoraggio (quali firewall, IDS, IPS, SIEM, ecc.) sono testati su base regolare, per esempio attraverso test di penetrazione.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

		DE.DP-4: L'informazione relativa agli eventi rilevati è comunicata a tutte le parti interessate	**Alta**	**PLC-084; PLC-085**	**PLC-084**	**CTR-M1-DE.DP-4-01**: È prevista entro il 6 maggio 2018 (data del recepimento della direttiva UE 2016/680) l'adozione di un piano per notificare tutte le violazioni di dati personali all'autorità di controllo senza ingiustificato ritardo, ai sensi dell'articolo 30 della Direttiva UE 2016/680.	DGSIA	Tutti gli UUGG e Data Center	D.Lgs. 196/2003 GDPR Dir. UE 2016/680
					PLC-084	**CTR-M1-DE.DP-4-02**: È prevista entro il 6 maggio 2018 (data del recepimento della direttiva UE 2016/680) l'adozione di un piano per comunicare, senza ingiustificato ritardo, la violazioni di dati personali direttamente all'interessato qualora la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ai sensi dell'articolo 31 della Direttiva UE 2016/680.	DGSIA	Tutti gli UUGG e Data Center	GDPR Dir. UE 2016/680
					PLC-085	**CTR-M1-DE.DP-4-03**: Le informazioni relative agli attacchi sono condivise con i CERT ed il Nucleo per la Sicurezza Cibernetica ai sensi della Direttiva 1/8/2015 del Presidente del Consiglio dei ministri.	DGSIA/CISIA	Tutti gli UUGG e Data Center	DPCM 01/08/2015
		DE.DP-5: I processi di monitoraggio sono oggetto di periodici miglioramenti e perfezionamenti	**Alta**	**PLC-083; PLC-094**	**PLC-094; PLC-083**	**CTR-M1-DE.DP-5-01**: Esiste una policy di miglioramento continuo del processo di monitoring che si avvale anche delle conoscenze acquisite dall'analisi degli incidenti passati.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

RESPOND (RS)	**Response Planning (RS.RP): Procedure e processi di risposa sono eseguiti e mantenuti per assicurare la tempestiva risposta agli eventi di cybersecurity rilevati.**	**RC.RP-1: Esiste un piano di ripristino (recovery plan) e questo viene eseguito durante o dopo un incidente**	**Alta**	**PLC-084; PLC-100**	**PLC-084; PLC-100**	**CTR-M1-RS.RP-1-01 (CIS CSC 19.1):** Esiste un piano di risposta agli incidenti.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
	Communications (RS.CO): Le attività di risposta sono coordinate con le parti interne ed esterne, per includere eventuale supporto da parte degli organi di legge o dalle forze dell'ordine.	**RS.CO-1: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente**	**Alta**	**PLC-100; PLC-106**	**PLC-100**	**CTR-M1-RS.CO-1-01**: Esiste un team di risposta agli incidenti.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-106; PLC-100	**CTR-M1-RS.CO-1-02** (CIS CSC 19.1): Il piano di risposta identifica e definisce i ruoli del personale di risposta agli incidenti.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-106; PLC-100	**CTR-M1-RS.CO-1-03** (CIS CSC 19.2): Il piano di risposta assegna le responsabilità del personale di risposta agli incidenti.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-100	**CTR-M1-RS.CO-1-04** (CIS CSC 19.6): Sono pubblicate e note al personale tutte le informazione e le procedure per comunicare gli incidenti ai responsabili del team di risposta degli incidenti.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

		RS.CO-2: Sono stabiliti dei criteri per documentare gli incidenti/eventi	**Alta**	**PLC-084; PLC-096; PLC-100**	**PLC-100; PLC-084; PLC-096**	**CTR-M1-RS.CO-2-01** (CIS CSC 19.4): Esiste una procedura documentata per riportare gli incidenti, che individui il tipo di informazioni che devono essere incluse nella notifica dell'incidente.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	GDPR
		RS.CO-3: Le informazioni sono condivise in maniera coerente con il piano di risposta	**Non Selezionata**						
		RS.CO-4: Il coordinamento con le parti interessate dell'organizzazione avviene in coerenza con i piani di risposta	**Alta**	**PLC-084; PLC-100**	**PLC-100; PLC-084**	**CTR-M1-RS.CO-4-01**: Esiste una procedura documentata che disciplina il coordinamento tra le parti interessate, in caso di incidente, in coerenza al piano di risposta.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

		RS.CO-5: E' attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awareness)	**Alta**	**PLC-096; PLC-101; PLC-120**	**PLC-101; PLC-120**	**CTR-M1-RS.CO-5-01** (NIST SP 800-53 IR.7): Ci si avvale di organizzazioni esterne (es. CERT) a supporto del team di risposta agli incidenti.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-096; PLC-101	**CTR-M1-RS.CO-5-02** (NIST SP 800-53 IR.6.7): Esiste un processo documentato per la condivisione delle informazioni inerenti un incidente con le parti esterne interessate (es. invio informazioni al CERT).	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
	Analysis (RS.AN): Vengono condotte analisi per assicurare un'adeguata riposta e supporto alle attività di ripristino	**RS.AN-1: Le notifiche provenienti dai sistemi di monitoraggio vengono sempre visionate e analizzate**	**Alta**	**PLC-075; PLC-084**	**PLC-075; PLC-084**	**CTR-M1-RS.AN-1-01** (ISO 27001 A.12.4.1): Esiste un sistema di reportistica degli eventi di sicurezza provenienti dai sistemi di monitoraggio che permette l'analisi e la gestione (anche la visualizzazione) degli stessi.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

		RS.AN-2: Viene compreso l'impatto di ogni incidente	**Alta**	**PLC-084; PLC-101**	**PLC-084; PLC-101**	**CTR-M1-RS.AN-2-01** (ISO 27001 A.16.1.4): Viene valutato l'impatto degli incidenti.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		RS.AN-3: A seguito di un incidente viene svolta un'analisi forense	**Alta**	**PLC-094; PLC-101**	**PLC-094; PLC-101**	**CTR-M1-RS.AN-3-01** (ISO 27001 A.16.1.7): Esistono delle procedure documentate per identificare, collezionare ed acquisire informazioni che possono essere usate come evidenza di un attacco.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		RS.AN-4: Gli incidenti sono categorizzati in maniera coerente con i piani di risposta	**Non Selezionata**						
	Mitigation (RS.MI): Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i sui effetti e per rimuovere l'incidente.	**RS.MI-1: In caso di incidente vengono messe in atto procedure atte a contenerne l'impatto**	**Alta**	**PLC-084; PLC-100**	**PLC-100; PLC-084**	**CTR-M1-RS.MI-1-01** (ISO 27001 A.17.1.1): In caso di incidente viene tempestivamente applicato il piano di risposta associato per contenerne l'impatto e/o mitigarne gli effetti.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

		RS.MI-2: In caso di incidente vengono messe in atto procedure atte a mitigarne gli effetti	**Non Selezionata**						
		RS.MI-3: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato	**Critica**	**PLC-118; PLC-120**					
	Improvements (RS.IM): Le attività di risposta sono migliorate incorporando le "lesson learned" da attività precedenti di monitoraggio e risposta.	**RS.IM-1: I piani di risposta agli incidenti tengono in considerazione le esperienze passate (lesson learned)**	**Alta**	**PLC-059; PLC-100; PLC-101; PLC-102**	**PLC-101**	**CTR-M1-RS.IM-1-01:** Gli incidenti sono analizzati e classificati al fine di aggiornare e migliorare il piano di risposta.	CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-059; PLC-100; PLC-102	**CTR-M1-RS.IM-1-02** (ISO 27001 A.16.1.6): Esiste una procedura documentata che disciplina l'aggiornamento del piano di risposta agli incidenti in considerazione delle esperienze passate.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		RS.IM-2: Le strategie di risposta agli incidenti sono aggiornate	**Alta**	**PLC-059; PLC-100**	**PLC-059; PLC-100**	**CTR-M0-RS.IM-2-01:** Il piano di risposta è aggiornato regolarmente.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	

RECOVER (RC)	**Recovery Planning (RC.RP): I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un tempestivo recupero dei sistemi o asset coinvolti da un evento di cybersecurity.**	**RC.RP-1: Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un evento**	**Critica**	**PLC-102; PLC-103; PLC-048**	**PLC-102;**	**CTR-M1-RC.RP-1-01**: Esiste un piano di ripristino.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
	Improvements (RC.IM): I piani di ripristino ed i relativi processi sono migliorati tenendo conto delle "lesson learned" per le attività future.	**RC.IM-1: I piani di riprisitino tengono in considerazione le esperienze passate (lesson learned)**	**Alta**	**PLC-059; PLC-102**	**PLC-059; PLC-102**	**CTR-M1-RC.IM-1-01:** Le esperienze passate vengono utilizzate al fine di aggiornare e migliorare il piano di ripristino.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
					PLC-102	**CTR-M1-RS.IM-1-02**: Esiste una procedura documentata che disciplina l'aggiornamento del piano di ripristino che tiene in considerazione le esperienze passate.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
		RC.IM-2: Le strategie di recupero sono aggiornate	**Alta**	**PLC-059; PLC-102**	**PLC-059; PLC-102**	**CTR-M1-RC.IM-2-01**: Il piano di ripristino è aggiornato regolarmente.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	
	Communications (RC.CO): Le attività di ripristino a seguito di un incidente sono coordinate con le parti interne ed esterne, come ad	**RC.CO-1: A seguito di un incidente vengono gestite le pubbliche relazioni**	**Alta**	**PLC-084; PLC-105**	**PLC-084; PLC-105**	**CTR-M1-RC.CO-1-01**: Esiste una procedura documentata di gestione delle pubbliche relazione in seguito ad un incidente.	DGSIA	Uffici centrali DGSIA	

	esempio, le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT.	**RC.CO-2: A seguito di un incidente viene ripristinata la reputazione**	**Non Selezionata**						
		RC.CO-3: Le attività di recupero condotte a seguito di un incidente vengono comunicate alle parti interessate interne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione	**Alta**	**PLC-059; PLC-104**	**PLC-059; PLC-104**	**CTR-M1-RC.CO-3-01**: Il personale che esegue le operazioni di ripristino in risposta ad un incidente produce un report dettagliato in cui vengono documentate le attività eseguite. Tale report viene condiviso con tutte le parti interne interessate.	DGSIA/CISIA/Assistenza Tecnica (esterna)	Tutti gli UUGG e Data Center	