	DIREZIONE GENERALE UNITA' PRIVACY	Rev. 2.2 21/12/2022
ID misura	**Misura per designazione**	**Riferimenti a standard**
ID.AM-1	I sistemi e gli apparati fisici in uso nell'organizzazione devono essere censiti	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5 Misure Minime AgID ABSC 1
ID.AM-2	Le piattaforme e le applicazioni software in uso nell'organizzazione devono essere censite	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5 Misure Minime AgID ABSC 2
ID.AM-3	I flussi di dati e comunicazioni inerenti l'organizzazione devono essere identificati	CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 Misure Minime AgID ABSC 5.1.4, 13.3.1, 13.4.1, 13.6, 13.7.1, 13.8.1
ID.AM-4	I sistemi informativi esterni all'organizzazione devono essere catalogati	CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
ID.AM-5	Le risorse (es: hardware, dispositivi, dati, allocazione temporale, personale e software) devono essere prioritizzate in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione	CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6 Misure Minime AgID ABSC 13.1.1, 13.2.1
ID.AM-6	I ruoli e le responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner) devono essere definiti e resi noti	CIS CSC 17, 19 COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 D.Lgs. 18/5/2018 n. 65 Art. 16(2)-(4) Misure Minime AgID ABSC 5.2.1, 5.4, 5.10, 8.11.1
DP-ID.AM-7	I ruoli e le responsabilità inerenti al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner) devono essere definiti e resi noti	GDPR - Artt. 24, 26-29, 37-39 D.Lgs. 30/6/2003 n. 196 Artt. 2-quaterdecies, 2-quinquiesdecies, 2-sexiesdecies ISO/IEC 29100:2011 4.2, 4.3, 5.10
DP-ID.AM-8	I trattamenti di dati personali devono essere identificati e catalogati	GDPR - Art. 30 ISO/IEC 29100:2011 4.4
ID.BE-4	Le interdipendenze e le funzioni fondamentali per la fornitura di servizi critici devono essere identificate e rese note	COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-5	I requisiti di resilienza a supporto della fornitura di servizi critici per tutti gli stati di esercizio (es. sotto stress/attacco, in fase di recovery, normale esercizio) devono essere identificati e resi noti	COBIT 5 BAI03.02, DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13, SA-14
ID.GV-1	Una policy di cybersecurity deve essere identificata e resa nota	CIS CSC 19 COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02 ISA 62443-2-1:2009 4.3.2.6 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 4 - 1 controls from all security control families D.Lgs. 18/5/2018 n. 65 Artt. 13(2), 15(2)
ID.GV-2	Ruoli e responsabilità inerenti la cybersecurity devono essere coordinati ed allineati con i ruoli interni ed i partner esterni	CIS CSC 19 COBIT 5 APO01.02, APO10.03, APO13.02, DSS05.04 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1 NIST SP 800-53 Rev. 4 PS-7, PM-1, PM-2
ID.GV-4	La governance ed i processi di risk management devono includere la gestione dei rischi legati alla cybersecurity	COBIT 5 EDM03.02, APO12.02, APO12.05, DSS04.02 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 ISO/IEC 27001:2013 Clause 6 NIST SP 800-53 Rev. 4 SA-2, PM-3, PM-7, PM-9, PM-10, PM-11 D.Lgs. 18/5/2018 n. 65 Artt. 12(1), 14(1)
ID.RA-1	Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione devono essere identificate e documentate	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 Misure Minime AgID ABSC 4.1.1, 4.1.2, 4.6.1
ID.RA-2	L'organizzazione deve ricevere informazioni su minacce, vulnerabilità ed altri dati configurabili come Cyber Threat Intelligence da fonti esterne (e.g. CERT, fonti aperte, forum di information sharing)	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
ID.RA-3	Le minacce, sia interne che esterne, devono essere identificate e documentate	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
ID.RA-5	Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti devono essere utilizzati per determinare il rischio	CIS CSC 4 COBIT 5 APO12.02 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16 Misure Minime AgID ABSC 4.8.1
ID.RA-6:	Le risposte al rischio devono essere identificate e prioritizzate	CIS CSC 4 COBIT 5 APO12.05, APO13.02 ISO/IEC 27001:2013 Clause 6.1.3 NIST SP 800-53 Rev. 4 PM-4, PM-9
ID.RM-1	I processi di risk management devono essere stabiliti, gestiti e concordati tra i responsabili dell'organizzazione (c.d. stakeholder)	CIS CSC 4 COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3 NIST SP 800-53 Rev. 4 PM-9 D.Lgs. 18/5/2018 n. 65 Artt. 12(1), 14(1), 14(13)
ID.RM-2	Il rischio tollerato dall'organizzazione deve essere identificato ed espresso chiaramente	COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.2.6.5 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 PM-9 D.Lgs. 18/5/2018 n. 65 Artt. 12(1), 14(1), 14(13)
ID.RM-3:	Il rischio tollerato deve essere determinato tenendo conto del ruolo dell'organizzazione come infrastruttura critica e dei rischi specifici presenti nel settore industriale di appartenenza	COBIT 5 APO12.02 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 SA-14, PM-8, PM-9, PM-11 D.Lgs. 18/5/2018 n. 65 Artt. 12(1), 14(1), 14(13)
ID.SC-1	I processi di gestione del rischio inerenti la catena di approvvigionamento cyber devono essere identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione	CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9
ID.SC-2	I fornitori e i partner terzi di sistemi informatici, componenti e servizi devono essere identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber	COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
ID.SC-3	I contratti con i fornitori e i partner terzi devono essere utilizzati per realizzare appropriate misure progettate per rispettare gli obiettivi del programma di cybersecurity dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento cyber	COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3 NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM-9
ID.SC-4	Fornitori e partner terzi devono essere regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali	COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 ISA 62443-2-1:2009 4.3.2.6.7 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
ID.SC-5	La pianificazione e la verifica della risposta e del ripristino devono essere condotti con i fornitori e i partner terzi	CIS CSC 19, 20 COBIT 5 DSS04.04 ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
DP-ID.DM-1	Il ciclo di vita dei dati deve essere definito e documentato	GDPR - Art. 5,6,9-11, 30
DP-ID.DM-2:	I processi riguardanti l'informazione dell'interessato in merito al trattamento dei dati devono essere definiti, implementati e documentati	GDPR - Artt. 12-14 ISO/IEC 29100:2011 5.2, 5.8 ISO/IEC 29151:2017 A.3, A.9 ISO/IEC 27018:2014 A.1, A.7
DP-ID.DM-3	I processi di raccolta e revoca del consenso dell'interessato al trattamento di dati devono essere definiti, implementati e documentati	GDPR - Artt. 7, 8 D.Lgs. 30/6/2003 n. 196 Art. 2-quinquies ISO/IEC 29100:2011 5.2 ISO/IEC 29151:2017 A.3 ISO/IEC 27018:2014 A.1
DP-ID.DM-4	I processi per l'esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) dell'interessato devono essere definiti, implementati e documentati	GDPR - Art 15- 22 D.Lgs. 30/6/2003 n. 196 Art. 2-terdecies ISO/IEC 29100:2011 5.4, 5.5, 5.6, 5.7, 5.8, 5.9 ISO/IEC 29151:2017 A.5, A.6, A.7, A.8, A.9, A.10 ISO/IEC 27018:2014 A.3, A.4, A.5, A.6, A.7, A.8
DP-ID.DM-5	I processi di trasferimento dei dati in ambito internazionale devono essere definiti, implementati e documentati	GDPR - Artt. 44-49 ISO/IEC 29100:2011 4.5
PR.AC-CDM1	Le credenziali di accesso ai sistemi devono essere nominative e le password devono sottostare a una policy che imponga la definizione di password con una complessità minima tale da renderle sicure	Controllo inserito dal Comune di Milano
PR.AC-1	Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati devono essere amministrate, verificate, revocate e sottoposte a audit sicurezza	CIS CSC 1, 5, 15, 16 COBIT 5 DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 5.6.1, 5.7, 5.8.1, 5.11 GDPR - Artt. 25, 32 ISO/IEC 29100:2011 5.11
PR.AC-2	L'accesso fisico alle risorse deve essere protetto e amministrato	COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 5.11.2, 10.4.1 GDPR - Art. 32 ISO/IEC 29100:2011 5.11

PR.AC-3:	L'accesso remoto alle risorse deve essere amministrato	CIS CSC 12 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 3.4.1, 8.3.2 GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.AC-4	I diritti di accesso alle risorse e le relative autorizzazioni devono essere amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	CIS CSC 3, 5, 12, 14, 15, 16, 18 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 5.1.1, 5.1.2, 5.1.3, 13.9.1 GDPR - Artt. 25, 32 ISO/IEC 29100:2011 5.11
PR.AC-5	L'integrità di rete deve essere protetta (es. segregazione di rete, segmentazione di rete)	CIS CSC 9, 14, 15, 18 COBIT 5 DSS01.05, DSS05.02 ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 13.3.1 GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.AC-7:	Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti, i dispositivi e altri asset devono essere commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)	CIS CSC 1, 12, 15, 16 COBIT 5 DSS05.04, DSS05.10, DSS06.10 ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.AT-1	Tutti gli utenti devono essere informati e addestrati	CIS CSC 17, 18 COBIT 5 APO07.03, BAI05.07 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 NIST SP 800-53 Rev. 4 AT-2, PM-13 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 8.7.2, 8.7.3, 8.7.4
PR.AT-2	Gli utenti dotati di privilegi (es. amministratori di sistema) devono essere coscienti dei propri ruoli e responsabilità	CIS CSC 5, 17, 18 COBIT 5 APO07.02, DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 5.2.1, 5.6.1, 5.7.1, 5.7.2, 5.7.3, 5.7.6, 5.8.1, 5.9.1, 5.10.3, 5.10.4, 5.11.1
PR.AT-3	Tutte le terze parti (es. fornitori, clienti, partner) devono essere coscienti dei propri ruoli e responsabilità	CIS CSC 17 COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2 NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13)
PR.AT-4	I dirigenti e i vertici aziendali devono essere coscienti del proprio ruoli e responsabilità	CIS CSC 17, 19 COBIT 5 EDM01.01, APO01.02, APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13)
PR.AT-5	Il personale addetto alla sicurezza fisica e alla cybersecurity deve essere cosciente dei propri ruoli e responsabilità	CIS CSC 17 COBIT 5 APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13)
PR.PT-CDM1	Tutti i dispositivi client (postazioni di lavoro e dispositivi mobili) devono essere dotati di software per garantire la endpoint security (antivirus o antimalware)	Controllo inserito dal Comune di Milano
PR.DS-1	I dati memorizzati devono essere protetti	CIS CSC 13, 14 COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 ISA 62443-3-3:2013 SR 3.4, SR 4.1 ISO/IEC 27001:2013 A.8.2.3 NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 13.3.1 GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.DS-2	La trasmissione di dati deve avvenire in maniera protetta	CIS CSC 13, 14 COBIT 5 APO01.06, DSS05.02, DSS06.06 ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 3.3.2 GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.DS-3	I processi di trasferimento fisico, di rimozione e di distruzione dei dispositivi atti alla memorizzazione di dati devono essere gestiti attenendosi a un processo formale	CIS CSC 1 COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.1 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.DS-4	I sistemi devono disporre in maniera adeguata di risorse in modo da garantirne la disponibilità	CIS CSC 1, 2, 13 COBIT 5 APO13.01, BAI04.04 ISA 62443-3-3:2013 SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.DS-5	Devono essere implementate tecniche di protezione (es. controllo degli accessi) per contrastare data leak	CIS CSC 13 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ISA 62443-3-3:2013 SR 5.2 ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 13.2.1, 13.7.1, 13.8.1, 13.9.1 GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.DS-6	Devono essere impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e informazioni	CIS CSC 2, 3 COBIT 5 APO01.06, BAI06.01, DSS06.02 ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 NIST SP 800-53 Rev. 4 SC-16, SI-7 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 3.5.1, 3.5.2, 10.3.1 GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.DS-7	Gli ambienti di sviluppo e test devono essere separati dall'ambiente di produzione	CIS CSC 18, 20 COBIT 5 BAI03.08, BAI07.04 ISO/IEC 27001:2013 A.12.1.4 NIST SP 800-53 Rev. 4 CM-2 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 4.10.1, 8.2.3
PR.IP-1	Devono essere definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	CIS CSC 3, 9, 11 COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 3.1.1, 3.1.2, 3.2.1, 5.3.1, 8.4 GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.IP-2	Deve essere implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle)	CIS CSC 18 COBIT 5 APO13.01, BAI03.01, BAI03.02, BAI03.03 ISA 62443-2-1:2009 4.3.4.3.3 ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 NIST SP 800-53 Rev. 4 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 3.1.3, 3.2.2, 3.3 GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.IP-3	Devono essere attivi processi di controllo della modifica di configurazioni	CIS CSC 3, 11 COBIT 5 BAI01.06, BAI06.01 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 3.2.3, 3.5.3, 3.5.4, 3.6.1, 3.7.1, 5.4, 8.2.1, 8.2.2 GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.IP-4	I backup delle informazioni devono essere eseguiti, amministrati e verificati	CIS CSC 10 COBIT 5 APO13.01, DSS01.01, DSS04.07 ISA 62443-2-1:2009 4.3.4.3.9 ISA 62443-3-3:2013 SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 10.1, 10.2.1, 10.4.1 GDPR - Art. 32 ISO/IEC 29100:2011 5.11

PR.IP-5	Devono essere rispettate le policy e i regolamenti relativi agli ambienti fisici in cui operano le risorse dell'organizzazione	COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 10.4.1 GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.IP-6	I dati devono essere distrutti in conformità con le policy	COBIT 5 BAI09.03, DSS05.06 ISA 62443-2-1:2009 4.3.4.4.4 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 NIST SP 800-53 Rev. 4 MP-6 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) GDPR - Art. 5, 17, 32 ISO/IEC 29100:2011 5.11
PR.IP-7	I processi di protezione devono essere sottoposti a miglioramenti	COBIT 5 APO11.06, APO12.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 ISO/IEC 27001:2013 A.16.1.6, Clause 9, Clause 10 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.IP-8	L'efficacia delle tecnologie di protezione deve essere condivisa	COBIT 5 BAI08.04, DSS03.04 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.IP-9	In caso di incidente/disastro, devono essere attivi e amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery)	CIS CSC 19 COBIT 5 APO12.06, DSS04.03 ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 10.4.1 GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.IP-10	I piani di risposta e recupero a incidenti/disastri devono essere verificati nel tempo	CIS CSC 19, 20 COBIT 5 DSS04.04 ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev. 4 CP-4, IR-3, PM-14 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.IP-11	Le problematiche inerenti la cybersecurity devono essere incluse nei processi di gestione del personale (es: screening, deprovisioning)	CIS CSC 5, 16 COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 NIST SP 800-53 Rev. 4 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.IP-12	Deve essere sviluppato e implementato un piano di gestione delle vulnerabilità	CIS CSC 4, 18, 20 COBIT 5 BAI03.10, DSS05.01, DSS05.02 ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 4.7, 4.8, 4.9.1 GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.MA-1	La manutenzione e la riparazione delle risorse e dei sistemi deve essere eseguita e registrata con strumenti controllati e autorizzati	COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05 ISA 62443-2-1:2009 4.3.3.3.7 ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, MA-6 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 4.5, 8.2.2
PR.MA-2	La manutenzione remota delle risorse e dei sistemi deve essere approvata, documentata e svolta in modo da evitare accessi non autorizzati	CIS CSC 3, 5 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 NIST SP 800-53 Rev. 4 MA-4 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 3.4.1, 8.2.2
PR.PT-1	Deve esistere ed essere attuata una policy per definire, implementare e revisionare i log dei sistemi	CIS CSC 1, 3, 5, 6, 14, 15, 16 COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 ISA 62443-2-1:2009 4.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 4 AU Family D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 5.5.1 GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.PT-2	I supporti di memoria removibili devono essere protetti e il loro uso deve essere ristretto in accordo alle policy	CIS CSC 8, 13 COBIT 5 APO13.01, DSS05.02, DSS05.06 ISA 62443-3-3:2013 SR 2.3 ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 5.9.1, 8.7.1, 8.8.1, 13.5 GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.PT-3	Deve essere adottato il principio di minima funzionalità configurando i sistemi in modo che questi forniscano unicamente le funzionalità necessarie	CIS CSC 3, 11, 14 COBIT 5 DSS05.02, DSS05.05, DSS06.06 ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 ISO/IEC 27001:2013 A.9.1.2 NIST SP 800-53 Rev. 4 AC-3, CM-7 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 5.1.1, 5.1.2, 5.1.3, 5.9.1, 8.3.1 GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.PT-4	Le reti di comunicazione e controllo devono essere protette	CIS CSC 8, 12, 15 COBIT 5 DSS05.02, APO13.01 ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) Misure Minime AgID ABSC 5.9.1 GDPR - Art. 32 ISO/IEC 29100:2011 5.11
PR.PT-5	Devono essere implementati meccanismi (es. failsafe, load balancing, hot swap) che permettano di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse	COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 ISA 62443-2-1:2009 4.3.2.5.2 ISA 62443-3-3:2013 SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6 D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) GDPR - Art. 32 ISO/IEC 29100:2011 5.11
DE.AE-1	Devono essere definite, rese note e gestite delle pratiche di riferimento (c.d. baseline) inerenti all'utilizzo della rete e i flussi informativi attesi per utenti e sistemi	CIS CSC 1, 4, 6, 12, 13, 15, 16 COBIT 5 DSS03.01 ISA 62443-2-1:2009 4.4.3.3 ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4 Misure Minime AgID ABSC 5.1.4, 5.5.1, 8.3.2, 13.3.1
DE.AE-2	Gli eventi rilevati devono essere analizzati per comprendere gli obiettivi e le metodologie dell'attacco.	CIS CSC 3, 6, 13, 15 COBIT 5 DSS05.07 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
DE.AE-3	Le informazioni relative agli eventi devono essere raccolte e correlate da sensori e sorgenti multiple	CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 COBIT 5 BAI08.02 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1, A.16.1.7 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 Misure Minime AgID ABSC 8.1.3
DE.AE-4	Deve essere determinato l'impatto di un evento	CIS CSC 4, 6 COBIT 5 APO12.06, DSS03.01 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4
DE.AE-5	Devono essere definite delle soglie di allerta per gli incidenti	CIS CSC 6, 19 COBIT 5 APO12.06, DSS03.01 ISA 62443-2-1:2009 4.2.3.10 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8 Misure Minime AgID ABSC 5.5.1
DE.CM-1	Deve essere svolto il monitoraggio della rete informatica per rilevare potenziali eventi inerenti all'aspetto di cybersecurity	CIS CSC 1, 7, 8, 12, 13, 15, 16 COBIT 5 DSS01.03, DSS03.05, DSS05.07 ISA 62443-3-3:2013 SR 6.2 NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 D.Lgs. 18/5/2018 n. 65 Art. 14(2)-(3) Misure Minime AgID ABSC 5.5.1, 8.1.2, 8.1.3, 8.5.1, 8.6.1, 8.9, 8.10.1, 13.4.1, 13.6, 13.7.1, 13.8.1
DE.CM-2	Deve essere svolto il monitoraggio degli spazi fisici per rilevare potenziali eventi inerenti all'aspetto di cybersecurity	COBIT 5 DSS01.04, DSS01.05 ISA 62443-2-1:2009 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20 D.Lgs. 18/5/2018 n. 65 Art. 14(2)-(3)
DE.CM-3	Viene svolto il monitoraggio del personale per rilevare potenziali eventi inerenti all'aspetto di cybersecurity	CIS CSC 5, 7, 14, 16 COBIT 5 DSS05.07 ISA 62443-3-3:2013 SR 6.2 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3 NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 D.Lgs. 18/5/2018 n. 65 Art. 14(2)-(3) Misure Minime AgID ABSC 5.2
DE.CM-4	Il codice malevolo deve essere rilevato	CIS CSC 4, 7, 8, 12 COBIT 5 DSS05.01 ISA 62443-2-1:2009 4.3.4.3.8 ISA 62443-3-3:2013 SR 3.2 ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 4 SI-3, SI-8 Misure Minime AgID ABSC 8.1.1, 8.2.2, 8.2.3, 8.5, 8.6.1, 8.7.2, 8.7.3, 8.7.4, 8.8.1, 8.9, 8.10.1, 8.11.1

DE.CM-5	Il codice non autorizzato su dispositivi mobili deve essere autorizzato	CIS CSC 7, 8 COBIT 5 DSS05.01 ISA 62443-3-3:2013 SR 2.4 ISO/IEC 27001:2013 A.12.5.1, A.12.6.2 NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44 Misure Minime AgID ABSC 8.1.1
DE.CM-6	Deve essere svolto il monitoraggio delle attività dei servizie provider esterni per rilevare potenziali eventi inerenti all'aspetto di cybersecurity	COBIT 5 APO07.06, APO10.05 ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4 D.Lgs. 18/5/2018 n. 65 Art. 14(9)
DE.CM-7	Deve essere svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16 COBIT 5 DSS05.02, DSS05.05 ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 Misure Minime AgID ABSC 5.8.1, 8.3
DE.CM-8	Devono essere svolte scansioni per l'identificazione di vulnerabilità	CIS CSC 4, 20 COBIT 5 BAI03.10, DSS05.01 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-5 Misure Minime AgID ABSC 4.1, 4.2, 4.3, 4.4.1, 4.6.1
DE.DP-1	Devono essere ben definiti ruoli e responsabilità per i processi di monitoraggio al fine di garantire la accountability	CIS CSC 19 COBIT 5 APO01.02, DSS05.01, DSS06.03 ISA 62443-2-1:2009 4.4.3.1 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14 Misure Minime AgID ABSC 8.2.1
DE.DP-2	Le attività di monitoraggio devono soddisfare tutti i requisiti applicabili	COBIT 5 DSS06.01, MEA03.03, MEA03.04 ISA 62443-2-1:2009 4.4.3.2 ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
DE.DP-3	I processi di monitoraggio devono essere testati	COBIT 5 APO13.02, DSS05.02 ISA 62443-2-1:2009 4.4.3.2 ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.14.2.8 NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14 D.Lgs. 18/5/2018 n. 65 Art. 14(2)-(3)
DE.DP-4	L'informazione relativa agli eventi rilevati deve essere comunicata	CIS CSC 19 COBIT 5 APO08.04, APO12.06, DSS02.05 ISA 62443-2-1:2009 4.3.4.5.9 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.16.1.2, A.16.1.3 NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4
DE.DP-5	I processi di monitoraggio devono essere oggetto di periodici miglioramenti e perfezionamenti	COBIT 5 APO11.06, APO12.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
RS.RP-1	Deve esistere un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	CIS CSC 19 COBIT 5 APO12.06, BAI01.10 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8 GDPR Art. 33
RS.CO-1	Il personale deve essere cosciente del proprio ruolo e delle operazioni che deve svolgere in caso di necessaria risposta a un incidente	CIS CSC 19 COBIT 5 EDM03.02, APO01.02, APO12.03 ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1 NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8 D.Lgs. 18/5/2018 n. 65 Art. 9(2) Misure Minime AgID ABSC 8.1.3
RS.CO-2	Devono essere stabiliti dei criteri per documentare gli incidenti	CIS CSC 19 COBIT 5 DSS01.03 ISA 62443-2-1:2009 4.3.4.5.5 ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8 D.Lgs. 18/5/2018 n. 65 Artt. 12(7), 14(5)
RS.CO-3	Le informazioni devono essere condivise in maniera coerente al piano di risposta	CIS CSC 19 COBIT 5 DSS03.04 ISA 62443-2-1:2009 4.3.4.5.2 ISO/IEC 27001:2013 A.16.1.2, Clause 7.4, Clause 16.1.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
RS.CO-4	Il coordinamento con le parti interessate dell'organizzazione deve avvenire in coerenza con i piani di risposta	CIS CSC 19 COBIT 5 DSS03.04 ISA 62443-2-1:2009 4.3.4.5.5 ISO/IEC 27001:2013 Clause 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RS.CO-5	Deve essere attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggiore consapevolezza della situazione (c.d. situational awareness)	CIS CSC 19 COBIT 5 BAI08.04 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15 D.Lgs. 18/5/2018 n. 65 Artt. 12(5), 12(7)-(8), 14(4)-(5), 14(7)-(9) Misure Minime AgID ABSC 8.11.1
DP-RS.CO-6	Gli incidenti che si configurano come violazioni di dati personali devono essere documentati ed eventualmente vanno informate le autorità di riferimento e gli interessati	GDPR - Artt. 33, 34 ISO/IEC 29100:2011 5.10 ISO/IEC 29151O:2017 A.11 ISO/IEC 27018:2014 A.9.1 ISO/IEC 27001:2013 A.16 Misure Minime AgID ABSC
RS.AN-1	Le notifiche provenienti dai sistemi di monitoraggio devono essere sempre applicate, visionate e analizzate.	CIS CSC 4, 6, 8, 19 COBIT 5 DSS02.04, DSS02.07 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
RS.AN-2	L'impatto di ogni incidente deve essere compreso	COBIT 5 DSS02.02 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISO/IEC 27001:2013 A.16.1.4, A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4 D.Lgs. 18/5/2018 n. 65 Artt. 12(5), 12(7)-(8), 14(4)-(5), 14(7)-(9)
RS.AN-3	A seguito di un incidente deve essere svolta un'analisi forense	COBIT 5 APO12.06, DSS03.02, DSS05.07 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 ISO/IEC 27001:2013 A.16.1.7 NIST SP 800-53 Rev. 4 AU-7, IR-4
RS.AN-4	Gli incidenti devono essere categorizzate in maniera coerente con i piani di risposta	CIS CSC 19 COBIT 5 DSS02.02 ISA 62443-2-1:2009 4.3.4.5.6 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
RS.AN-5	Devono essere definiti processi per ricevere, analizzare e rispondere a informazioni riguardi vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)	CIS CSC 4, 19 COBIT 5 EDM03.02, DSS05.07 NIST SP 800-53 Rev. 4 SI-5, PM-15
RS.MI-1	In caso di incidente devono essere messe in atto procedure atte a contenerne l'impatto	CIS CSC 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.6 ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4 D.Lgs. 18/5/2018 n. 65 Artt. 12(2), 14(2)-(3) Misure Minime AgID ABSC 8.1.3, 8.4
RS.MI-2	In caso di incidente devono essere messe in atto procedure atte a mitigarne gli effetti	CIS CSC 4, 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4 D.Lgs. 18/5/2018 n. 65 Artt. 12(2), 14(2)-(3) Misure Minime AgID ABSC 8.4
RS.MI-3	Le nuove vulnerabilità devono essere mitigate o documentate come rischio accettato	CIS CSC 4 COBIT 5 APO12.06 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5 Misure Minime AgID ABSC 4.7, 4.9.1
RS.IM-1	I piani di risposta agli incidenti devono tenere in considerazione le esperienze passate (lessons learned)	COBIT 5 BAI01.13 ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RS.IM-2	Le strategie di risposta agli incidenti devono essere aggiornate	COBIT 5 BAI01.13, DSS04.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RC.RP-1	Deve esistere un piano di ripristino (recovery plan) e deve essere eseguito durante o dopo un incidente di cybersecurity	CIS CSC 10 COBIT 5 APO12.06, DSS02.05, DSS03.04 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8 Misure Minime AgID ABSC 3.2.2
RC.IM-1	I piani di recupero devono tenere in considerazione le esperienze passate (lesson learned)	COBIT 5 APO12.06, BAI05.07, DSS04.08 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 Misure Minime AgID ABSC 3.1.3
RC.IM-2	Le strategie di recupero devono essere aggiornate	COBIT 5 APO12.06, BAI07.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RC.CO-1	A seguito di un incidente devono essere gestite le pubbliche relazioni	COBIT 5 EDM03.02 ISO/IEC 27001:2013 A.6.1.4, Clause 7.4
RC.CO-2	A seguito di un incidente deve essere ripristinata la reputazione	COBIT 5 MEA03.02 ISO/IEC 27001:2013 Clause 7.4
RC.CO-3	Le attività di ripristino condotte a seguito di un incidente devono essere comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione	COBIT 5 APO12.06 ISO/IEC 27001:2013 Clause 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4