Presidenza del Consiglio dei Ministri

CONFERENZA PERMANENTE PER I RAPPORTI
TRA LO STATO, LE REGIONI E LE PROVINCIE AUTONOME
DI TRENTO E DI BOLZANO

Accordo, ai sensi dell'articolo 4, del decreto legislativo 28 agosto 1997, n. 281, tra il Governo, le Regioni e Province autonome di Trento e Bolzano, in merito alle Linee guida per gli Operatori di Servizi Essenziali di cui all'articolo 12, commi 3 e 7, del decreto legislativo 18 maggio 2018, n. 65.

Rep. Atti n. 183/CSR 7 novembre 2019

LA CONFERENZA PERMANENTE PER I RAPPORTI TRA LO STATO, LE REGIONI E LE PROVINCE AUTONOME DI TRENTO E BOLZANO

Nella seduta del 7 novembre 2019

VISTO il decreto legislativo 28 agosto 1997, n. 281, articoli 2, comma 2, lettera *b)* e 4, comma 1, che affidano a questa Conferenza il compito di promuovere e sancire accordi tra il Governo, le Regioni e le Province autonome di Trento e di Bolzano, in attuazione del principio di leale collaborazione, al fine di coordinare l'esercizio delle rispettive competenze e svolgere attività di interesse comune;

VISTO il decreto legislativo 18 maggio 2018, n. 65, di attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, in particolare:
- l'articolo 7, comma 1, lettera d), rubricato *"Autorità nazionali competenti e punto di contatto unico"*, il quale individua, tra le Autorità competenti NIS (autorità NIS - Network and Information Security) *" il Ministero della salute per l'attività di assistenza sanitaria, come definita dall'articolo 3, comma 1, lettera a), del decreto legislativo 4 marzo 2014, n. 38, prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità sanitarie territorialmente competenti, per le attività di assistenza sanitaria prestata dagli operatori autorizzati e accreditati delle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza*";
- l'articolo 4, il quale prevede che *"con propri provvedimenti, le autorità competenti NIS identificano per ciascun settore e sottosettore di cui all'allegato II, gli operatori di servizi essenziali con una sede nel territorio nazionale. Gli operatori che prestano attività di assistenza sanitaria sono individuati con decreto del Ministro della salute, di intesa con la Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Provincie autonome di Trento e di Bolzano*";
- l'articolo 12, commi 3 e 7, rubricato "Obblighi in materia di sicurezza e notifica degli incidenti", il quale prevede – con riguardo alle misure tecniche e organizzative a carico degli OSE - la predisposizione di linee guida, concernenti altresì la notifica degli incidenti;

VISTA la nota del 2 agosto 2019, diramato in data 6 agosto 2019 dell'Ufficio di Segreteria di questa Conferenza, con la quale il Ministero della salute ha inviato lo schema di accordo unitamente alle Linee guida indicate in epigrafe;

RILEVATO che le citate linee guida definiscono gli obblighi a carico delle amministrazioni pubbliche, degli operatori di servizi essenziali e dei fornitori di servizi digitali per la sicurezza delle reti e dei sistemi informativi e per la notifica degli incidenti con impatto rilevante sulla continuità dei servizi;

VISTA la nota del 16 ottobre 2019 con la quale è stata convocata una riunione tecnica per il giorno 30 ottobre 2019, annullata con nota del 29 ottobre 2019, su richiesta del Coordinamento della Commissione salute delle Regioni in quanto è stato espresso l'assenso tecnico sul provvedimento con nota del 29 ottobre 2019;

CONSIDERATO che, nel corso dell'odierna seduta di questa Conferenza, le Regioni, le Province autonome di Trento e Bolzano hanno espresso avviso favorevole sullo schema di accordo del Ministero della salute;

ACQUISITO l'assenso del Governo, delle Regioni e delle Province autonome di Trento e Bolzano;

SANCISCE ACCORDO

tra il Governo, le Regioni e le Province autonome di Trento e Bolzano in merito alle Linee guida per gli Operatori di Servizi Essenziali (OSE), ai sensi dell'articolo 12 commi 3 e 7, del decreto legislativo 18 maggio 2018, n. 65, allegato A al presente accordo.

SEGRETARIO
Cons. Elisa Grande

IL PRESIDENTE
On. Francesco Boccia

All. A

REGIONE .....

Autorità NIS – Settore Salute

Linee guida per gli Operatori di Servizi Essenziali (OSE)

Versione 1.0 - 16 luglio 2019

Sommario

Elenco di distribuzione 3
Definizioni e acronimi 4
Introduzione 7
Capitolo 1: Framework nazionale di cyber security 8
Capitolo 2: Processo di gestione della sicurezza 10
Capitolo 3: Processo di gestione dei rischi 11
Capitolo 4: Descrizione delle Funzioni Core 14
4.1 Identify 14
4.2 Protect 16
4.3 Detect 18
4.4 Response 19
4.5 Recover 20
Capitolo 5: Pianificazione delle attività 22
Capitolo 6: Procedure di notifica degli incidenti 23
6.1 Procedure di notifica 23
6.2: Parametri di notifica settore SALUTE 24
ALLEGATO 1: Misure di sicurezza e Livelli di maturità 26
ALLEGATO 2: Misure di sicurezza – Scadenze settore Salute 27

Elenco di distribuzione

ENTI

Presidenza del Consiglio dei ministri, Dipartimento informazioni per la sicurezza, Punto di contatto unico NIS

Operatori di Servizi Essenziali (OSE) nel settore Salute di competenza della Regione

Definizioni e acronimi

DEFINIZIONI

Direttiva NIS: Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, recepita in Italia con il decreto legislativo 18 maggio 2018, n. 65.

Sicurezza della rete e dei sistemi informativi: la capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi.

Nucleo per la Sicurezza Cibernetica: organo collegiale costituito presso il DIS ai sensi del DPCM 17 febbraio 2017, a supporto del Presidente del Consiglio dei ministri e del CISR, nella materia della sicurezza dello spazio cibernetico, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

Punto di contatto unico: organo incaricato a livello nazionale di coordinare le questioni relative alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione europea. Il Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei ministri è designato quale punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi.

CSIRT italiano: il Computer Security Incident Response Team è un organo che studia la sicurezza delle reti e dei sistemi informativi per fornire servizi di risposta agli incidenti alle vittime di attacchi, pubblicare avvisi riguardanti vulnerabilità e minacce, offrire altre informazioni per migliorare la sicurezza dei computer e delle reti.

Autorità competente NIS: il D.Lgs. 65/2018 individua le seguenti cinque autorità settorialmente competente in materia di sicurezza delle reti e dei sistemi informativi:

- MiSE per il settore energia, sottosettori energia elettrica, gas e petrolio e per il settore infrastrutture digitali, sottosettori IXP, DNS, TLD, nonche' per i servizi digitali;
- MIT per il settore trasporti, sottosettori aereo, ferroviario, per vie d'acqua e su strada;
- MEF per il settore bancario e per il settore infrastrutture dei mercati finanziari, in collaborazione con le autorita' di vigilanza di settore, Banca d'Italia e Consob, secondo modalita' di collaborazione e di scambio di informazioni stabilite con decreto del Ministro dell'economia e delle finanze;
- Ministero della salute per l'attivita' di assistenza sanitaria prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso;
- Regioni e Province autonome di Trento e di Bolzano per le attivita' di assistenza sanitaria prestata dagli operatori autorizzati e accreditati delle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza;

- MATTM e Regioni e Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorita' territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.

Operatore di servizi essenziali: soggetto pubblico o privato, della tipologia di cui all'allegato II al decreto legislativo 18 maggio 2018, n. 65, che soddisfa i criteri di cui all'articolo 4, comma 2, del medesimo decreto. Nel settore fornitura e distribuzione di acqua potabile sono OSE i fornitori e distributori di acque destinate al consumo umano individuati con decreto del Ministro dell'ambiente e della tutela del territorio e del mare, di intesa con la Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano. Per le attività di assistenza sanitaria, con decreto del 9 novembre 2018 del Ministro della salute, di intesa con la Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano, sono stati definiti i criteri per l'identificazione degli OSE nel settore salute.

Incidente: ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi, che può nel tempo tramutarsi in incidente rilevante.

Incidente rilevante: incidente avente un impatto rilevante sulla continuità dei servizi essenziali forniti.

Trattamento dell'incidente: tutte le procedure necessarie per l'identificazione, l'analisi e il contenimento di un incidente e l'intervento in caso di incidente.

Rischio: ogni circostanza o evento ragionevolmente individuabile con potenziali effetti pregiudizievoli per la sicurezza della rete e dei sistemi informativi.

Informazioni non classificate controllate: informazioni non classificate che, in ragione della loro sensibilità, richiedono misure di protezione minime, individuate nelle disposizioni applicative del DPCM 6 novembre 2015, n. 5, per le quali la diffusione è limitata al controllato circuito di coloro che ne hanno necessità per lo svolgimento del proprio incarico.

ACRONIMI

CIS: Communication and Information System.

CSIRT: Computer Security Incident Report Team.

ICS: Industrial Control System.

MATTM: Ministero dell'ambiente e della tutela del territorio e del mare.

MEF: Ministero dell'economia e delle finanze.

MiSE: Ministero dello sviluppo economico.

MIT: Ministero delle infrastrutture e dei trasporti.

NIS: Network and Information Security (rif. Direttiva NIS).

NSC: Nucleo per la Sicurezza Cibernetica.

OSE: Operatore di servizi essenziali.

OCS: Organo centrale di sicurezza.

OT: Operational Technology.

Introduzione

Il presente documento costituisce una guida per l'implementazione degli articoli 12 "Obblighi in materia di sicurezza e notifica degli incidenti" e 13 "Attuazione e controllo" del D. Lgs. 18 giugno 2018, n. 65 con il quale la Direttiva (UE) 1148/2016 è stata recepita nell'ordinamento.

In particolare, l'articolo 12 prevede che gli operatori di servizi essenziali adottino misure tecniche organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi. Tali misure devono assicurare un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente nonché prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali, al fine di assicurare la continuità di tali servizi.

Al riguardo le Autorità competenti NIS possono definire specifiche misure di sicurezza (Art. 12, comma 4).

Ai sensi del medesimo articolo 12 gli operatori di servizi essenziali sono altresì tenuti a notificare al CSIRT (Computer Security Incident Report Team) e all'Autorità competente NIS gli incidenti con impatto rilevante sulla fornitura dei servizi essenziali; a sua volta il CSIRT è tenuto a inoltrare tempestivamente le notifiche ricevute dagli OSE al NSC, per la prevenzione e preparazione ad eventuali crisi cibernetiche e l'attivazione delle procedure di allertamento.

Per uniformare le procedure di notifica le Autorità competenti NIS possono predisporre linee guida per la notifica degli incidenti (art. 12, comma 7).

L'Articolo 13 affida alle Autorità competenti NIS il compito di valutare il rispetto da parte degli operatori di servizi essenziali degli obblighi previsti dall'articolo 12, nonché dei relativi effetti sulla sicurezza della rete e dei sistemi informativi.

Il presente documento è stato predisposto nell'ambito di un Tavolo costituitosi presso il DIS con la partecipazione delle Autorità competenti NIS di cui all'articolo 7 del D.Lgs. 65/2018, in attesa dell'approvazione del Decreto della Presidenza del Consiglio che definirà l'organizzazione e il funzionamento del Comitato di raccordo di cui all'articolo 9, comma 1, del predetto decreto.

La collaborazione tra le Autorità NIS in relazione al presente documento ha lo scopo di assicurare un'applicazione uniforme delle disposizioni nell'ottica di una crescita omogenea della sicurezza nei settori di rispettivo interesse.

Ciò premesso, nel presente documento sono fornite indicazioni sia in merito all'analisi del rischio che gli operatori di servizi essenziali dovranno condurre, sia in merito alle misure di sicurezza che gli stessi dovranno adottare a seguito degli esiti della predetta analisi del rischio.

Nel documento sono altresì individuati i casi in cui gli incidenti di sicurezza possono avere un impatto rilevante sulla fornitura del servizio essenziale e le modalità per la notifica di tali incidenti.

Le presenti Linee Guida saranno revisionate con cadenza almeno biennale in base alle evoluzioni tecnologiche e ad eventuali nuove tipologie di minaccia cyber.

Capitolo 1: Framework nazionale di cyber security

Il Comitato che riunisce le Autorità NIS ha condiviso l'opportunità di utilizzare il Framework Nazionale di Cyber Security (Versione 2.0 Febbraio 2019) predisposto dal CINI Cybersecurity National Lab (Consorzio Interuniversitario Nazionale per l'Informatica e dal CIS-Sapienza (Research Center of Cyber Intelligence and Information Security - Sapienza Università di Roma) come base di riferimento per la predisposizione delle linee guida oggetto del presente documento.

Le indicazioni che si forniscono, pertanto, si basano su tale framework il cui scopo è quello di offrire alle organizzazioni uno strumento per affrontare la cyber security al fine di ridurre il rischio delle minacce cyber. Si tratta infatti di un utile quadro di riferimento nel quale possono essere inquadrati gli standard e le norme di settore esistenti e future. L'approccio è strettamente legato a una analisi del rischio e non a standard tecnologici.

"Il core rappresenta la struttura del ciclo di vita del processo di gestione della cybersecurity, sia dal punto di vista tecnico sia organizzativo. Il core è strutturato gerarchicamente in function, category e subcategory. Le function, concorrenti e continue, sono: Identify, Protect, Detect, Respond, Recover e costituiscono le principali tematiche da affrontare per operare una adeguata gestione del rischio cyber in modo strategico. Il Framework quindi definisce, per ogni Function, Category e Subcategory, le quali forniscono indicazioni in termini di specifiche risorse, quali processi e tecnologie, da mettere in campo per gestire la singola Function.

Per chiarezza, di seguito si descrivono con maggiore dettaglio tali funzioni: [1]

Identify – In primo luogo è necessario analizzare il contesto aziendale, focalizzando l'attenzione sugli asset che supportano i processi critici ai fini della disponibilità del servizio e dei relativi rischi associati. La comprensione del contesto consente a un'organizzazione di definire risorse e investimenti in linea con la strategia di gestione del rischio e con gli obiettivi aziendali.

Le Categorie all'interno di questa funzione sono: Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy, Supply Chain Risk Management e Data Management.

Protect – La funzione PROTEGGERE è associata all'implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica.

Le category all'interno di questa function sono: Identity Management, Authentication and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, Protective Technology.

Detect- La funzione RILEVARE è associata alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica.

Le category all'interno di questa function sono: Anomalies and Events, Security Continuous Monitoring, Detection Processes

Respond – La funzione RISPONDERE è associata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato. L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica.

Le category all'interno di questa function sono: Response Planning, Communications, Analysis, Mitigation, Improvements

[1] Dal "Framework Nazionale di cyber security"

RECOVER - La funzione RIPRISTINARE è associata alla definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente. L'obiettivo è garantire la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, supportare il recupero tempestivo delle business operations.

Le category all'interno di questa function sono: Recovery Planning, Improvements, Communications

Una organizzazione, per utilizzare il Framework, come primo passo deve identificare una contestualizzazione su cui valutare il proprio profilo di rischio attuale. Una contestualizzazione del Framework implica la selezione delle sottocategorie del Framework Core applicabili al settore e al tipo di attività e la definizione dei relativi livelli di priorità e di maturità."[2]

La contestualizzazione del Framework consente di delineare il profilo attuale dell'Operatore rispetto al rischio cyber e, con la guida dell'Autorità NIS, seguire un profilo obiettivo per incrementare la sicurezza delle proprie reti e sistemi informativi.

I livelli di priorità definiscono qual è la priorità con cui devono essere effettuate le singole attività indicate nelle Sottocategorie del Framework Core . Nella presente linea guida il concetto di priorità proprio del Framework è stato riproposto in termini di scadenze più o meno stringenti a seconda dell'urgenza di implementazione di ogni Subcategory.

I livelli di maturità definiscono il modo con cui le attività vengono effettuate e permettono di fornire una misura del livello di attuazione di una procedura o di una contromisura di sicurezza. Devono essere definiti in modo crescente e prevedendo pratiche incrementali rispetto al livello di maturità precedente.

Il Framework utilizza inoltre un concetto relativo livello di integrazione dei processi di gestione del rischio cyber all'interno dell'organizzazione. In particolare sono previsti quattro livelli di valutazione: parziale, informato, ripetibile e adattivo. Un OSE dovrebbe attestarsi su un modello di gestione del rischio almeno "Ripetibile" di cui di seguito si riporta la definizione [3] :

Il modello di gestione del rischio cyber di una organizzazione è ripetibile se è formalmente definito ed approvato e se l'organizzazione aggiorna regolarmente le proprie pratiche di cybersecurity basandosi sull'output del processo di risk management. La gestione del rischio cyber è pervasiva a tutti i livelli organizzativi ed il personale è formato per gestire i ruoli che in merito gli vengono assegnati. L'organizzazione scambia regolarmente informazione inerenti alla cybersecurity con altri attori operanti nello stesso ecosistema.

In particolare nel seguito i Capitoli dal numero 2 al numero 4 definiscono una modalità ai fini dell'applicazione delle misure di sicurezza, mentre il capitolo 5 individua una programmazione delle attività prevedendo l'invio della documentazione di interesse all'Autorità NIS e infine il capitolo 6 è dedicato alla definizione dei parametri e relativi valori di soglia che qualificano la rilevanza di un incidente fornendo elementi per la procedura di notifica dello stesso.

[2] Dal "Framework Nazionale di cyber security)
[3] Dal "Framework Nazionale di cyber security)

Capitolo 2: Processo di gestione della sicurezza

Il processo di gestione della sicurezza è un processo ciclico a fasi successive, finalizzato ad incrementare la sicurezza informatica delle reti e dei sistemi informativi per ridurre al minimo la probabilità di interruzione del servizio essenziale.

Ciò equivale a dire che l'azione dell'Autorità NIS sarà volta alla verifica di tutte quelle attività che potrebbero avere un impatto negativo sulla fornitura dei servizi.

Pertanto le attività che, ad esempio, sono legati ad aspetti commerciali gestiti dall'Operatore non sono oggetto del presente documento come pure gli aspetti connessi alla protezione dei dati personali, nella misura in cui non risultano essere causa di interruzione del servizio.

Le due fasi fondamentali del processo di gestione della sicurezza sono il *"risk assessment"*, che prevede l'identificazione, l'analisi del rischio e la sua valutazione e il *"risk treatment"* che ne prevede il trattamento tramite l'adozione di misure necessarie a ridurlo fino ad una soglia ritenuta accettabile.

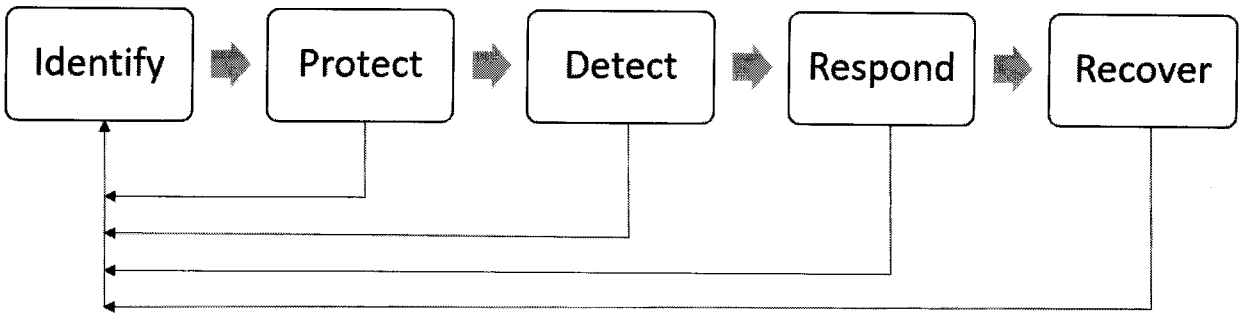
Tale soglia è individuata sulla base dei valori che definiscono l'incidente con impatto rilevante come definito nel paragrafo 6.2.

Nell'affrontare queste due fasi l'operatore deve focalizzarsi solo sugli aspetti connessi alla disponibilità del servizio essenziale di cui è fornitore.

Gli effetti di tale trattamento dovranno essere continuamente monitorati e le informazioni relative all'efficacia di tali misure dovranno essere documentate, per ottenere un miglioramento continuo tramite la reiterazione del processo.

Il processo nella sua interezza può essere categorizzato nelle cinque aree (o funzioni) principali *Identify, Protect, Detect, Respond, Recover* del Framework nazionale.

Processo di gestione della sicurezza



Capitolo 3: Processo di gestione dei rischi

Il processo di gestione dei rischi è incluso nel processo di gestione della sicurezza. Le attività che ne fanno parte sono principalmente categorizzate nelle function "Identify" e "Protect" ma anche le restanti function contribuiscono all'efficacia dello stesso, fornendo informazioni per un miglioramento continuo.

Per quanto riguarda l'implementazione del processo, l'operatore dovrà fare riferimento ad una metodologia standard al fine di:

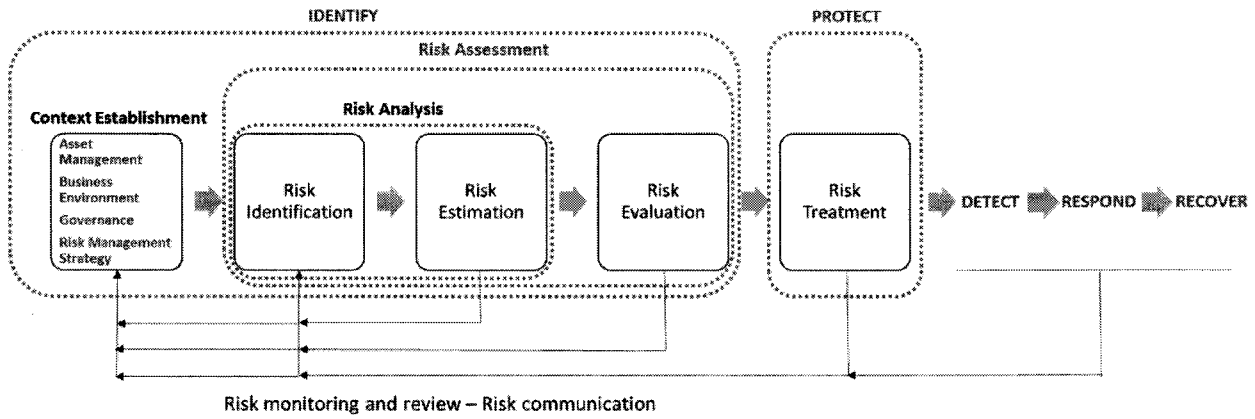
- individuare i principali rischi per la sicurezza delle reti e dei sistemi informativi tenendo conto delle minacce che insistono sugli asset;
- definire una metodologia di gestione dei rischi e utilizzare strumenti basati sugli standard di settore;
- verificare l'effettivo utilizzo di tali metodologie e strumenti di gestione del rischio da parte del personale;
- stabilire una priorità nelle azioni da condurre per ridurre l'impatto dei rischi e misurare l'efficacia del trattamento dei rischi.
- assicurarsi che i rischi residui, anche derivanti da vincoli realizzativi, siano minimizzati rispetto alla probabilità del verificarsi di incidenti;
- reiterare, monitorare e verificare il processo regolarmente.

Prima di procedere con le attività di identificazione dei rischi, l'operatore dovrà COMPRENDERE il rischio di cybersecurity inerente la propria operatività.

Di seguito si riporta uno schema del processo di gestione dei rischi secondo la ISO 27005 nel quale si è cercato di evidenziare la relazione con alcune Function e Category del Framework nazionale.

Nello schema sono state indicate in rosso le Function e in blu le Category.

Processo di gestione dei rischi



Il processo di gestione dei rischi è un processo ciclico e comprende le seguenti fasi:

1) Fase preliminare di Context Establishment (definizione del contesto)
2) Risk Identification (Identificazione dei rischi)

3) Risk Estimation (Analisi dei rischi) e Risk Evaluation (Ponderazione dei rischi)

Tali fasi sono contenute nelle attività descritte nella function "Identify"

4) Risk Treatment (Trattamento dei rischi)

Tale fase è contenuta nelle attività descritte nella function "Protect"

5) Valutazione del rischio residuo, monitoraggio continuo, revisione e reiterazione del processo.

Tali fasi sono contenute nelle attività descritte nelle restanti function.

1) Definizione del contesto

In questa fase l'operatore dovrà COMPRENDERE il rischio di cybersecurity inerente la propria operatività, ossia i servizi erogati (in particolare i servizi essenziali), le funzioni, il ruolo ricoperto all'interno del sistema paese, gli asset e gli individui (Category: Asset Management, Business Environment).

Ciò significa che l'operatore dovrà dotarsi di una documentata, diffusa e applicata politica di sicurezza che definisca le priorità, i requisiti dell'organizzazione e la tolleranza al rischio, per poi supportare le decisioni sul rischio operativo (Category: Governance, Risk Management Strategy).

2) Identificazione dei rischi

Lo scopo dell'identificazione del rischio è quello di determinare quali eventi possano accadere e quali possano essere le relative conseguenze (impatti) in caso tali eventi si verifichino.

Ciò significa che gli operatori dovranno svolgere e documentare le seguenti azioni:

1. Identificare gli asset che fanno parte dei sistemi informativi o che ne siano in qualche modo collegati (es. personale di gestione dei sistemi informativi, servizi erogati dipendenti dai sistemi informatici, ecc.)
2. Identificare le minacce e le vulnerabilità sia interne che esterne, che incombono sugli asset (es. procedure, processi, configurazione dei sistemi informatici, ecc.)
3. Identificare i controlli e le misure già in atto.
4. Identificare le conseguenze in caso di accadimento di ogni rischio identificato (evento). (es. interruzione dei servizi)

3) Analisi e ponderazione dei rischi

Lo scopo di tali attività è la valutazione della probabilità che un rischio identificato nella fase precedente si possa verificare. Tale valutazione può avvenire con un criterio qualitativo o quantitativo.

Ciò significa che gli operatori dovranno svolgere e documentare le seguenti azioni:

1. Valutare la probabilità che un rischio si verifichi
2. Valutare l'impatto del verificarsi dell'evento

3. Assegnare differenti priorità e livelli ai rischi in accordo con i risultati dell'analisi, per poter poi pianificarne il trattamento.

4) Trattamento dei rischi

Lo scopo di tale fase è scegliere e applicare le azioni di mitigazione del rischio in accordo a quanto emerso dall'analisi precedente e in accordo alla politica di gestione del rischio stabilita dall'azienda. Tali azioni costituiranno il piano di trattamento dei rischi.

Ciò significa che gli operatori dovranno svolgere e documentare le seguenti azioni:

1. Definire un livello minimo di tolleranza al rischio al di sotto del quale i rischi vengono accettati ed al di sopra del quale i rischi devono essere trattati con azioni mirate.
2. Stabilire per ogni rischio un'azione mirata, ossia una misura.
3. Applicare tali misure

5) Valutazione del rischio residuo, monitoraggio continuo, revisione e reiterazione del processo.

Lo scopo di tale fase è verificare l'efficacia delle misure applicate, monitorando gli eventi e i processi messi in atto.

Ciò significa che gli operatori dovranno svolgere e documentare le seguenti azioni:

1. Verificare costantemente l'efficacia delle misure applicate
2. Tenere traccia e reagire agli eventi.
3. Analizzare gli eventi per migliorare il processo reiterandolo.

Capitolo 4: Descrizione delle Funzioni Core

Nel presente capitolo si riportano nel dettaglio le attività da condurre selezionate dal framework, in coerenza con i processi delineati nei capitoli precedenti.

Le informazioni raccolte, le decisioni assunte e le azioni intraprese in merito a tali attività sono adeguatamente e regolarmente documentate.

4.1 Identify

Asset Management:

IDENTIFICARE E GESTIRE i dati, il personale, i dispositivi, i sistemi e le facilities necessari all'organizzazione, in coerenza con gli obiettivi di erogazione dei servizi e con la strategia di rischio dell'organizzazione.

Attività

- Censire i sistemi, gli apparati fisici, le piattaforme e le applicazioni software in uso nell'organizzazione
- Identificare i flussi di dati e le comunicazioni effettuate dall'organizzazione
- Catalogare i sistemi informativi esterni all'organizzazione
- Classificare tutti gli asset in base alla loro criticità e valore per i servizi erogati dall'operatore assegnando un livello di priorità per ogni asset
- Definire e rendere noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)

La documentazione minimale che fornisce evidenza di tali attività è costituita da una lista organizzata di tutti gli asset identificati e di tutte le informazioni raccolte in coerenza con quanto sopra.

Business Environment:

COMPRENDERE E VALUTARE i servizi erogati, gli obiettivi, le attività e le persone coinvolte in termini di priorità, per gestire di conseguenza i ruoli, le responsabilità di cybersecurity e le decisioni in materia di gestione del rischio.

Attività:

- Identificare e rendere noto il ruolo dell'organizzazione all'interno della filiera produttiva e nel settore industriale di riferimento
- Definire e rendere note le priorità per quanto riguarda la missione, i servizi erogati, gli obiettivi e le attività dell'organizzazione
- Identificare e rendere note interdipendenze e funzioni fondamentali per la fornitura di servizi essenziali
- Identificare e rendere noti i requisiti di resilienza a supporto della fornitura di servizi essenziali per tutti gli stati di esercizio (es. sotto stress/attacco, in fase di recovery, normale esercizio)

Governance:

COMPRENDERE E UTILIZZARE le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) nella gestione del rischio di cybersecurity.

Attività

- Predisporre, ratificare e divulgare internamente una policy di cybersecurity
- Coordinare e allineare ruoli e responsabilità inerenti la cybersecurity, con i ruoli aziendali interni ed i partner esterni
- Comprendere e gestire i requisiti legali in materia di cybersecurity
- Includere la gestione dei rischi legati alla cybersecurity nella governance e nei processi di risk management

Risk Management Strategy:

DEFINIRE E UTILIZZARE le priorità, i requisiti dell'organizzazione e la tolleranza al rischio, per supportare le decisioni sul rischio operativo.

Attività

- Definizione e gestione dei processi di risk management da parte dei responsabili dell'organizzazione
- Definire un livello minimo di tolleranza al rischio al di sotto del quale i rischi vengono accettati ed al di sopra del quale i rischi devono essere trattati con azioni mirate tenendo principalmente conto dei servizi erogati dell'organizzazione

La documentazione minimale che fornisce evidenza di tali attività è costituita da un documento contenente la policy aziendale di cybersecurity in coerenza con quanto definito.

Risk Assessment:

COMPRENDERE il rischio di cybersecurity inerente l'operatività dell'organizzazione con specifico riferimento ai servizi essenziali.

Attività

- Identificare le vulnerabilità degli asset
- Identificare le minacce che si originano nell'ambiente interno all'organizzazione e quelle provenienti dall'esterno
- Identificare i potenziali impatti sull'erogazione del servizio e le relative probabilità di accadimento
- Analizzare il rischio sulla base delle minacce, vulnerabilità, probabilità di accadimento e conseguenti impatti
- Identificare e definire le priorità delle risposte ai rischi
- Stabilire un'azione mirata per il trattamento di ogni rischio
- Valutare il rischio residuo a seguito delle azioni stabilite

La documentazione minimale che fornisce evidenza di tali attività è costituita dalla "Dichiarazione di Applicabilità", ossia un documento in cui vengono dettagliati i risultati delle azioni effettuate in coerenza con quanto sopra.

Supply Chain Risk Management:

STABILIRE E UTILIZZARE le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione, per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. Definire e implementare processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.

Attività

- Identificare, definire, validare, gestire e approvare i processi di gestione del rischio inerenti la catena di approvvigionamento cyber assicurando che i rischi residui che non sono gestiti dalla terza parte siano minimizzati rispetto alla probabilità del verificarsi di incidenti e che siano accettati dalla Direzione
- Identificare e valutare i fornitori e i partner terzi di sistemi informativi, componenti e servizi, assegnando una scala di priorità sulla base dell'attività definita nel punto precedente
- Definire i requisiti di sicurezza nei contratti con i fornitori e i partner terzi nel rispetto degli obiettivi del programma di cybersecurity dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento cyber.
- Valutare regolarmente fornitori e partner terzi utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali
- Condurre con i fornitori e i partner terzi la pianificazione e la verifica della risposta, del ripristino ed eventualmente l'analisi del rischio qualora fosse necessario.

La documentazione minimale che fornisce evidenza di tali attività è costituita da un documento in cui vengono dettagliati i risultati delle azioni effettuate in coerenza con quanto sopra. In alternativa tali informazioni potrebbero essere comprese nei documenti citati in precedenza, ma in ogni caso le informazioni devono essere specificatamente evidenziate.

4.2 Protect

Identity Management, Authentication and Access Control:

LIMITARE al personale, ai processi e ai dispositivi autorizzati l'accesso agli asset fisici e logici ed alle relative risorse. GESTIRE l'accesso in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate

Attività

- Amministrare, verificare, revocare e sottoporre a audit di sicurezza, le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati
- Proteggere e gestire l'accesso fisico alle risorse (limitando l'ingresso e l'uscita del personale in un'area, ad esempio un edificio per uffici, una suite, un data center o una stanza, contenente apparecchiature per l'elaborazione delle informazioni).
- Amministrare l'accesso remoto alle risorse
- Amministrare con un processo formale i diritti di accesso alle risorse e le relative autorizzazioni secondo il principio del privilegio minimo e della separazione delle funzioni, ossia limitare le risorse logiche del sistema (transazioni, dati, programmi, applicazioni) al minimo necessario.
- Proteggere l'integrità di rete (es. segregazione di rete, segmentazione di rete)
- Comprovare le identità, associarle a credenziali e verificarle durante le interazioni
- Commisurare al rischio della transazione (es. rischi legati alla erogazione del servizio essenziale) le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti, i dispositivi e altri asset

Awareness and Training:

SENSIBILIZZARE E ISTRUIRE il personale e le terze parti in materia di cybersecurity per adempiere ai propri compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti

Attività

- Informare tutti gli utenti sui principali rischi cyber e istruirli sulle norme comportamentali da seguire e sulle procedure da eseguire
- Far comprendere agli utenti con privilegi (es. Amministratori di Sistema), a tutte le terze parti (es. fornitori) e al personale addetto alla sicurezza fisica e alla cybersecurity, i loro ruoli e responsabilità

Data Security:

GESTIRE E ARCHIVIARE i dati al fine di garantirne l'integrità, la confidenzialità e la disponibilità in accordo alla strategia di gestione del rischio dell'organizzazione.

Attività

- Proteggere i dati memorizzati
- Proteggere i dati durante la trasmissione
- Gestire attraverso un processo formale il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati
- Fornire ai sistemi adeguate risorse per poter garantire la disponibilità
- Implementare tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).
- Impiegare meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni
- Separare gli ambienti di sviluppo e test dall'ambiente di produzione
- Impiegare meccanismi di controllo dell'integrità per verificare l'integrità del hardware

Information Protection Processes and Procedures:

ATTUARE E AGGIORNARE nel tempo le politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), oltreché i processi e le procedure per gestire la protezione dei sistemi informativi e degli asset.

Attività

- Definire e gestire processi e procedure operative per la configurazione dei sistemi IT, che incorporano principi di sicurezza (es. principio di minima funzionalità)
- Implementare un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle).
- Attivare processi di controllo della modifica delle configurazioni
- Eseguire, amministrare e verificare i backup delle informazioni
- Verificare il rispetto delle policy e dei regolamenti relativi agli ambienti fisici in cui operano le risorse dell'organizzazione
- Distruggere i dati in conformità con le policy
- Verificare l'efficacia dei processi e tecnologie di protezione per sottoporli a miglioramento continuo.
- Attivare e amministrare piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro
- Verificare ed eseguire regolarmente i piani di risposta e recupero a seguito di incidenti/disastri
- Includere le problematiche inerenti la cybersecurity, nei processi di gestione del personale (es: assunzioni, dimissioni, ecc.)
- Sviluppare e implementare un piano di gestione delle vulnerabilità

Maintenance:

EFFETTUARE la manutenzione dei sistemi informativi in accordo con le politiche e le procedure esistenti.

Attività

- Eseguire e tenere traccia documentata della manutenzione e riparazione delle risorse e dei sistemi, mediante strumenti controllati ed autorizzati
- Approvare, documentare e svolgere la manutenzione remota delle risorse e dei sistemi in modo da evitare accessi non autorizzati

Protective Technology:

GESTIRE le soluzioni tecniche di sicurezza per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.

Attività

- Redigere e attuare una policy per definire, implementare e revisionare i log dei sistemi
- Proteggere i supporti di memorizzazione removibili e utilizzarli in accordo alle policy
- Adottare il principio di minima funzionalità configurando i sistemi in modo che forniscano solo le funzionalità necessarie
- Proteggere le reti di comunicazione e controllo
- Implementare meccanismi che permettono di soddisfare requisiti di resilienza

4.3 Detect

Anomalies and Events:

RILEVARE E ANALIZZARE le attività anomale e il loro impatto potenziale

LIMITARE al personale, ai processi e ai dispositivi autorizzati l'accesso agli asset fisici e logici ed alle relative risorse. GESTIRE l'accesso in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate

Attività

- Definire rendere note e gestire delle pratiche di riferimento (c.d. baseline) inerenti l'utilizzo della rete ed i flussi informativi attesi per utenti e sistemi
- Analizzare gli eventi rilevati per comprendere gli obiettivi e le metodologie dell'attacco
- Raccogliere e correlare le informazioni relative agli eventi, mediante sensori e sorgenti multiple
- Determinare l'impatto di un evento
- Definire delle soglie di allerta per gli incidenti

Security Continuous Monitoring:

MONITORARE i sistemi informativi e gli asset per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.

Attività

- Svolgere il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity
- Svolgere il monitoraggio degli spazi fisici per rilevare potenziali eventi di cybersecurity
- Svolgere il monitoraggio del personale per rilevare potenziali eventi di cybersecurity
- Predisporre e implementare strumenti di rilevazione di codice malevolo
- Predisporre e implementare strumenti di rilevazione di codice non autorizzato su dispositivi mobili
- Svolgere il monitoraggio delle attività dei service provider esterni per rilevare potenziali eventi di cybersecurity
- Svolgere il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati
- Svolgere scansioni per l'identificazione di vulnerabilità

Detection Processes:

ADOTTARE, MANTENERE e VERIFICARE processi e procedure di monitoraggio per assicurare la rilevazione di eventi anomali.

Attività

- Definire ruoli e responsabilità per i processi di monitoraggio al fine di garantire l'accountability
- Fare in modo che le attività di monitoraggio soddisfino tutti i requisiti applicabili
- Verificare i processi di monitoraggio
- Comunicare l'informazione relativa agli eventi rilevati
- Migliorare e perfezionare in modo periodico i processi di monitoraggio

4.4 Response

Response Planning:

ESEGUIRE E MANUTENERE procedure e processi di risposta per assicurare una reazione agli incidenti di cybersecurity rilevati.

Attività

- Definire un piano di risposta (response plan) per poi eseguirlo durante o dopo un incidente
- Verificare che si risponda agli incidenti secondo le procedure documentate

Communications:

COORDINARE le attività di risposta con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).

Attività

- Formare e istruire il personale affinché conosca il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente
- Stabilire dei criteri per documentare gli incidenti

- Documentare gli incidenti acquisendo e conservando le informazioni relative allo stesso (es. data dell'evento, impatto, ecc.)
- Condividere le informazioni in maniera coerente con il piano di risposta
- Effettuare il coordinamento con le parti interessate dell'organizzazione, in coerenza con i piani di risposta
- Attuare 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)

Analysis:

EFFETTUARE analisi per assicurare un'efficace riposta e supporto alle attività di ripristino.

Attività

- Visionare e analizzare tutte le notifiche provenienti dai sistemi di monitoraggio
- Comprendere l'impatto di ogni incidente
- Svolgere un'analisi a seguito di un incidente
- Categorizzare gli incidenti in maniera coerente con i piani di risposta
- Definire i processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)

Mitigation:

ESEGUIRE azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i sui effetti e per risolvere l'incidente.

Attività

- In caso di incidente mettere in atto procedure atte a contenerne l'impatto
- In caso di incidente mettere in atto procedure atte a mitigarne gli effetti
- Reiterare il processo di gestione dei rischi, considerando le nuove vulnerabilità per poi mitigarne gli effetti o documentarle come rischio accettato

Improvements:

MIGLIORARE le attività di risposta incorporando le "lesson learned" da attività precedenti di monitoraggio e risposta.

Attività

- Tenere in considerazione le esperienze passate (lesson learned) nella stesura dei piani di risposta agli incidenti
- Aggiornare le strategie di risposta agli incidenti

4.5 Recover

Recovery Planning:

ESEGUIRE E MANUTENERE processi e procedure di ripristino per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.

Attività

- Definire un piano di ripristino (recovery plan) che possa essere eseguito durante o dopo un incidente di cybersecurity

Improvements:

MIGLIORARE i piani di ripristino ed i relativi processi tenendo conto delle di quanto accaduto in precedenza per pianificare migliori risposte nelle le attività future.

Attività

- Tenere in considerazione le esperienze passate (lesson learned) nella stesura nei piani di ripristino
- Aggiornare le strategie di ripristino

Communications:

COORDINARE le attività di ripristino a seguito di un incidente con le parti interne ed esterne (es. le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT).

Attività

- Comunicare alle parti interessate interne ed esterne all'organizzazione (inclusi i dirigenti ed i vertici dell'organizzazione) le attività di ripristino condotte a seguito di un incidente

Capitolo 5: Pianificazione delle attività

Entro quattro mesi dalla notifica agli OSE della presente linea guida, gli OSE medesimi invieranno all'Autorità competente NIS regionale le seguenti informazioni:

a. la "Dichiarazione di Applicabilità" risultante dal "Risk Assessment";
b. le misure di sicurezza già implementate ed il relativo livello di maturità;
c. le misure di sicurezza da implementare, indicando la relativa priorità (scadenza) conformemente a quanto indicato in Allegato 2 per le classi di servizi Emergenza-urgenza, Ricovero per acuti, Lungodegenza/riabilitazione/regime ambulatoriale, e sulla base dell'analisi del rischio per gli altri servizi;
d. il cronoprogramma di incremento del livello di maturità delle misure già implementate.

Le informazioni relative ai punti b) e c) dovranno essere compilate secondo la tabella in Allegato 1 e trasmesse in formato elettronico; la citata tabella contiene le subcategory del Framework Nazionale di Cyber Security descritto nel Capitolo 1 e, per ciascuna subcategory, la corrispondenza, laddove possibile, con le 'Misure minime di sicurezza ICT per le pubbliche amministrazioni' emanate da AgID e con i 'Controlli essenziali di cybersecurity 2016' pubblicati dai già citati CINI Cybersecurity National Lab e CIS-Sapienza. Inoltre, per le pertinenti sub-category, la valutazione del livello di maturità e della priorità (scadenza) di implementazione dovrà tener conto di quanto previsto dal documento redatto da AgID "Linee guida sicurezza nel procurement ICT".

Le informazioni di cui ai punti a), b), c) e d) dovranno essere inviate, con le modalità riservate previste dall'Art. 38 del dPCM 6 novembre 2015, n.5, all'indirizzo di posta certificata (PEC) della Autorità competente NIS regionale.

Come già descritto in precedenza, il livello di priorità (scadenza) è da intendersi riferito alla maggiore o minore urgenza nell'implementazione delle misure. In particolare:

- entro 9 mesi dalla notifica della presente linea guida gli operatori sono tenuti ad implementare le misure con livello di priorità (scadenza) alta e media;
- entro 12 mesi dalla notifica della presente linea guida gli operatori sono tenuti ad implementare le misure con livello di priorità (scadenza) bassa;