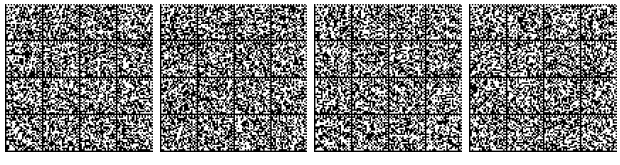
Allegato A

(articolo 2)

Tassonomia degli incidenti



Identificativo (incidente con impatto-ICP)	**Categoria**	**Descrizione**
ICP-A-1	**Infezione (*Initial exploitation*)**	**Infezione** (***Initial exploitation***). Il soggetto ha evidenza dell'effettiva esecuzione non autorizzata di codice o *malware* veicolato attraverso vettori di infezione o sfruttando vulnerabilità di risorse esposte in rete.
ICP-A-2	**Guasto (*Fault*)**	Violazione del livello di servizio atteso, definito dal soggetto incluso nel perimetro ai sensi di quanto previsto nelle misure di sicurezza di cui all'allegato B, in termini di risorse di calcolo, memoria e/o banda passante.
ICP-A-3		Violazione del livello di servizio atteso, definito dal soggetto incluso nel perimetro ai sensi di quanto previsto nelle misure di sicurezza di cui all'allegato B, di *hot-replica* e/o *cold-replica* e/o sito(i) di *disaster recovery*, se previsti.
ICP-A-4		Violazione del livello di servizio atteso, definito dal soggetto incluso nel perimetro ai sensi di quanto previsto nelle misure di sicurezza di cui all'allegato B, in termini di indisponibilità, di perdita irreversibile o di corruzione irreversibile dei dati provenienti dalle componenti di campo (attuatori e sensori).
ICP-A-5		Dati *hot-replica* e/o *cold-replica* e/o sito(i) di *disaster recovery* e/o *backup*, se previsti, persi o corrotti in modo irreversibile.
ICP-A-6		Perdita di confidenzialità o integrità.
ICP-A-7		Perdita e/o corruzione dati irreversibile.
ICP-A-8		Perdita e/o compromissione di chiavi di cifratura e/o certificati.
ICP-A-9		Perdita e/o compromissione di credenziali utenti.
ICP-A-10		Violazione del livello di servizio atteso, definito dal soggetto incluso nel perimetro ai sensi di quanto previsto dalle misure di sicurezza di cui all'allegato B, in termini di impossibilità di accesso fisico alle componenti.

Identificativo (incidente con impatto-ICP)	**Categoria**	**Descrizione**
ICP-A-11	**Installazione**	**Ottenimento di privilegi di livello superiore (*Privilege Escalation*)**. Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte dall'interno della rete, utili ad ottenere
	(*Establish persistence*)	permessi di livello superiore.
ICP-A-12		**Persistenza (*Persistence*)**. Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte dall'interno della rete, utili ad ottenere persistenza di codice malevolo o d'accesso.
ICP-A-13		**Evasione delle difese (*Defence Evasion*)**. Il soggetto ha evidenza dell'impiego non autorizzato di tecniche attraverso cui sono stati effettivamente elusi i sistemi di sicurezza.
ICP-A-14		**Comando e Controllo (*Command and Control*).** Il soggetto ha evidenza di comunicazioni non autorizzate verso l'esterno della rete.
ICP-A-15	**Movimenti laterali (*Lateral Movement*)**	**Esplorazione (*Discovery*)**. Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte dall'interno della rete, utili a effettuare attività di ricognizione.
ICP-A-16		**Raccolta di credenziali (*Credential Access*)**. Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad acquisire, dall'interno della rete, credenziali valide per l'autenticazione alle risorse di rete o ne rinviene copie non autorizzate.
ICP-A-17		**Movimenti laterali (*Lateral Movement*)**. Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad accedere o eseguire codice tra risorse interne della rete.
ICP-A-18	**Azioni sugli obiettivi (*Action on objs*)**	**Raccolta (*Collection*)**. Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad raccogliere, dall'interno della rete, dati di interesse di terze parti o ne rinviene copie non autorizzate.
ICP-A-19		**Esfiltrazione (*Exfiltration*)**. Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad esfiltrare dati dall'interno della rete verso risorse esterne.

TABELLA 2

Identificativo	Categoria	Descrizione
ICP-B-1	**Azioni sugli obiettivi (*Actions on objectives*)**	**Inibizione delle funzioni di risposta (*Inhibit Response Function*)**. Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a inibire l'intervento delle funzioni di sicurezza, di protezione e di "*quality assurance*" dei sistemi di controllo industriale predisposte per rispondere a un disservizio o a uno stato anomalo.
ICP-B-2		**Compromissione dei processi di controllo (*Impair Process Control*).** Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a manipolare, disabilitare o danneggiare i processi di controllo fisico di sistemi di controllo industriale.
ICP-B-3		**Disservizio intenzionale (*Impact*).** Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a manipolare, degradare, interrompere o distruggere i sistemi, i servizi o i dati. In tale ambito rientrano ad esempio gli eventi di tipo *Denial of Service*/*Distributed Denial of Service* che hanno impatto sui beni ICT.
ICP-B-4	**Disservizio (*Failure*)**	Violazione del livello di servizio atteso, definito dal soggetto incluso nel perimetro ai sensi di quanto previsto nelle misure di sicurezza di cui all'allegato B, specie in termini di disponibilità, del bene ICT.
ICP-B-5		Divulgazione di dati corrotti o esecuzione operazioni corrotte tramite il bene ICT.
ICP-B-6		Divulgazione non autorizzata di dati digitali relativi ai beni ICT.