CyberSecurity Enti Sanitari

Milano, Giugno 2023

Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

laboratorio SANITÀ 2030™
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

AGENDA

- TIMELINE DI PROGRAMMAZIONE STRATEGICA E TATTICA
- ARIA SPA
- APPROFONDIMENTI SULLE ATTIVITÀ SVOLTE
- MATURITA' CYBER DEGLI ENTI TERRITORIALI WELFARE
- ATTIVITA' PROPOSTE PER I PROSSIMI ANNI

Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

Timeline di programmazione strategica e tattica

Timeline di programmazione strategica

2006 - 2016

Sviluppo del **corpo documentale** (Linee Guida, Baseline, Framework, Indirizzi Tecnici, …)
Attività di Analisi dei Rischi IT
Verifiche ispettive (audit e sicurezza)
Analisi di **processo** (Gap Analysis, maturity Assessment)
Monitoraggio piani di remediation
Certificazione **ISO 27001**
Formazione e Awareness

2017

Attivazione del **centro di competenza** di CyberSecurity e collaborazione con **Polizia Postale**
Cyber Threat Intelligence
Costituency **CSOC**
Conformità **misure di sicurezza AgID** supporto all'adeguamento al **GDPR**

2018

Aggiornamento **Gap Analysis & AgID**
Supporto adeguamento AgID
Supporto operativo nel programma di **conformità al GDPR** sulla base del remediation plan identificato
Erogazione a regime del **ciclo di sensibilizzazione, verifica, assistenza e supporto**

2019

Redazione **Programma triennale integrato** di Sicurezza e Privacy di **Regione Lombardia**
Sviluppo **strategie di sicurezza (ARIA)**
multicompliance framework (AgID, GDRP, NIS)
Estensione del modello federato del SGSI
Integrazione **DPIA/A.d.R.**
Sviluppo processo di **gestione dei data-breach** ed integrazione nell'**incident management**
Estensione e formalizzazione dei servizi di **CSOC** per recepimento della direttiva **NIS**

23 Dicembre 2019

Con DGR **2683/XI** del 23 Dicembre 2019, la Giunta Regionale di **Regione Lombardia** approva formalmente il **Programma Triennale Integrato di Sicurezza e Privacy** di Regione Lombardia

2020-2022

Attuazione del **programma** triennale Integrato di **sicurezza e privacy** con report annuale di **governance** e monitoraggio del processo attuativo.

Redazione del nuovo programma di sicurezza con focus sugli E.S.

Entro primo semestre 2023

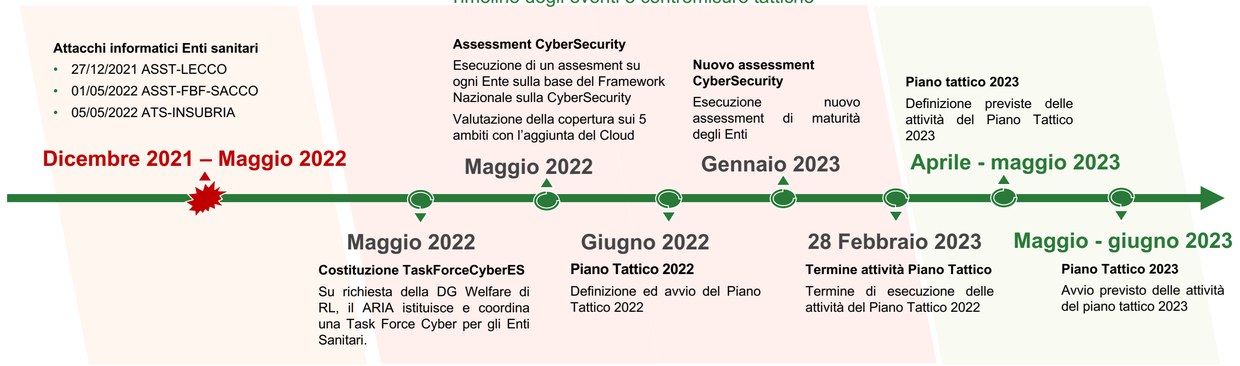
E' intenzione di **Regione Lombardia**, portare in approvazione entro il primo semestre 2023, il **nuovo programma triennale integrato di sicurezza e privacy**, in **continuità** e rafforzamento del precedente.

#sanita2030 www.sanita2030.it

Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

Timeline di programmazione strategica e tattica

Timeline degli eventi e contromisure tattiche



Nel corso del 2022 è stato necessario programmare, in modalità coordinata da Aria e condivisa con tutti gli Enti, interventi per il progressivo e continuo **innalzamento del livello di sicurezza informatica dell'intera architettura dei sistemi informativi regionali**, in particolare:

- Attivazione di **Task Force Regionale** e esecuzione di un assessment per la valutazione dello stato di protezione delle infrastrutture dei singoli Enti e la programmazione di interventi mirati
- Attivazione azioni verticali per ogni Ente previste dal piano tattico
- Introduzione e attivazione presso tutti gli Enti di un servizio di **Cyber Threat Intelligence**
- Attivazione del nuovo servizio regionale **MDA** per la gestione centralizzata dei "Security Incidents" rilevati dalle **piattaforme EDR/XDR**

Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

ARIA SpA: Chi siamo e cosa facciamo!

ARIA S.p.A. nasce dalla fusione delle 4 società di Regione Lombardia a totale partecipazione pubblica.

Siamo il partner strategico di Regione Lombardia

*Il nostro ruolo è quello di **generare valore** tra la domanda della **Pubblica Amministrazione**, l'offerta del **Mercato** e le esigenze di **Cittadini e Imprese**.*

E lo facciamo attraverso 4 linee di business volte a **governare la spesa pubblica, guidare la trasformazione digitale della P.A., progettare e gestire le infrastrutture, governare la gestione energetica** e **promuovere i territori della Lombardia**, supportando le politiche regionali tramite attività di governance-by-data.

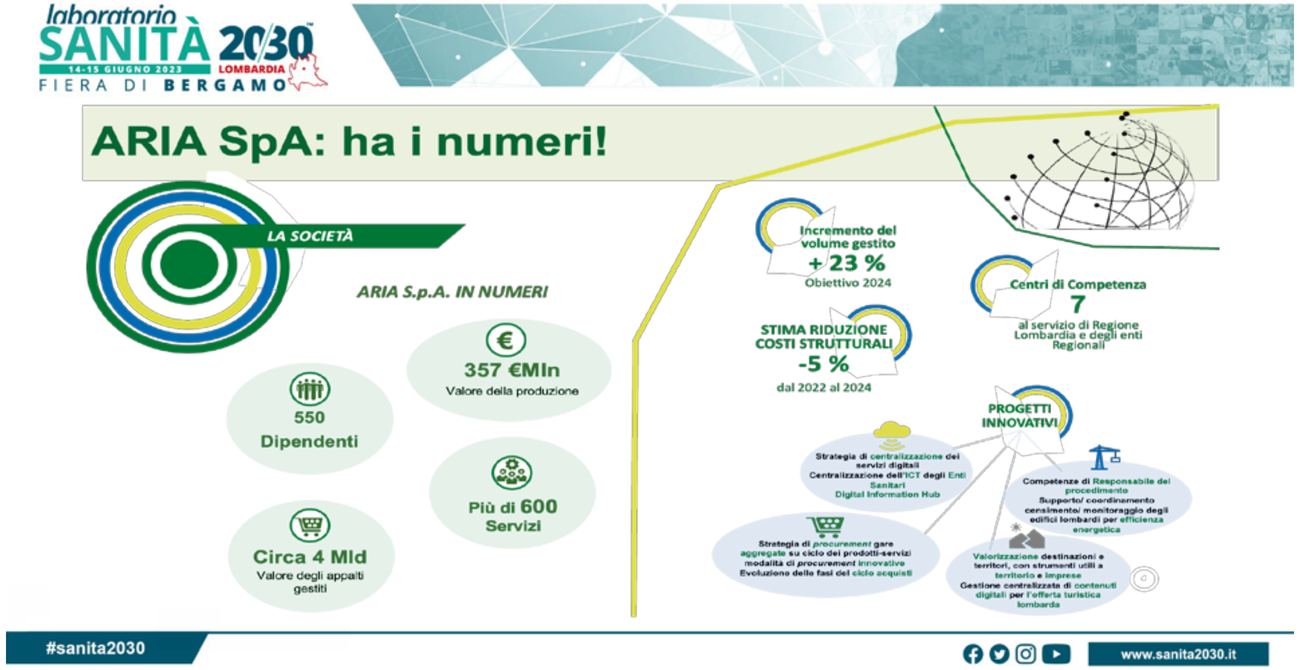
Nel ruolo di **Centrale di Committenza e di Soggetto Aggregatore nazionale**, ci occupiamo di **ottimizzare e razionalizzare** le procedure di acquisto in raccordo e coordinamento con la Regione Lombardia e il Ministero dell'Economia e delle Finanze.

Ci occupiamo di realizzare e riorganizzare le **strutture ospedaliere**, di conservare e rinnovare il **patrimonio immobiliare** di Regione Lombardia e di realizzare alcune **autostrade** regionali e nazionali. Svolgiamo anche una importante attività per la **gestione energetica** finalizzata all'uso razionale dell'energia.

Progettiamo nuove soluzioni e sperimentiamo **nuove tecnologie** in ambito e-health e e-government per migliorare l'efficienza della **Pubblica Amministrazione**, aumentare la competitività delle **Imprese**, semplificare la vita delle **Persone**.

Ci occupiamo della **promozione dell'intera offerta turistica del territorio regionale** lombardo, guidando anche le strategie di promozione turistica verso i mercati nazionali e internazionali in completa armonia e sinergia con le realtà locali.

Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001



Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

La Task Force di cybersecurity

Overview

- ✓ Su iniziativa della DG Welfare di Regione Lombardia, è stata predisposta una **TaskForce** composta da personale tecnico di aziende specializzate in **CyberSicurezza.**
- ✓ La task force ha il compito di intervenire presso le strutture per supportarle nella predisposizione di un piano volto ad **innalzare la posture di sicurezza**, supportandole inoltre nell'**implementazione delle misure** necessarie al raggiungimento di tale obiettivo.
- ✓ Con il supporto della Task Force è stato effettuato **un assessment di posture tecnologica** con lo scopo di identificare eventuali carenze infrastrutturali e/o di funzionalità, ovvero implementazioni che non garantiscono un sufficiente livello di sicurezza all'infrastruttura.
- ✓ I dati sono stati **aggregati ed omogeneizzati** per indirizzare i successivi interventi di rafforzamento delle infrastrutture ICT.

Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

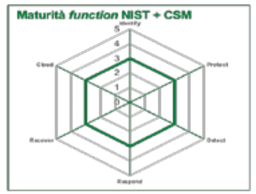
La Task Force di cybersecurity

Assessment preliminare

A seguito dell'assessment è stata avviata una fase di **condivisione** dei risultati suggerendo agli Enti Sanitari una serie di attività (azioni tattiche) specifiche per ciascun Ente sulla base delle proprie necessità, da implementarsi nel breve/medio periodo, tutte orientate ad un **innalzamento progressivo** dei livelli di protezione e sicurezza puntando ad una copertura omogenea degli ambiti della **metodologia NIST**:

- Identify
- Protect
- Detect
- Respond
- Recover

aggiungendo l'ambito Cloud.



Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

Metodologia di analisi e proposta delle azioni

Viene di seguito descritto il modello utilizzato per la valutazione del livello di maturità di ciascun Ente.

- Il framework di analisi (framework di riferimento) è composto da 236 basati sugli standard NIST, Cyber Security Framework e CSA con riferimento alla sezione Cloud
- Per ogni controllo è stato assegnato un livello di maturità su una scala a 6 livelli basata sul modello CMMI, da «Non Adeguato» (Livello 0) fino a «Stabile e Flessibile» (Livello 5)
- È stato individuato il **Livello 3 «Approccio Proattivo» quale livello target** a cui tendere
- Tale Livello target corrisponde alla copertura di **66 requisiti di sicurezza** identificati come minimi in termini di postura Cyber degli Enti, che rappresentano un sottoinsieme dei controlli corrispondenti alle 236 domande incluse nella checklist

Con riferimento ai 66 requisiti minimi, sono stati identificate **25 azioni tattiche** (slide successiva) allo scopo di attivare un piano immediato e sostenibile di rafforzamento della postura di sicurezza degli Enti
Tali azioni e la loro immediatamente successiva evoluzione (e.g. l'implementazione di specifiche tecnologie di sicurezza individuate nella fase tattica) permetteranno il raggiungimento del Livello 3 (target)

Scala valutazione Maturità *function* NIST e CSA

4,1 - 5	**Stabile e Flessibile.** Le attività volte alla copertura del controllo e dei rischi inerenti rispettano gli standard del livello precedente, integrando l'uso di strumenti dedicati alla misurazione dei risultati ai fini del miglioramento continuo e dell'aggiornamento dei processi
3,1 - 4,0	**Approccio Misurato e Controllato.** Le attività volte alla copertura del controllo e dei rischi inerenti prevedono la presenza di standard di sicurezza aggiuntivi rispetto ai requisiti minimi identificati
2,1 - 3,0	**Approccio Proattivo e Soddisfacimento dei requisiti minimi.** Le attività volte alla copertura del controllo e dei rischi inerenti avvengono secondo un processo standardizzato che prevede il soddisfacimento dei requisiti minimi di sicurezza identificati
1,1 - 2,0	**Approccio Destrutturato.** Le attività volte alla copertura del controllo e dei rischi inerenti avvengono secondo un processo ripetibile ma non sono presenti processi formali diffusi su tutto il perimetro in oggetto
0,6 - 1,0	**Approccio Reattivo.** Le attività volte alla copertura del controllo e dei rischi inerenti sono implementati occasionalmente, in base alla necessità o all'iniziativa dei singoli
0 - 0,5	**Non Adeguato.** Non sono rilevati un numero sufficiente di elementi atti alla copertura dei requisiti oggetto del controllo

Il livelli di maturità raggiunto da ogni Ente è stato rappresentato da un grafico a ragno che considera le 5 Function del NIST più il livello di maturità in ambito cloud

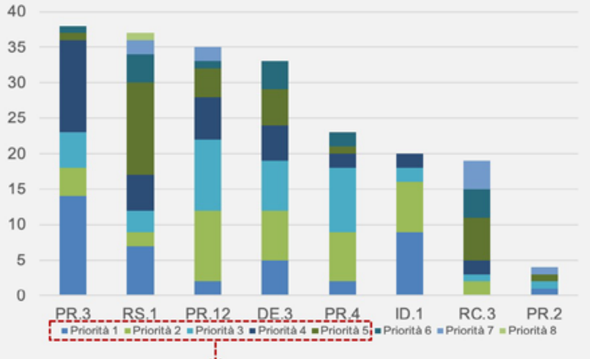
Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

laboratorio SANITÀ 2030™
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

Azioni svolte col piano tattico 2022

ID azione	Descrizione azione	N° Enti su cui è stata erogata da RL
ID.1	Identificare il perimetro degli **asset critici** (in termini di disponibilità, integrità e riservatezza dei dati), incluse dipendenze e priorità di recovery, e selezionare una soluzione di Asset Management da implementare	OMISSIS
PR.2	Analizzare la **segmentazione di rete** e controllare i flussi tra i vari segmenti	OMISSIS
PR.3	Eseguire una review di tutti gli **accessi privilegiati**, disabilitando quelli non necessari, e selezionare una soluzione di Privileged Access Management (PAM) da implementare	OMISSIS
PR.4	Supporto all'individuazione di un meccanismo di **Multi-Factor Authentication (MFA)** per l'accesso ad asset critici	OMISSIS
PR.6	Sviluppare un piano di **formazione/awareness** su temi di cybersecurity per tutto il personale	*Azioni proposte come prioritarie e rivolte a tutti gli Enti (coperte da RL)*
PR.11	Implementazione soluzione **EDR/XDR**	
PR.12	Analisi delle attuali politiche e configurazioni di **logging/auditing degli asset critici** al fine di avviare un percorso di integrazione con sistemi di log monitoring	OMISSIS
DE.3	Avviare tutte le analisi necessarie per dotarsi di un **servizio SOC/MDR** per il monitoraggio degli allarmi di sicurezza	OMISSIS
RS.1	Definire ruoli/responsabilità e processo per la **gestione degli incidenti di sicurezza** (e.g. Isolamento LAN interna e scollegamento macchine dalla rete; tempestiva comunicazione verso il CyberSOC ARIA)	OMISSIS
RC.3	Supporto all'individuazione dei mezzi di conservazione off-line della **golden copy**	OMISSIS

Distribuzione delle priorità selezionate dagli Enti per le azioni del piano tattico 2022



I costi delle azioni individuate da ciascun Ente fino a «priorità 5» sono stati coperti da Regione Lombardia.

#sanita2030 www.sanita2030.it

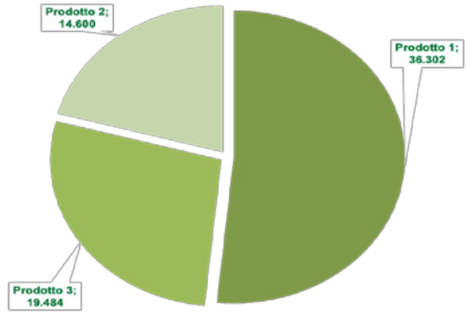
Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

Approfondimenti sulle attività svolte

EDR/XDR

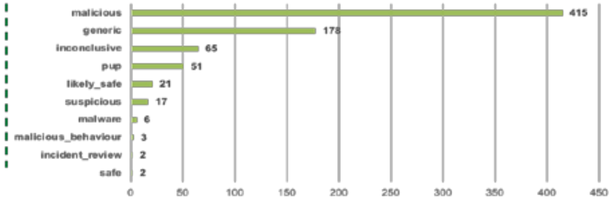
L'attività ha previsto l'implementazione di un sistema di **Endpoint/eXtended Detection Response** (**EDR/XDR**) per consentire la **protezione e il monitoraggio** della sicurezza di tutti i **server e i client** dell'Ente, attraverso il **rilevamento e la reazione** ad eventi significativi di sicurezza che abbiano come oggetto gli Endpoint.

TOTALE AGENTI EDR INSTALLATI*: 70.386 su **34 enti**



SECURITY INCIDENT Segnalazioni verso gli enti: **760**

SEGNALAZIONI PER TIPOLOGIA



#sanita2030

* Dati aggiornati al 15/06/2023

www.sanita2030.it

Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

Approfondimenti sulle attività svolte

Cyber Threat Intelligence

L'attività di **monitoraggio CTI** sugli Enti Sanitari si basa sui risultati di un assessment preliminare svolto per individuare il perimetro di ciascun Ente, e, attraverso analisi automatiche e manuali, mira ad identificare informazioni esposte pubblicamente, evidenziando potenziali rischi collegati alla loro presenza al di fuori del perimetro aziendale.

Tipologia di segnalazioni

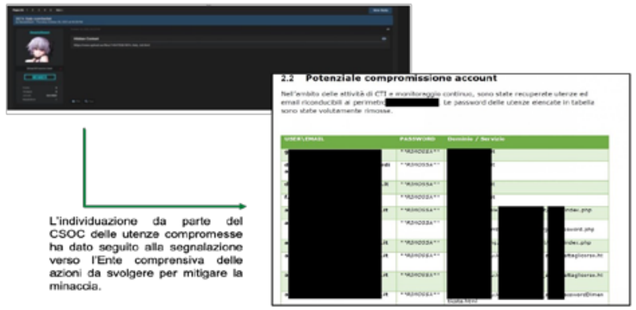
- Esfiltrazione dati
- Credenziali esposte
- Campagne malevole in corso che hanno come target l'Ente
- Account compromessi

Numero di segnalazioni inviate dall'avvio dell'attività:

103

Dati aggiornati al 16/05/2023

Ad esempio, attraverso l'attività di monitoraggio continuo il CSOC ha individuato la presenza di potenziali utenze compromesse di un Ente pubblicate su un forum underground*.



L'individuazione da parte del CSOC delle utenze compromesse ha dato seguito alla segnalazione verso l'Ente comprensiva delle azioni da svolgere per mitigare la minaccia.

Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

Approfondimenti sulle attività svolte
Formazione e awareness

Le attività formative e di awareness sono state erogate centralmente da ARIA secondo **due differenti modalità rivolte a interlocutori diversi**.

Formazione in ambito cyber governance e tech

Attività svolta attraverso sessioni formative rivolte a:
- **Responsabili e amministratori IT (personale SIA e IC),**
- **responsabili Sicurezza IT,**
- **Referenti NIS,**
- **Referenti applicativi/Key user,**
- **Responsabili trattamenti,**
- **Risk manager.**

Gli argomenti sono stati divisi su **2 moduli della durata di 4 ore ciascuno.**

Enti partecipanti.....40

Totale iscritti:.....647

Totale Partecipanti:.....577

Attività di awareness

Il piano di awareness prevede un corso svolto in modalità e-learning con quiz interattivi di sicurezza informatica con focus specifico sui seguenti scenari:

L'iniziativa è e rivolta a **tutta la popolazione** operante all'interno degli Enti sanitari erogata attraverso la **piattaforma FAD (Formazione a Distanza)** di RL e le piattaforme già presenti presso qualche Ente.

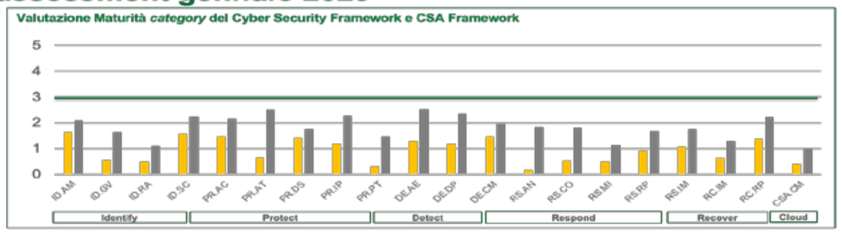
L'attività è attualmente in corso di svolgimento

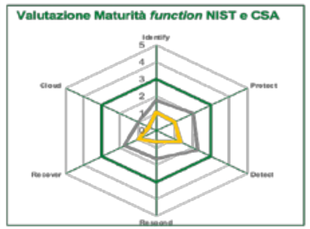
Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

Maturità cyber degli Enti Territoriali Welfare

Risultati del maturity assessment gennaio 2023

Functions	Category	ID
Identify	Asset Management	ID.AM
	Governance	ID.GV
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
Protect	Access Control	PR.AC
	Awareness and training	PR.AT
	Data Security	PR.DS
	Information Protection Processes and Procedures	PR.IP
	Protective Technology	PR.PT
Detect	Anomalies and events	DE.AE
	Detection Processes	DE.DP
	Security Continuous Monitoring	DE.CM
Respond	Analysis	RS.AN
	Communications	RS.CO
	Mitigations	RS.MI
	Response Planning	RS.RP
	Improvement	RS.IM
Recover	Improvement	RC.IM
	Recovey planning	RC.RP
Cloud	Cloud Security Alliance Controls Matrix	CSA.CM





Note

- Rispetto all'anno passato l'assessment è stato svolto anche sugli Enti AREU e ASST Fatebenefratelli/Sacco. Tuttavia nel calcolo della media riportata nelle rappresentazioni grafiche non sono inseriti i dati relativi a IRCCS Policlinico San Matteo. Il totale di Enti considerati è pertanto di 39 Enti.
- Come per lo scorso anno, l'assessment è stato eseguito in modalità self-assessmen da parte dell'Ente, pertanto non sono state richieste e verificate le evidenze a supporto delle risposte fornite dai singoli referenti al service manager che ha supportato lo svolgimento dell'attività.

Legenda Maturità
2022
2023
Target

Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

Ipotesi attività 2023

Nel corso del 2023 è intenzione di Regione Lombardia andare in continuità con quanto svolto lo scorso anno, implementando alcune soluzioni tecnologiche sugli Enti in modo da completare alcune azioni eseguite nel corso del 2022 che sono state propedeutiche e preparatorie all'avvio di un percorso di protezione di più lungo termine.

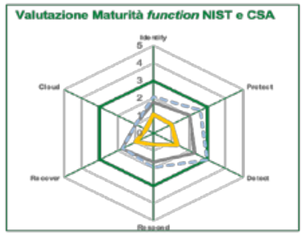
ID azione	Descrizione azione svolta nel 2022	Attività implementativa	Possibili soluzioni tecnologiche
ID.1	Identificare il perimetro degli **asset critici** (in termini di disponibilità, integrità e riservatezza dei dati), incluse dipendenze e priorità di recovery, e selezionare una soluzione di Asset Management da implementare	Implementazione di uno **strumento di asset management**	OMISSIS
PR.2	Analizzare la **segmentazione di rete** e controllare i flussi tra i vari segmenti	Supporto tecnico per l'implementazione della **segmentazione della rete**	OMISSIS
PR.3	Eseguire una review di tutti gli **accessi privilegiati**, disabilitando quelli non necessari, e selezionare una soluzione di Privileged Access Management (PAM) da implementare	Implementazione di uno strumento di **Privileged Access Management (PAM)**	OMISSIS
PR.4	Supporto all'individuazione di un meccanismo di **Multi-Factor Authentication (MFA)** per l'accesso ad asset critici	Implementazione dei meccanismi di **Multi-Factor Authentication (MFA)**	OMISSIS
PR.12	Analisi delle attuali politiche e configurazioni di **logging/auditing degli asset critici** al fine di avviare un percorso di integrazione con sistemi di log monitoring	Implementazione di uno **strumento di Log Collector**	OMISSIS
DE.3	Avviare tutte le analisi necessarie per dotarsi di un **servizio SOC/MDR** per il monitoraggio degli allarmi di sicurezza	Attivazione del **servizio SOC di ARIA**	OMISSIS
RS.1	Definire ruoli/responsabilità e processo per la **gestione degli incidenti di sicurezza** (e.g. Isolamento LAN interna e scollegamento macchine dalla rete; tempestiva comunicazione verso il CyberSOC ARIA)	Declinazione del processo rispetto agli attori specifici dell'Ente, **personalizzazione e test dei playbook** rispetto alle infrastrutture e alle tecnologie	OMISSIS
RC.3	Supporto all'individuazione dei mezzi di conservazione off-line della **golden copy**	Implementazione **mezzi di conservazione off-line della golden copy**	OMISSIS

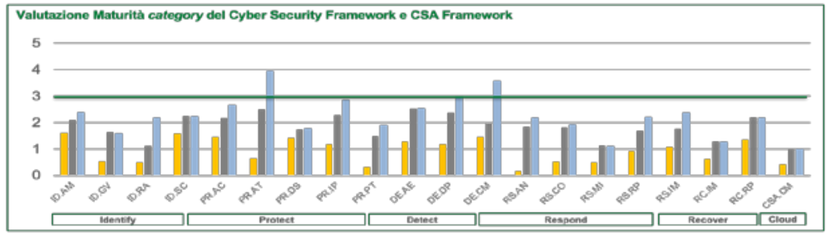
Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

Attività proposte per i prossimi anni

Previsione del livello di maturità dato dallo svolgimento delle azioni proposte

Si riporta di seguito una previsione della variazione dei grafici relativi al livello di maturità complessivo qualora vengano eseguite le attività previste dal programma riportato alla slide precedente.





Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

DOMANDE

Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

GRAZIE

Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001

Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1)
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2)
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941)
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

Torna all'inizio