Allegato A1

Disciplinare Tecnico

DISCIPLINA PER L'ACCESSO AI SERVIZI CLOUD REGIONALI PER ENTI COMUNALI

Codice documento:			
Versione:	**01**		
Data di emissione:		**Stato:**	

INDICE

1. Introduzione

1.1 Il contesto

Come già definito nel "Programma Strategico Semplificazione e Trasformazione Digitale", Regione Lombardia promuove la razionalizzazione delle proprie infrastrutture ICT e offre un reale contributo alla razionalizzazione delle PAL del territorio, adottando un nuovo modello di erogazione dei servizi infrastrutturali basato sul paradigma multicloud ibrido.

Già nel gennaio del 2014 Regione Lombardia con il supporto di ARIASPA (ex Lombardia Informatica) ha definito il piano triennale regionale per la trasformazione e razionalizzazione delle infrastrutture ICT delle pubbliche amministrazioni del territorio regionale, perseguendo i seguenti obiettivi:

- offrire servizi ICT con livelli di servizio in linea con gli standard di mercato;
- ridurre i costi operativi tipici dei data center (consumi elettrici, manutenzione, ecc);
- recuperare, ove possibile, spazi occupati dalle sale CED locali;
- rispondere alle specifiche direttive afferenti all'ambito ambientale.

In considerazione della specifica natura e dei diversi gradi di autonomia degli enti amministrativi coinvolti, è stato ritenuto opportuno organizzare il Piano secondo tre macro-aree di focalizzazione suddivise in:

- Ente Regione Lombardia e sue società strumentali;
- Aziende Socio Sanitarie Territoriali (ASST e ATS);
- Enti locali del territorio lombardo (Province, Comuni, Comunità montane, ecc.).

Il Piano è stato successivamente attuato con l'avvio nel maggio 2017 della gara "Procedura ristretta ai sensi dell'art. 61 del D.lgs. 50/2016 per l'Outsourcing dei servizi strumentali alla gestione ed alla evoluzione delle infrastrutture tecnologiche di Lombardia Informatica S.p.a. funzionali all'erogazione dei servizi applicativi".

La strategia di trasformazione digitale di Regione Lombardia e della sua società in house ARIASPA, ha identificato nel paradigma cloud il modello operativo per

soddisfare le crescenti richieste di agilità rispetto ai tempi di deployment di un nuovo servizio, di resilienza dei servizi per i cittadini ed imprese lombarde e di ottimizzazione dei costi infrastrutturali ICT.

Il Piano di consolidamento e razionalizzazione dei CED della Pubblica Amministrazione che Regione Lombardia è impostato sui seguenti obiettivi:

- Attuare il processo di trasformazione digitale su due direttrici:

  1. la razionalizzazione delle proprie infrastrutture, consolidando gli attuali 4 data center regionali in un unico moderno Data Center, con rilevanti risparmi in termini di riutilizzo delle facility e ottimizzazione dei costi energetici (power&cooling) e di esercizio;

  2. la migrazione verso il cloud pubblico di almeno il 70% dei servizi regionali erogati attualmente sulle proprie infrastrutture, con una riduzione significativa del parco infrastrutturale installato e, grazie all'approccio cloud first, senza più acquisire nuovo hardware all'interno dei propri data center per realizzare nuovi servizi.

- Offrire tale modello di trasformazione anche alle altre PP.AA del territorio lombardo per fruire dei benefici di tale approccio, promuovendo economie di scala dei costi ICT infrastrutturali ed incrementando i livelli di continuità operativa del "sistema regionale" nel suo complesso.

Solo In Lombardia sono presenti circa 2.000 CED distribuiti presso la quasi totalità delle Pubbliche amministrazioni locali e sanitarie.

Dal punto di vista tecnologico, la razionalizzazione delle infrastrutture ICT adotta il modello di erogazione dei servizi basato sul paradigma multi-cloud ibrido, che abilita ARIASPA al ruolo di broker dei servizi innovativi disponibili sulle principali piattaforme cloud pubbliche.

Tale strategia è in linea con l'impostazione complessiva che vede già ARIASPA qualificata come Cloud service provider per erogare servizi ad altre PP.AA, mantenendo il pieno controllo sulla "centralità del dato" e perseguendo importanti risparmi di spesa ICT corrente sul territorio regionale.

Per attuare tali traguardi, ARIASPA ha indetto e aggiudicato una gara per attuare "industrialmente" il processo di razionalizzazione dei CED delle PP.AA, selezionando il partner tecnologico in grado supportare questo processo di trasformazione dall'attuale modello "IT centric" al modello "IT as a Service".

1.2 La strategia per la PAL lombarda

Regione Lombardia con delibera deliberazione N° XI / 106 del 14/05/2018 ha approvato un protocollo di intesa con ANCI Lombardia per l'attuazione di iniziative di innovazione e digitalizzazione dei comuni lombardi ed in particolare la legge Regionale n.20 del 8 luglio 2015 esplicita il tema della razionalizzazione dei data center comunali, utilizzando il data center della Regione Lombardia.

Regione Lombardia assume il ruolo di promotore del processo di innovazione presso tutte le PP.AA della regione, identificando un processo di promozione e di supporto a tutte le PP.AA che ormai sono obbligate dalla normativa a perseguire i nuovi paradigmi digitali, ma non hanno la capacità motu proprio di realizzarli.

Il percorso condotto da Regione Lombardia (RL) per la razionalizzazione dei CED degli Enti pubblici lombardi si inserisce nel più ampio "Piano nazionale triennale di razionalizzazione e consolidamento dei CED della Pubblica Amministrazione", la cui predisposizione è stata normativamente affidata all'Agenzia per l'Italia Digitale (AgID) ai sensi dell'articolo 33-septies del decreto legge 18 ottobre 2012 n. 179 convertito nella Legge n. 221/2012, come modificato dall'art. 16 del decreto legge del 21 giugno 2013 n. 69.

Regione Lombardia ha contribuito al vasto Piano nazionale, tramite il proprio Piano regionale (di seguito, il Piano), contenente la declinazione della strategia di razionalizzazione degli Enti regionali, degli Enti Sanitari pubblici e degli altri Enti amministrativi locali (quali Province, Comuni, Comunità montane, ecc.) del proprio territorio.

In coerenza con quanto previsto da AgID nelle "Linee Guida per la razionalizzazione della infrastruttura digitale della Pubblica Amministrazione", il Piano contempla percorsi di consolidamento che indicano nella centralizzazione e armonizzazione

infrastrutturale la strategia di indirizzo per consentire alle Pubbliche Amministrazioni di affrontare specifiche tematiche su cui sono direttamente coinvolti, e in particolare:

- offrire servizi ICT con livelli di servizio in linea con gli standard di mercato;
- ridurre i costi operativi tipici di un data center (consumi elettrici, manutenzione, ecc);
- recuperare gli spazi attualmente occupati dalle sale CED locali;
- rispondere alle specifiche direttive in ambito ambientale.

Il processo di razionalizzazione delle infrastrutture di un Ente prevede due fasi distinte:

1) Fase di progettazione per identificare la migliore strategia di migrazione in cloud dei servizi applicativi. Tale attività è stata strutturata nella gara con un costo una tantum.
2) Fase di erogazione del servizio Cloud il cui costo operativo è un canone pay x use, in funzione delle risorse virtuali realmente utilizzate.

1.3 Il processo di razionalizzazione dei CED degli Enti sanitari regionali

Nel corso del periodo 2015 – 2020 LISPA, ora ARIASPA, ha dato corso con successo alla fase progettuale di consolidamento e razionalizzazione dei CED di 10 ASST, 2 ATS e 2 Fondazioni ASST.

Sulla base della qualità dei servizi offerti e per i benefici in termini di resilienza e di economicità dei servizi il progetto si è esteso e sta gradualmente raggiungendo la totalità delle aziende sanitarie.

Tale progetto ha consentito alle aziende di dotarsi delle infrastrutture necessarie per lo sviluppo e l'evoluzione dei loro centri elaborazione dati, cogliendo inoltre i seguenti ulteriori benefici:

1) La migrazione dei sistemi informativi in essere presso i CED delle ASST verso nuovi ambienti infrastrutturali ed operativi conformi allo stato dell'arte

tecnologico, allineati a standard implementativi consolidati, secondo le "best practice" di riferimento;

2) L'alleggerimento in capo alle singole ASST degli oneri e della complessità gestionale di erogazione dei servizi informativi attualmente a loro carico, permettendo loro di concentrare la propria attenzione all'esecuzione di attività applicative a maggior valore;

3) L'incremento del livello di misurabilità e controllo dei costi ICT.

1.4 Glossario

AgID	Agenzia per l'Italia Digitale
ARIA	Azienda Regionale per l'Innovazione e gli Acquisti
DC	Data Center
DR	Disaster Recovery
EL	Ente Comunale, provinciale, Consorzio di Comuni, Comunità montana
EE.LL.	Enti Comunali, provinciali, Consorzi di Comuni, Comunità montane
MPLS	Multi Protocol Label Switching
RA	Reference Architecture
RL	Regione Lombardia
RPO	Il Recovery Point Objective (RPO) fornisce la misura della massima quantità di dati che il sistema può perdere a causa di guasto improvviso.
RTO	Il Recovery Time Objective (RTO) è il tempo necessario per il pieno recupero dell'operatività di un sistema
SLA	Service Level Agreement (livelli di servizio)
VDC	Virtual Data Center
VPN	Virtual Private Network (rete privata virtuale)
WAN	Wide Area Network (rete dati geografica)

2. Soggetti ricompresi nell'iniziativa

2.1 Soggetti negli allegati A1 e A2 della legge regionale n. 30/2006 (Sireg)

I soggetti di cui all'allegato A1 e A2 della Legge Regionale n. 30/2006 possono fruire dei servizi cloud e dei relativi servizi di migrazione del parco applicativo, sottoscrivendo un accordo di collaborazione tra Regione Lombardia, ARIASPA ed Ente con i relativi ristori dei costi incrementali, in conformità alla Legge 136/2010 e al decreto del Presidente del Consiglio dei ministri 30 giugno 2011 come determinato nel paragrafo "CRITERI DI QUANTIFICAZIONE E MODALITA' DI RISTORO DEI COSTI".

2.2 Amministrazioni pubbliche con sede nel territorio della Regione Lombardia

Le Amministrazioni con sede nel territorio della Regione possono fruire dei servizi cloud e dei relativi servizi di migrazione del parco applicativo, previa stipula di accordo bilaterale con ARIASPA che preveda il ristoro dei costi calcolati secondo le modalità previste nel paragrafo "CRITERI DI QUANTIFICAZIONE E MODALITA' DI RISTORO DEI COSTI".

3.I servizi previsti

I servizi previsti per gli Enti e PP.AA. sono descritti nel catalogo dei servizi infrastrutturali appositamente progettati per perseguire la razionalizzazione delle infrastrutture ICT pubbliche.

Gli Enti potranno scegliere diversi livelli di supporto per la gestione operativa della propria infrastruttura, sulla base delle classi di servizio che identificano il livello di criticità di un servizio applicativo dell'Ente.

Un'importante distinzione che definisce i perimetri di progetto e di erogazione del servizio è data dalla tipologia del servizio che si andrà ad erogare:

- IaaS
- Full Managed

3.1 Servizi di progettazione e migrazione delle applicazioni in cloud

Per gli Enti che sottoscrivono l'accordo di collaborazione, ARIASPA progetta e realizza la migrazione dei servizi applicativi utilizzati presso i CED degli EE.LL. Sono previste le seguenti fasi:

- Analisi preliminare: in questa fase si effettua una panoramica della situazione attuale dell'Ente e dei suoi servizi sia dal punto di vista tecnico che gestionale;
- Assessment: in questa fase, ripetuta per ogni servizio da migrare, si analizzano dal punto di vista tecnico i server che erogano il servizio e le loro componenti (DB, AppSvr, Flussi, etc.);
- Progettazione: in questa fase, ripetuta per ogni servizio da migrare, si studia come ridisegnare il servizio seguendo le linee guida architetturali previste e si studia una possibile strategia di migrazione che si condivide con l'Ente;
- Realizzazione: in questa fase, ripetuta per ogni servizio da migrare, si predispongono, all'interno del DataCenter o nel Cloud di ARIASPA, le VM così come previsto dalla progettazione e si consegnano alle Software House per il rilascio della parte software e per i test pre-migrazione;
- Migrazione: in questa fase, ripetuta per ogni servizio da migrare, si concorda con l'Ente data, ora e durata del fermo per la migrazione del servizio. A seguire sono effettuati tutti i test di collaudo per certificare l'avvenuta migrazione.

Il ristoro dei costi relativi a tale servizio è una tantum.

3.2 I servizi di Virtual Data Center

I servizi di Virtual Data Center (VDC) sono costituiti dall'insieme dei servizi abilitanti e necessari all'erogazione delle applicazioni degli Enti e comprendono in parte o totalmente i servizi di gestione operativa relativi a:

- tecnologie impiantistiche (impianti elettrici, raffreddamento, antincendio, etc.);
- guardianato e controllo accessi;
- infrastruttura di rete;
- infrastruttura di sicurezza di rete;
- infrastruttura di virtualizzazione;
- sistemi storage e di protezione del dato (backup);
- monitoraggio;
- disaster recovery in funzione dei requisiti applicativi e delle classi di servizio individuate.

In particolare, l'infrastruttura messa a disposizione degli Enti potrà essere fornita secondo due modalità:

- **On-premise**: è resa disponibile un'infrastruttura hardware, presso i Datacenter di ARIASPA, comune e condivisa fra gli Enti dove, attraverso tecnologie che garantiscono la "*multi-tenancy*" per l'accessibilità e il controllo delle risorse assegnate, viene garantita la segregazione.
- **On-cloud**: si rende disponibile un'infrastruttura public Cloud dedicata ad ARIASPA, nella quale sarà definito ed organizzato un *tenant* distinto per ogni Ente.

I servizi di VDC possono essere fruiti secondo due modalità distinte illustrate nei paragrafi seguenti:

- IaaS
- Full Managed

Il ristoro dei costi relativi al servizio di VDC è a canone trimestrale.

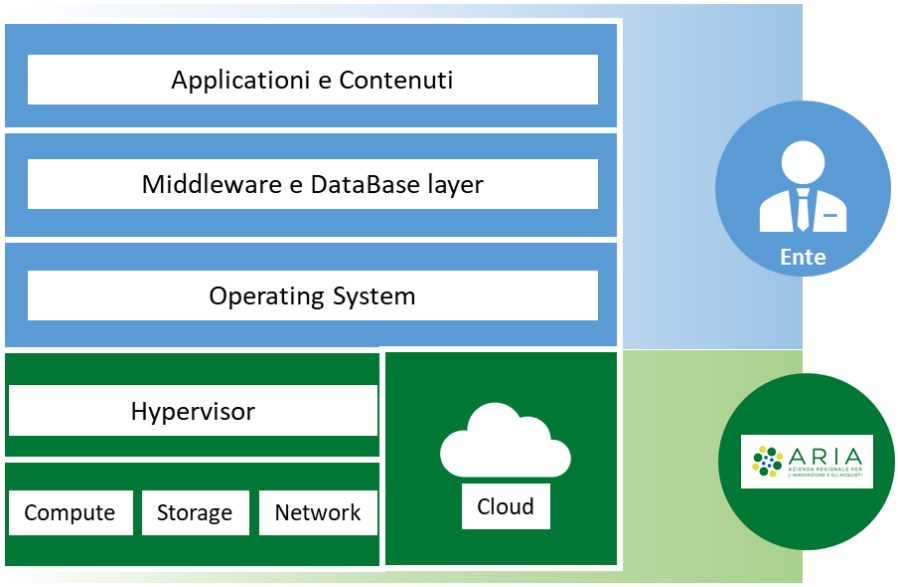
3.2.1 Offerta IaaS

L'offerta IaaS consiste nella messa a disposizione degli Enti di uno o più Virtual Data Center (VDC) remoti che permettano di creare e gestire in completa autonomia risorse virtuali, quali server e aree di storage.
Il servizio include una virtual network preconfigurata per VDC.
Le Virtual Machine saranno rese disponibili in tagli pre-configurati, rispetto al rapporto fra numero di CPU [vCPU] e quantità di RAM [GB]. Sarà inoltre possibile, per ogni VM, configurare aree storage, nelle quantità desiderate, diversificate per tier. I diversi livelli di tier storage offerti garantiscono la copertura delle necessità dell'Ente rendendo disponibili sia tier ad alte prestazioni e bassa latenza sia tier di storage capacitivi per dati di archiviazione, tipicamente a lungo termine.
Sarà sempre possibile effettuare un ridimensionamento delle VM nell'ambito dei tagli pre-configurati, sia in aumento (scale-up) sia in diminuzione (scale-down).
Le tipologie di template resi disponibili per le VM, comprensive di licenza di SO (in Reference Architecture), sono:

- Template con SO Microsoft Windows
- Template con SO Linux Red Hat Enterprise

Per I sistemi non in Reference Architecture sarà data la possibilità di effettuare, ove tecnicamente possibile, l'importazione delle immagini dei sistemi esistenti.

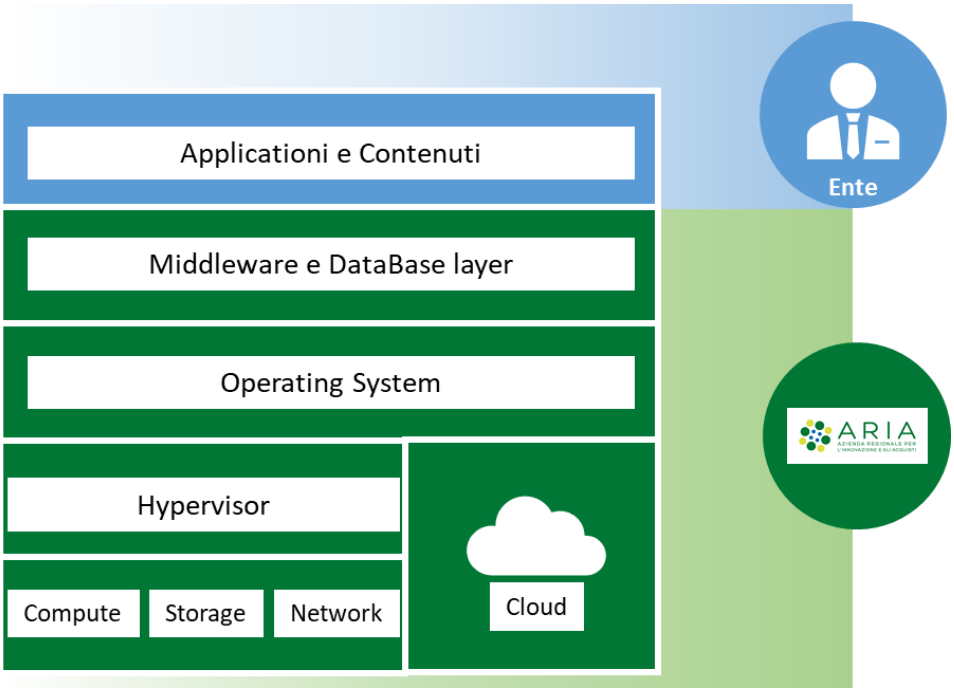
L'aggiornamento delle componenti software presenti nella macchina virtuale (es. patching del Sistema Operativo) è a carico dell'Ente che fruisce del servizio. Nell'immagine che segue sono indicati, per l'offerta IaaS, in blu/azzurro gli ambiti di responsabilità dell'Ente ed in verde quelli di Aria.



3.2.2 Offerta Full Managed

L'offerta Full Managed estende l'ambito di responsabilità di ARIASPA riducendo quello dell'Ente. In questo caso, oltre a quanto descritto nell'offerta IaaS, ARIASPA si occuperà della fornitura e gestione della componente Operating System, Middleware e Database. Resta sempre e comunque a carico dell'Ente la gestione delle componenti applicative e dei loro contenuti, dati compresi.

La figura seguente rappresenta le aree di competenza sulle componenti dei vari layer architetturali per l'offerta Full Managed.



3.3 Il servizio di connettività dati

Per ottenere il massimo valore dal cloud è necessario esaminare il migliore modello di connettività e la scelta del provider di connettività.

Per ottenere tale obiettivo è indispensabile identificare i requisiti di rete (banda, velocità) richiesti per ciascuna applicazione che sarà migrata in cloud.

Per le PAL sono disponibili tre metodi per connettere il provider di servizi cloud (CSP):

1. **Accesso Internet;**
2. **Accesso privato diretto;**
3. **Accesso Interconnesso.**

Ogni metodo presenta i suoi vantaggi, a seconda del caso d'uso aziendale per i servizi cloud.

1. ***Flessibilità del modello di accesso***

Il modello di accesso si basa su un'ampia varietà di tecnologie di connettività, come ad esempio MPLS ed Ethernet e diverse tipologie di porte di connessione. Attraverso la selezione e la combinazione di tali elementi è possibile configurare una soluzione di accesso cloud privata, pubblica o ibrida.

2. ***Accesso in soluzione di continuità***

I metodi di accesso possono includere un'esperienza utente di alta qualità da un capo all'altro della connessione, realizzata attraverso un collegamento effettuato su più punti (Point-of-Presence - PoP) della rete privata del CSP e su più punti d'interscambio pubblici (Internet eXchange Point – IXP) della rete pubblica del CSP.

3. ***Accesso con Service Level Agreement (SLA)***

L'accesso privato diretto è l'unico metodo di connessione in grado offrire uno SLA robusto a livello end-to-end, per garantire la perdita di pacchetti e le prestazioni di rete (latenza) tra l'utente finale e il PoP del CSP. Il provider di connettività scelto è in grado di offrire strumenti di reportistica in tempo reale per la verifica delle prestazioni SLA.

4. ***Accesso con diverse opzioni di larghezza di banda***

I metodi di accesso condividono le opzioni di larghezza di banda offerte dal programma di connettività del CSP e dal provider di connettività in modo che abbiano la flessibilità di scalare al crescere delle esigenze.

3.3.1 Accesso internet

L'accesso al cloud si realizza attraverso una VPN IPSec che interconnette la rete della PAL alla rete virtuale del CSP mediante una connessione internet di qualità.

3.3.1.1Qualità della connessione e scelta del provider di connettività

La qualità della connessione internet è garantita dai seguenti requisiti fondamentali:

1. Utilizzo di un Internet Service Provider (ISP) tier-2, scelto tra quelli della gara SPC-2, che effettua scambio di traffico (peering BGP) direttamente con i CSP attraverso punti d'interscambio pubblici (IXP), tra cui il MIX-IT di Milano, il DE-CIX di Francoforte e/o attraverso partner exchange, come Equinix Cloud Exchange, CoreSite, ecc., con grande capacità di banda e ampio numero di reti IP annunciate;
2. Gli indirizzi IP pubblici per le comunicazioni tra la PAL e il CSP sono assegnati esclusivamente dall'Internet Service Provider (ISP) selezionato.

3. Gli indirizzi IP pubblici per le istanze cloud sono assegnati esclusivamente dal Cloud Service Provider (CSP).
4. È possibile trasferire parte o tutto il piano di indirizzamento IP pubblico di proprietà della PAL al CSP di riferimento. In questo caso la PAL continua a mantenere il possesso degli indirizzi IP pubblici mentre il CSP li annuncia su internet e li assegna alle istanze cloud. (***non possono essere utilizzati indirizzi IP pubblici di proprietà della Regione Lombardia***).
5. Le connessioni lato PAL sono attivate attraverso nuovi link di accesso / gateway dedicati (no esistenti), opportunamente dimensionati in base ai requisiti di rete di ciascuna applicazione che sarà migrata in cloud.

3.3.1.2Sicurezza della connessione

Attraverso la soluzione VPN IPSec è realizzata una piattaforma di sicurezza che garantisce la connettività privata e sicura per le sedi remote della PAL e per utenti mobili.

La soluzione consente la gestione degli utenti roaming che necessitano di un accesso sicuro in mobilità alle risorse aziendali.

Per l'accesso VPN in mobilità è disponibile una duplice soluzione:

1. Client IPSec;
2. Clientless VPN SSL.

Per entrambi i casi sono adottate procedure di strong authentication per garantire l'accesso ai soli utenti autorizzati.

3.3.1.2.1 Garanzia delle informazioni

L'assicurazione delle informazioni include la protezione dell'integrità, della disponibilità, dell'autenticità, del non ripudio e della riservatezza dei dati della PAL.

Pertanto, il metodo di accesso garantisce le seguenti operazioni, ovunque tra i gateway IPSec:

- Protezione da intercettazioni; riservatezza dei dati;
- Protezione dall'inserimento di pacchetti non validi poiché l'origine dei pacchetti è autenticata;
- Autenticazione dei pacchetti inviati dal mittente IPsec; garanzia dell'integrità dei pacchetti;
- Protezione da replay di pacchetti vecchi o duplicati; anti-replay.

3.3.1.2.2 Certificazione della protezione dei dati

La certificazione della protezione dei dati si basa su standard di riferimento:

- Common Criteria (CC): Standard internazionale mirato a profili di protezione predefiniti e certificati (protection profile), relativi a tipologie omogenee di prodotti;
- FIPS 140-2: Standard Americano e Canadese mirato alla valutazione dei sistemi basati su crittografia, complementare ai Common Criteria.

L'attenzione si rivolge alla sicurezza dei prodotti utilizzati per la protezione dei dati [Common Criteria (CC)] e al modello di erogazione del servizio di cifratura, che richiede attenzione anche verso i processi organizzativi sulla corretta gestione della sicurezza degli algoritmi nel tempo (FIPS140-2).

3.3.1.2.3 Gestione degli algoritmi e delle chiavi di cifratura

La gestione delle chiavi si realizza attraverso la pianificazione delle possibili modifiche all'utilizzo degli algoritmi durante tutto l'arco temporale del contratto.
Tale gestione include la transizione da un algoritmo o lunghezza della chiave a un altro nel momento che questi sono dichiarati insicuri o per la disponibilità di nuove tecniche di crittografia più potenti.

L'approccio adottato per la transizione degli algoritmi o lunghezza delle chiavi è quello descritto nelle pubblicazioni speciali del National Institute of Standard and Technology (NIST).
Le raccomandazioni del National Institute of Standard and Technology (NIST) hanno lo scopo di fornire dettagli sulle transizioni associate all'uso della crittografia per la protezione di informazioni sensibili ma non classificate. La raccomandazione e le

relative revisioni affrontano l'uso degli algoritmi e delle lunghezze di chiave, aggiornano la guida alla transizione fornita nella versione precedente.

3.3.2 Accesso privato diretto

L'accesso si realizza attraverso una connessione Wan privata e diretta al PoP di accesso alla rete del CSP.

3.3.2.1Programma di connettività dei CSP e scelta del provider di connettività

La connessione Wan è realizzata da un provider di connettività, scelto tra i fornitori della gara SPC-2 e presente nelle liste dei partner di recapito dei programmi di connettività dei CSP di riferimento:

- Programma di connettività AWS Direct Connect di Amazon;
- Programma di connettività ExpressRoute di Microsoft;
- Programma di connettività Google Cloud Interconnect;

L'insieme delle tecniche considerate corrette per l'esecuzione dei programmi sopraindicati è garantita dal network provider che ha superato la convalida del programma di recapito della connettività per consentire ai propri clienti di accedere ai CSP di riferimento.

Per ogni programma di connettività sono disponibili le seguenti tecnologie di connessione, che si pongono in modo trasparente tra la PAL e il CSP:

- Ethernet;
- IP VPN MPLS.

3.3.2.1.1 Direct Connect Amazon

Sono disponibili due opzioni di servizio Direct Connect associabili al circuito fornito dal network provider:

1. Servizi forniti su **dedicated port** per connessioni con ampiezze di banda fino a 10Gbps. L'opzione con porta dedicata supporta diverse applicazioni AWS (es: EC2, ecc) per circuito e permette alla PAL il controllo diretto della banda.
2. Servizi forniti su **hosted port** per connessioni con ampiezze di banda disponibili sotto il 1Gbps tramite interfaccia condivisa (Network-to-Network Interface - NNI). L'opzione con interfaccia condivisa con altri clienti supporta una sola applicazione AWS per circuito e non permette alla PAL il controllo diretto della banda.

La tabella seguente mostra la gamma di larghezze di banda offerte dal CSP e le relative tecnologie di connettività disponibili.

Banda AWS	Connessione ad AWS	Ethernet	IP VPN MPLS	PoP di accesso Direct Connect
100-500 Mbps	Hosted connection	si	si	PoP in Milano per Region UE (Francoforte)
1Gbps/10Gbps	Dedicated port	si	no	

3.3.2.1.2 ExpressRoute Microsoft

È disponibile un'opzione di servizio Google Cloud Interconnect associabile al circuito fornito dal network provider:

1. Servizi forniti su **interfaccia condivisa** (Network-to-Network Interface - NNI) per connessioni con ampiezze di banda fino a 10Gbps.

La tabella seguente mostra la gamma di larghezze di banda offerte dal CSP e le relative tecnologie di connettività disponibili.

Banda Azure	Connessione ad Azure	ETHERNET	IP VPN MPLS	PoP di accesso ExpressRoute
50/100/200/500 Mbps, 1Gbps	NNI condiviso	si	si	PoP in Milano per Region UE (Francoforte)
2/5/10Gbps		si	su richiesta	

3.3.2.1.3 Google Cloud Interconnect

Sono disponibili due opzioni di servizio Google Cloud Interconnect (GCI) associabili al circuito fornito dal network provider:

1. Servizi forniti su **dedicated port** per connessioni con ampiezze di banda fino a 10Gbps;

2. Servizi forniti su **partner port** per connessioni con ampiezze di banda fino a 10Gbps tramite interfaccia condivisa (Network-to-Network Interface - NNI).

La tabella seguente mostra la gamma di larghezze di banda offerte dal CSP e le relative tecnologie di connettività disponibili.

Banda Google	Connessione a Google	ETHERNET	IP VPN MPLS	PoP di accesso Google Cloud
50Mbps-10Gbps	Interconnect Partner port	si	si	PoP in Milano per Region UE (Francoforte)
10Gbps	Interconnect dedicated	si	si	

3.3.3 Accesso interconnesso

L'accesso si realizza attraverso una connessione Wan diretta a un cloud interconnect (partner exchange) che ha connettività verso un gran numero di CSP geograficamente distribuiti.

3.3.3.1Programma di connettività dei CSP e scelta del partner exchange

Il network provider, scelto tra i fornitori della gara SPC-2, si connette al partner exchange, come Equinix Cloud Exchange, CoreSite, Telx, ecc, per scambiare il traffico privato. I CSP di riferimento dispongono di connettività verso questi partner exchange che sono geograficamente distribuiti e, in molti casi, condividono lo stesso sito.
I programmi di connettività dei CSP, le larghezze di banda, le tecnologie di connessione e le opzioni di servizio sono le medesime indicate per l'accesso privato diretto.

3.4 Servizio opzionale di supporto alla trasformazione digitale

L'Ente che sottoscrive la collaborazione con ARIASPA per la progettazione ed erogazione dei servizi cloud potrà richiedere, oltre ai servizi già previsti all'interno del progetto di migrazione, specifici servizi opzionali di supporto specialistico su:

- Revisione tecnologica su quanto rimasto ancora presso il DataCenter dell'Ente;
- Processi di trasformazione digitale dell'Ente.

I servizi opzionali saranno erogati grazie al supporto di figure specialistiche nei vari ambiti, sia tecnologici che gestionali, ma i costi sono da considerarsi al di fuori del perimetro della migrazione e il ristoro degli stessi è a misura di risorsa.

3.5 Servizio Implementazione Virtual Desktop (VDI)

L' infrastruttura VDI verrà erogata in modalità Cloud in modo da garantire all'utente una modalità d'uso e prestazioni del tutto analoghe a quelle che si avrebbero utilizzando PC fisici reali.

La soluzione VDI sarà in grado di:

- replicare il livello di prestazioni e di esperienza utente degli attuali sistemi HW (CPU, RAM, Spazio disco, risoluzione);
- supportare l'attuale parco applicativo in uso e le relative periferiche;
- soddisfare gli stessi requisiti di sicurezza e continuità definiti per le PdL non virtualizzate nel rispetto della normativa e delle policy di Aria;
- offrire una disponibilità H24 del servizio.

La soluzione di virtualizzazione sarà erogata da un'infrastruttura cloud comprensiva di:

- capacità elaborativa per la gestione delle immagini;
- spazio disco per applicazioni e dati utente;
- strumenti di monitoraggio e logging adeguati alle policy di ARIASPA non gestiti direttamente dal Fornitore che ne deve tuttavia assicurare la fruibilità e la conformità di quanto registrato;
- licenze software necessarie.

Di seguito sono descritti i principali requisiti che la soluzione deve soddisfare:

- possibilità di utilizzare la più ampia tipologia di dispositivi fisici: Desktop, Notebook, Thin Client, Tablet PC;

- piena compatibilità con le principali suite di produttività personale (ad es. Microsoft Office, Open Office) e di collaborazione (ad es. Lotus Mail, Microsoft Exchange);
- accesso a documenti, applicazioni e risorse;
- erogazione del servizio di virtualizzazione da una libreria di "immagini di desktop virtuali", per garantire rapide migrazioni e la possibilità di ripristinare precedenti versioni;
- possibilità di condividere una medesima immagine fra più utenti mantenendo gli elementi di personalizzazione e profilazione (es. mailbox, risorse condivise, ecc.);
- supporto della stampa in locale e di stampanti di rete;
- possibilità di effettuare il provisioning di più virtual desktop contemporaneamente;
- disponibilità di una console di gestione web-based;
- possibilità di monitorare lo stato di integrità e i parametri della connessione di singoli virtual desktop;

Sotto il profilo della sicurezza la soluzione:

- consente l'accesso e la connessione al desktop virtuale o alle applicazioni virtuali solo alle persone autorizzate;
- utilizza le credenziali impostate da un amministratore oppure le credenziali dell'Active Directory esistenti;
- garantisce il supporto Multi-Factor Authentication (MFA);
- supporta la possibilità di impostare policy per gruppi di utenti;
- garantisce l'adeguato livello di sicurezza e riservatezza alle comunicazioni "end-to-end";
- supporta la possibilità di crittografare i dati/volumi utente.

Inoltre, l'infrastruttura sarà attivabile tramite prodotti di registrazione nel caso di accesso diretto agli ambienti con dati reali in ottemperanza alla normativa vigente.

4. Classi di servizio

In funzione della tipologia di servizio di cui l'Ente intende avvalersi, è prevista un'offerta differenziata dei livelli di servizio previsti e delle modalità di gestione dei servizi applicativi

4.1 Offerta IaaS

Nel caso dell'offerta IaaS, ARIASPA garantisce la messa a disposizione delle risorse computazionali, la fornitura e gestione del layer di virtualizzazione, dei servizi di rete ed una funzionalità base di Backup denominata Data Recovery. Questa modalità, se attivata, prevede l'esecuzione di un full backup settimanale con "retention" di un mese, replicato su due siti, di tutte le VM ospitate nel VDC di ARIASPA. Lo storage utilizzato per ospitare il backup è contabilizzato all'Ente a parte.

4.2 Offerta Full Managed

Nel caso dell'offerta Full Managed, ARIASPA garantisce la messa a disposizione delle risorse computazionali, la fornitura e la gestione di :

- layer di virtualizzazione,
- sistema operativo,
- database,
- middleware,
- storage,
- servizi di rete,
- servizi di sicurezza
- Backup
- Cloud management platform
- Piattaforme di monitoraggio, performance, capacity, cmdb, service desk

In questa tipologia di offerta i servizi applicativi possono essere classificati dall'Ente in funzione delle specifiche esigenze in termini di resilienza architetturale, di livelli di servizio desiderati e di tempi di intervento e rilascio garantiti. I servizi più critici dispongono quindi di architetture a massima resilienza e supporto sistemistico prioritario. Per contro tali servizi hanno un incremento dei costi unitari come evidenziato dal modello di ristoro dei costi riportato nel documento di "Accordo di collaborazione".

Di seguito si presenta una tabella che riassume le diverse opzioni di livello di servizio disponibili e le funzionalità garantite per i diversi ambiti previsti dall'offerta Full Managed.

		Mission Critical	Business Premium	Business Standard	Basic
		Ambienti per le applicazioni definite dall'Ente come essenziali e su cui ARIASPA deve garantire il ripristino dei servizi con un intervallo minimo di disservizio	Ambienti che supportano le applicazioni fondamentali su cui ARIASPA realizza soluzioni in alta affidabilità con il massimo livello di supporto operativo	Ambienti che supportano sistemi di produzione a basso rischio consentendo un'ottimizzazione infrastrutturale con un adeguato livello di supporto	Ambienti che supportano i sistemi che vengono utilizzati per lo sviluppo, test, formazione, preproduzione o produzione con livelli minimi di supporto
Disaster Recovery		✓	✓		
Servizi Dedicati					
	APM con agent	✓			
	APM Agentless	✓	✓		
	Capacity	✓	✓		
	Monitoraggio con agente	✓			
	Monitoraggio senza agente	✓	✓	✓	✓
	Test sintetici end2end (robot)	✓			
Gestione Incident	Presidio Incident Manager	24X7	8-20X7	9-18X5	9-18X5
	Gestione Operativa Incident	24X7	24X7	24X7	24X7
	Disponibilità Incident Report	2 gg	3 gg	5 gg	7gg
Gestione Change	Major	15 gg	20 gg	20 gg	25 gg
	Minor	4 h	6 h	8 h	8 h

5. PROCESSI OPERATIVI

I processi operativi definiscono le regole di interscambio di informazioni e segnalazioni tra L'Ente e ARIASPA.
Di seguito sono elencati i principali processi operativi secondo la metodologia ITIL, ma ancor prima è meglio spiegare la figura dell'ITSM e il suo ruolo.

5.1 Il ruolo dell'ITSM

L'ITSM rappresenta la figura di raccordo tra gli EE.LL e i processi di gestione dei servizi erogati presso il DataCenter o il Cloud di ARIASPA.

Le principali responsabilità sono

- Garantire e monitorare l'erogazione operativa dei servizi;
- Garantire la coerenza delle soluzioni prospettate in ottica: architetturale, sicurezza e privacy basandosi sulle linee guida indicate da ARIASPA o dagli Enti preposti come AGID
- Garantire il rispetto agli SLA contrattuali e produrre, su richiesta, reportistica a supporto;
- Coinvolgere e supportare la funzione del Demand nella valutazione tecnico-economica degli interventi di evoluzione dei servizi e/o nella definizione di nuovi servizi;
- Gestione dei processi ITIL di seguito descritti verificando tempi e modi di evasione delle varie tipologie di richieste degli EE.LL.

5.2 Introduzione alla funzione di Service Desk

Il Service Desk è la funzione che rappresenta il punto unico di contatto per gli EE.LL, è disponibile per la gestione delle richieste di servizio o informative e per l'assistenza sull'infrastruttura tecnologica erogata dal Datacenter o dal Cloud.
Attraverso la funzione Service Desk vengono gestiti i seguenti eventi:

- Incident

- Change
- Service Request

Il Service Desk:

- è fruibile in modalità multicanale: telefono, mail, self ticketing mediante ServiceNow;
- si occupa di smistare verso il corretto gruppo di competenza le richieste pervenute e si pone come obiettivi:
  - istituire un unico punto di raccolta per tutte le possibili problematiche dell'utente;
  - offrire all'utenza un supporto omogeneo, costante e misurabile attraverso una struttura specialistica e gli opportuni supporti informatici;
  - disporre di una knowledge base affidabile relativa alle richieste pervenute ed ai livelli di servizi erogati.

5.3 Incident Management

Nell'ambito del presente modello di gestione sono gestiti eventi secondo la seguente classificazione:

Voce	Descrizione
Incident (o Anomalia)	Qualsiasi evento in grado di interferire sulla normale operatività, alterando le performance e/o provocando delle conseguenze dirette in termini di disponibilità di servizio.
Problem	Causa di uno o più Incident, relativi a componenti di infrastruttura o componenti applicative. Un Problem per il quale sono noti causa e soluzione costituisce un "known error".

La raccolta delle richieste e segnalazioni è in carico al gruppo Service Desk, operativo H24 7x7, secondo le modalità di seguito indicate.

Tipo Servizio	Giorni	Orari	Canale di Accesso	Riferimento
Service Desk	Lun-Ven	09.00 – 18.00	Telefonico	ITSM di competenza
	Lun-Dom	H24	e-mail *	supportoXXX@ariaspa.it
Reperibilità	Lun-Ven	18.00 – 09.00	Telefonico	ITSM Reperibile
	Sab–Dom	H24		

Per la gestione degli Incident la modalità è definita dalla classe di servizio assegnata al servizio; la tabella riassuntiva è presente nel capitolo 6.
La priorità può essere valutata in funzione di:

- **urgenza**: valutazione di quanto rapida deve essere la sua risoluzione;
- **impatto**: valutazione da compiere in relazione alla tipologia di servizio oggetto della problematica riscontrata.

5.4 Request Fullfilment

Si definisce Service Request un'esigenza generica che non comporta modifiche all'infrastruttura, ovvero tutte quelle richieste di intervento sui sistemi previste nell'ambito del servizio e che non hanno impatti sulle funzionalità dei servizi e delle infrastrutture.
Sono definite le seguenti tipologie di richieste:

- Gestione delle Utenze (server, database, application server, etc.)
- Recupero password
- Report generici sull'erogazione dei servizi
- Informativa su configurazione delle VM
- Informativa su configurazione componenti middleware e database
- Backup

- Restore
- Richieste inerenti alla valorizzazione economica del contratto

5.5 Change Management

Il Change Management si occupa della gestione delle Change Request ovvero le richieste formali di implementazione di un cambiamento nell'ambito della fornitura dei servizi erogati, aventi un impatto sull'infrastruttura HW, SW, sistemi di base e applicativi in esercizio.
La Change viene classificata come segue:

Voce	Descrizione
MAJOR CHANGE	Riguardano l'attivazione di nuovi servizi/infrastrutture o cambiamenti ai servizi/infrastrutture esistenti di elevata complessità e il loro perfezionamento richiede il coinvolgimento di più strutture aziendali. A fronte della loro complessità i "requisiti" del "cambiamento" devono essere formalizzati in modo strutturato mediante una RFC
MINOR CHANGE	Sono esigenze di cambiamento di bassa complessità, di norma riguardano una sola attività, la cui esecuzione può seguire modelli standardizzati e/o è espletabile da gruppi specialistici in autonomia.

5.5.1 Processo di gestione dei Major change

Il referente operativo dell'Ente attiva il processo di change management fornendo i macro requisiti infrastrutturali all'ITSM attraverso un template standard. ARIASPA analizza la fattibilità economica con le strutture preposte al controllo economico del progetto.
Una volta avuta la fattibilità l'ITSM attiva il processo interno di RFC, definisce un piano con tutti gli attori coinvolti e mantiene allineati tutti durante l'esecuzione della change.

5.5.2 Processo di gestione dei Minor change

I tempi di esecuzione delle change di tipo minor sono regolamentati rispetto alla relativa classe di servizio associata.

5.6 Gestione dei Rilasci applicativi nell'offerta Full Managed

Il processo di Release Management governa la pianificazione, schedulazione, esecuzione e controllo del passaggio in ambienti di preproduzione e/o di produzione dei rilasci. Il principale obiettivo del Release Management è effettuare il rilascio dei componenti assicurando nel contempo la protezione e l'integrità degli ambienti.
I fermi determinati da interventi di Release non saranno conteggiati come disservizi all'interno degli SLA, la gestione del processo di Release prevede la pianificazione congiunta tra ARIASPA e l'Ente per la gestione dei fermi.
Il processo è valido per tutti i sistemi in carico ad ARIASPA, comprende quindi sia i sistemi di produzione che preproduzione
Una volta approvata e pianificata una richiesta di cambiamento che implichi un rilascio in produzione, il processo di Release Management è attivato per regolamentare e gestire le attività necessarie, nel rispetto dei vincoli e della pianificazione della richiesta di cambiamento.
La responsabilità del rilascio e l'esecuzione delle attività associate sono in carico all'Ente, tramite utenze ad-hoc che dispongono dei privilegi necessari (es. creazione tabella, modifiche alla configurazione dell'application server), che deve quindi definire i contenuti della release, le attività, il piano di installazione e di rollback e alla compilazione delle Release Notes, sulla base di un template.
In ogni caso ARIASPA deve essere informata sulle attività e sul perimetro e validare le release notes, che devono prevedere anche eventuali azioni in carico ad ARIASPA, quali ad esempio la creazione di uno snapshot della VM.

6. Livelli di servizio

I livelli di servizio di seguito presentati sono garantiti in base alla classe assegnata al servizio in fase di assessment e/o rivista e confermata in sede di completamento del moving.

Servizi Dedicati		IAAS	Full Managed			
			MCRT	BPRM	BSTD	Basic
Livelli di Servizio	**Disponibilità Servizio**	99,20%	99,90%	99,80%	99,60%	99,20%
	Full Backup	Settimanale Retention un mese				
	RTO	24h	4h	4h	24h	24h
	Limite Indisponibilità	300min	60min	120min	180min	300min
	RPO	n.a.	0h	1h	2h	4h
Gestione Incident	**Presidio Incident Mgr**	9-18x5	24x7	8-20x7	9-18x5	9-18x5
	Disponibiità Incident Report	7gg	2gg	3gg	5gg	7gg
Gestione Change	**Major**	25gg	15gg	20gg	20gg	25gg
	Minor	8h	4h	6h	8h	8h

Tabella 1: SLA Servizi Data Center

Connettività (*)	
Disponibilità annua del servizio di connettività	99,99%
Tempo massimo di ripristino per guasti bloccanti (l'utente non è in grado di usufruire del servizio per indisponibilità o perché le prestazioni risultano decisamente	4 ore nel 95% dei casi
	8 ore nel 100% dei casi
Tempo massimo di ripristino per guasti non bloccanti (l'utente è in grado di usufruire, ma con prestazioni degradate)	16 ore nel 95% dei casi
	32 ore nel 100% dei casi

(*) Sono riportati gli SLA previsti dalla convenzione Consip SPC2

Tabella 2: SLA Servizi di Connettività

7.Governo della Sicurezza e protezione dei dati personali

Il Regolamento UE 2016/679 (Regolamento Europeo in materia di protezione dei dati personali, di seguito GDPR), il D.Lgs. 196/03 (Codice in matereria di protezione dei dati personali di seguido codice) nonché i Provvedimenti emanati dall'Autorità Garante per la Protezione dei dati personali, si prefiggono di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
La Normativa richiede in particolare:

- la necessità di strutturare e mettere in atto un'organizzazione specifica per la Privacy attraverso l'identificazione di opportuni ruoli e le relative procedure di nomina;
- un insieme di misure di sicurezza che devono essere applicate con lo scopo di assicurare un livello adeguato di protezione dei dati.

L'Autorità Garante per la Protezione dei dati personali ha inoltre espresso misure e accorgimenti specifici per i titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema (Provvedimento del 27 novembre 2008 e s.m.i.).

Oltre all'applicazione delle misure di sicurezza, il trattamento dei dati personali, da parte di ARIASPA e suoi Subfornitori, dovrà sempre ispirarsi al rispetto dei principi generali del Codice e del GDPR e quindi avvenire in modo lecito e secondo correttezza, valutando la pertinenza, la completezza e la non eccedenza dei dati rispetto alle finalità dei trattamenti in funzione delle attività assegnate.
In particolare, si evidenzia il principio di necessità (art.3) che prevede che gli strumenti elettronici siano configurati in modo da ridurre al minimo l'utilizzo di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite

possano essere realizzate mediante altri strumenti quali dati anonimi o altre modalità che permettano di identificare l'interessato solo in caso di necessità.

L'evoluzione della normativa sulla privacy, mediante la pubblicazione di provvedimenti, regolamenti, ecc. ad hoc da parte dell'Autorità Garante, ha richiesto e potrebbe richiedere in futuro, l'implementazione di misure di sicurezza ulteriori rispetto a quanto già contemplato nel già citato Codice. ARIASPA valuterà la possibilità di considerare e applicare ogni ulteriore misura che potrà derivare dall'evoluzione normativa.

Inoltre, come previsto dal GDPR, deve essere adottato un approccio basato sulla Security e Privacy by Design e by Default che prevede l'adozione di adeguate misure di sicurezza a tutela di tutto il ciclo di vita del trattamento dei dati personali. Tali misure non sono definite puntualmente dalla normativa ma devono essere selezionate dal Titolare e Responsabili attraverso opportune attività di analisi e verifica dei trattamenti e dei potenziali impatti in termini di privacy. ARIASPA garantirà il rispetto di tali misure e, al contempo, delle misure di sicurezza identificate come necessarie ed opportune da parte del Ente.

7.1 Servizi di sicurezza dei DC di ARIA

Di seguito vengono descritti i servizi disponibili:

1. servizio di hardening dei sistemi;
2. servizio di gestione utenze di Amministrazione dei Sistemi;
3. servizio di gestione configurazioni sugli apparati di sicurezza;
4. servizio di antivirus e antimalware sui sistemi
5. servizio di patching;
6. servizio di security monitoring;
7. servizio di monitoraggio applicativo
8. servizio di identity access management
9. servizio di logging
10. servizio di protezione delle basi dati
11. servizio di anti-DDOS
12. servizio di detection e blocking di attacchi APT

13. servizio di monitoraggio infrastruttura
14. servizio di IPS/IDS
15. servizio di threat emulation
16. servizio Web Application Firewall

Nei paragrafi che seguono descriveremo nel dettaglio i servizi che possono essere erogati da ARIASPA.
Tutti i servizi di sicurezza sono previsti per la soluzione di gestione completa (Full Managed) da parte di ARIASPA tranne dove espressamente indicato.

7.1.1 Servizio di hardening dei sistemi

L'obiettivo di questo servizio è la messa in sicurezza di tutti i sistemi attivi e di tutti quelli che vengono messi in produzione al fine di garantire elevati livelli di servizio in termini di sicurezza ed usabilità.
L'attività di hardening è un'attività orizzontale, che coinvolge le basi di tutti i *sistemi*, dove per *sistema* in questo contesto si intende un'entità che sia a rischio di attacchi. Sono quindi classificabili come sistemi (a titolo esemplificativo e non esaustivo):

- i sistemi operativi,
- i web server,
- gli application server,
- i database,
- gli applicativi complessi (come Oracle),
- gli apparati virtuali di rete;
- gli apparati virtuali di sicurezza.

Questo servizio richiede che l'hardening sia preventivo e non solo correttivo; si assume che la procedura di hardening sia integrata in quella di installazione e configurazione iniziale di ogni sistema.
L'attività di hardening fa riferimento a requisiti di configurazione e funzionalità, e si concretizza nel:

- definire gli indicatori (processi attivi, applicazioni installate, utenti gestiti, password policy, etc.) da usare per la definizione del livello di sicurezza del sistema;
- effettuare statistiche per valutare l'andamento nel tempo di tali indicatori;
- reperire, creare o personalizzare gli opportuni strumenti atti a monitorare la configurazione di ogni sistema;
- individuare e segnalare eventuali criticità nella configurazione dei sistemi maggiormente critici;
- intraprendere, a fronte di criticità di sicurezza emerse dalla fase di monitoraggio ed analisi, gli
- opportuni interventi correttivi che riportino il sistema al livello di sicurezza desiderato;
- stilare report che descrivano l'andamento nel tempo delle "misconfigurations" riscontrate, eventuali interventi correttivi effettuati e riassunto sul livello complessivo dello stato di sicurezza del sistema sia a livello di singolo servizio che di tipologia.

Riguardo alle attività di security tuning ARIASPA si avvale di strumenti di gestione ed analisi di sicurezza.

Saranno prese in carico da ARIASPA eventuali richieste attinenti tale servizio, inoltrate da un referente concordato dall'Ente.

A partire dal 6° mese successivo all'attivazione del contratto, ARIASPA con cadenza trimestrale renderà disponibile all'Ente report strutturati che descrivono lo stato di sicurezza dei sistemi.

Inoltre, per ogni sistema, oggetto della procedura di hardening, sarà predisposta e compilata la relativa check list, da rendere disponibile all'Ente in qualsiasi momento ne faccia richiesta.

Il servizio di hardening viene erogato nell'orario standard di lavoro solo nel caso possa essere svolto senza impattare l'erogazione dei servizi.

7.1.2 Servizio di gestione utenze di Amministrazione di Sistema

Le credenziali amministrative hanno da sempre una grande importanza negli ambienti della Pubblica Amministrazione. Sarà predisposto un sistema di cambio periodico (o a richiesta) delle credenziali amministrative tramite prodotti leader di mercato al fine di evitare la distribuzione incontrollata (o per errore) di tali credenziali seguendo le direttive indicate in precedenza o attuando misura restrittive a discrezione di quanto concordato dall'Ente con ARIASPA.

Il servizio "Gestione utenze di amministrazione di Sistema" comprende tutte le attività che ARIASPA è tenuta a svolgere in relazione alla gestione delle identità degli amministratori di sistema.
Il servizio consiste nel gestire tutte le utenze (nominali, applicative o di sistema) creare, modificare e cancellare utenze, garantire l'accesso ai gruppi richiesti, eliminare le utenze orfane e (ove possibile) quelle non nominali (hardening).
Il dominio di competenza della gestione delle utenze di amministrazione di Sistema comprende tutte le utenze d'accesso (ove tecnicamente possibile) ai sistemi operativi dei sistemi, database, application server, sistemi complessi, ecc. presenti sulle infrastrutture affidate in gestione ad ARIASPA.
Il servizio include le seguenti attività:

- individuare tutti i server del parco macchine dell'Ente (di seguito denominati *target*);
- mantenere il controllo dei *target*;
- tenere sotto controllo e, asintoticamente, eliminare le utenze orfane su ogni sistema;
- gestire il processo del ciclo di vita di ogni utenza;
- organizzare adeguatamente le utenze in gruppi;
- tracciare mediante Service Desk tutte le richieste di attività e le comunicazioni di avvenuta attività;
- tracciare ogni attività di intervento sugli utenti mediante il sistema di trouble ticketing;
- attivare i supporti tecnici di assistenza per il ripristino del funzionamento della piattaforma;

- documentare gli eventuali incident nel trouble ticket e, ove richiesto dall'Ente, mediante specifici report.

Per l'espletamento di questo servizio l'Ente dovrà innanzitutto identificare un Referente per il servizio un'interfaccia col compito e l'autorità di regolamentare, richiedere, modificare e cancellare le utenze legate sui target.

Il servizio viene erogato nell'orario standard di lavoro nel caso di profilazione di utenze nominali o di creazione di reportistica.

7.1.3 Servizio di gestione configurazioni sugli apparati di sicurezza

Il Servizio di ARIASPA è basato su una architettura di rete modulare in modo da poter erogare servizi in modalità di Business Continuity e Disaster Recovery. In questo contesto anche l'infrastruttura di sicurezza di rete deve mantenere un approccio modulare e distribuito.

L'architettura di sicurezza è composta da un modulo principale (modulo di management dei sistemi di sicurezza) e dai moduli funzionali che sono quelli che erogano attivamente il servizio.

Ognuno di questi moduli è stato realizzato utilizzando apparati configurati in alta affidabilità in modo da garantire la massima sicurezza, in termini di disponibilità, dei servizi erogati. Dovranno essere garantiti i principali benefici forniti dall' architettura modulare attualmente in essere (ad essere totale indipendenza di un modulo rispetto agli altri, distribuzione della capacità di calcolo delle macchine utilizzate come componenti dell'infrastruttura).

L'implementazione delle regole di sicurezza comprende tutte le attività per la gestione del ciclo di vita delle policy applicate agli apparati di sicurezza (firewall e security groups).

Tenuto conto che le regole di sicurezza sono il nodo centrale di una robusta infrastruttura, ARIASPA assicura la qualità della gestione del servizio e un attento controllo di ogni cambiamento.

Il servizio prevede che:

- la protezione sia realizzata mediante sistemi dedicati e ove possibile con infrastruttura basata su hardware dedicato;
- i sistemi implementati per tale servizio siano in *Alta Disponibilità*.

Saranno gestite tutte le fasi di implementazione delle regole di sicurezza. Nello specifico si identificano le seguenti fasi:

1) ricezione delle richieste di variazione;
2) registrazione delle richieste e classificazione;
3) analisi di impatto della richiesta;
4) valutazione del rischio nell'implementare la richiesta esaminata;
5) implementazione o rigetto motivato della richiesta.

Il servizio è prestato in orario standard di lavoro. Sarà facoltà della struttura dell'Ente (per il tramite del responsabile o suo delegato) richiedere ed autorizzare installazioni straordinarie di regole di sicurezza o modifiche di configurazioni, fuori dall'orario di lavoro, richiedendo l'intervento in regime di reperibilità.

Le regole di sicurezza, solo per l'infrastruttura di firewalling, saranno implementate e attivate due volte la settimana ed in giorni prestabiliti: tipicamente il lunedì ed il giovedì entro le ore 7.00 e dopo le ore 20 del giorno solare precedente.

Le richieste ritenute errate o incomplete da ARIASPA saranno chiuse segnalando in modo esaustivo al richiedente, entro 8 ore lavorative dall'invio della richiesta, l'anomalia riscontrata.

Saranno elaborate e prese in considerazione le richieste giunte (fa fede la data e l'ora di apertura del Ticket nel sistema di Trouble Ticketing) entro le ore 13.00 del giorno lavorativo precedente (per le regole installate al lunedì mattina varranno le richieste di cui è stato aperto il relativo ticket entro le ore 13.00 del venerdì precedente).

Per tutte le altre tipologie di richieste, ARIASPA provvederà all'evasione entro le 8 ore lavorative successive alla richiesta.

7.1.4 Servizio di antivirus e antimalware sui sistemi

La soluzione proposta basata su prodotti leader di mercato garantisce la compatibilità con sistemi Ms Windows, Red Hat Enterprise 4.x e successivi, SuSE Linux Enterprise

Server/Desktop 10.x and 11.x, Ubuntu 10.04 e successivi, CentOS 5.x e successivi, AIX. ed in generale a tutti gli ambienti in perimetro di gestione se facenti parte della "reference architecture" di ARIASPA. La soluzione consta di funzionalità di controllo di accesso basato su ruoli, di audit interno delle modifiche, monitoraggio del funzionamento degli agenti con possibilità di inviare alert in caso di mal funzionamento.

È garantito un servizio di distribuzione delle signature centralizzato e la possibilità di garantire la protezione da malware in modalità con o senza agent per i sistemi virtuali. L'aggiornamento delle signature è disponibile almeno su base giornaliera; è prevista la schedulazione delle scansioni e l'identificazione dei sistemi non protetti all'interno dello scope definito così come la non corretta protezione dei sistemi generando eventi di alerting permettendo la quarantena o l'eliminazione dei file infetti.

La gestione avviene tramite una console centralizzata in grado di garantire tutte le funzionalità presenti, fornendo un sistema di reportistica avanzato e prevede la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate. Per garantire una totale copertura da questa tipologia di attacchi ripulendo il traffico malevolo ed isolando il traffico lecito diretto verso le applicazioni, salvaguardando, pertanto, l'erogazione dei servizi esposti.

Su ogni istanza virtuale sarà installato e gestito un sistema Antivirus e Antimalware. L'installazione avverrà contestualmente alla preparazione del server. Tale installazione sarà ripetuta su una macchina su cui era già presente nei casi di guasti di varia natura o di oggettive problematiche software che hanno pregiudicato la funzionalità del servizio.

La frequenza (determinata in minuti) di aggiornamento delle firme identificanti codici malevoli e blacklist dei siti contenenti codici malevoli o sorgenti di spam sarà impostata su quella massima consentita dal sistema senza degradare la capacità di banda della rete.

Come già detto, tutto il servizio sarà gestito attraverso una console che permetterà una visualizzazione centralizzata dello stato di salute delle macchine su cui è presente il programma Antivirus/Antimalware e lo stato di aggiornamento di quest'ultimo con

la possibilità di fornire a richiesta entro 3 giorni lavorativi reportistica di dettaglio o complessiva (ad esempio per tipologia di server, per i servizi, ...).

Le operazioni di gestione (quali l'aggiornamento su tutta la base di installazione o l'applicazione di politiche di Sicurezza realizzate ad-hoc da ARIASPA in risposta alle caratteristiche di un codice malevolo o di una particolare esigenza ~~aziendale~~ dell'ente) saranno automatizzate in base alle possibilità del programma Antivirus e attraverso la console centralizzata del servizio.

Viceversa, la disinstallazione del programma Antivirus/Antimalware sui server sarà eseguita solo a fronte della dismissione degli stessi o su esplicita richiesta documentata dell'Ente.

L'orario del servizio per le attività di ordinaria manutenzione corrisponde all'orario standard di lavoro. È comunque prevista la copertura h24x7 mediante reperibilità per la gestione di anomalie e di ambienti di produzione.

Eventuali richieste di non installazione preventiva del software dovranno essere notificate dall'Ente prima della creazione dei server. L'Ente conseguenza si assumerà la responsabilità degli eventi causatati dall'assenza dell'installazione di tale software.

7.1.5 Servizio di Patching

Il servizio sarà erogato su istanze di server virtuali e componenti applicative.

Il servizio di Patching consiste nell'installazione di aggiornamenti (Service Patch, Hot Fix, etc.) che i produttori di software rendono disponibili a correzione di potenziali vulnerabilità di sicurezza individuate dopo il rilascio dei programmi (sistemi operativi, middleware, componenti software di infrastruttura, ...).

L'installazione di una patch deve avere come obiettivo la correzione di vulnerabilità presenti su un programma.

Ogni qualvolta si determina l'esigenza della installazione di una patch l'intervento e le relative modalità di esecuzione dovrà essere concordate con l'Ente e in ogni caso saranno svolte evitando il degrado delle prestazioni del servizio.

Su ciascun server o istanza virtuale o componente applicativa installata sarà valutata:

- l'opportunità o la necessità di installare le patch (patch, hotfix, etc) segnalate dai relativi Vendor;

- la scelta sulle patch da installare sarà attentamente valutata con l'Ente in modo da evitare eventuali problemi di compatibilità con altri programmi installati sullo stesso server o su altri server con cui deve sussistere un flusso di dati informatici;
- la scelta di non applicare una determinata patch (o un insieme di patch) sarà condivisa per approvazione con l'Ente, esplicitando le motivazioni della non installazione e indicando gli eventuali rischi informatici derivanti da tale scelta;
- l'esecuzione di esaustivi test di compatibilità per accertare sia la compatibilità che le eventuali modifiche (relative alle impostazioni di rete e sicurezza) da apportare alle preesistenti configurazioni nel caso in cui il Vendor non rilasci sufficienti informazioni o garanzie di compatibilità con altri programmi installate sullo stesso server;
- la definizione del livello di patching deve essere mantenuta adeguata attraverso il continuo aggiornamento;
- deve essere disponibile fuori linea la gold copy del software standard da installare sulle diverse tipologie di server e componenti applicative opportunamente aggiornato;
- la manutenzione del patching dei programmi sarà gestita, ove possibile, in maniera automatizzata mediante l'uso di un software che permetta di monitorare lo stato dei sistemi (ad esempio attraverso l'utilizzo di un servizio di *Early-Warning*) e il loro allineamento all'ultimo livello di patch;
- la manutenzione dei sistemi sarà effettuata evitando il degrado delle prestazioni di banda delle reti e dei servizi impattati;
- la gestione del servizio consentirà la possibilità di scegliere/impostare un determinato livello di patching per un gruppo di ambienti (server, database, application server, ...).

ARIASPA fornirà lo stato di patching delle istanze virtuali e componenti applicative attestati sull'infrastruttura in gestione con cadenza trimestrale dall'attivazione del contratto.

7.1.6 Servizio di security monitoring

Il servizio di Security Monitoring include la gestione di tutte gli apparati/sistemi/servizi di sicurezza presenti.

Di seguito sono descritte le principali funzioni attualmente svolte per il servizio di Security Monitoring :

- visione sempre aggiornata dello stato di sicurezza di apparati/sistemi/servizi gestiti e relativo aggiornamento;
- visione sempre aggiornata delle minacce informatiche;
- installazione, configurazione, monitoraggio e gestione delle infrastrutture di sicurezza;
- installazione, configurazione, monitoraggio e gestione dei software di sicurezza;
- supporto per la gestione degli incidenti informatici.

Il servizio, al fine di rilevare tentativi di attacchi informatici per contrastarli in modo efficace, deve monitorare le comunicazioni informatiche provenienti da Internet, da tutte le connessioni geografiche e dalla rete interna, verso apparati/sistemi/servizi e le comunicazioni interne all'intera infrastruttura gestita dal Fornitore; deve inoltre prevedere la raccolta e la correlazione dei dati di log degli apparati/sistemi/servizi di sicurezza e di rete.

Il servizio si articola nei seguenti ambiti:

a. Log Analysis e Correlation;
b. Vulnerability Assessment e Penetration Test
c. Security incident management.

a. Servizio di Log Analysis e Log Correlation

Per Log Analysis e Log Correlation s'intende il servizio di analisi dei log creati da software/apparati di sicurezza e network (ad esempio i firewall) o di altri sistemi/applicativi/componente applicative (ad esempio application server, DB, etc).

Lo scopo dell'analisi è quella di individuare anomalie (come i tentativi di attacco) o comportamenti compatibili con le mansioni a seguito di errate configurazioni sugli ambiti indicati tenendo ovviamente in considerazione l'allineamento della componente temporale (NTP Server).

Per la Log Analysis e Log Correlation è tipicamente previsto che:

- l'esame delle configurazioni rilevi eventuali misconfiguration sfruttabili da minacce informatiche;
- l'esame, a parità di sistema/servizio rilevi ed evidenzi modifiche avvenute rispetto alla precedente configurazione;
- per ciascun sistema/servizio il report dell'analisi riporti anche dei dati statistici sia in termini di utilizzo medio delle componenti CPU/memoria/disco e sia i dati relativi all'accesso ai sistemi (da locale e da remoto) o i tentativi di accesso;
- sia possibile determinare l'invio dei dati sia su base temporale e sia ogni qualvolta si ritenga necessario fornendo una correlazione di eventi;
- la possibilità di ricercare per sistemi e/o comandi eseguiti al fine di poter svolgere attività di analisi forense;
- siano redatti report che diano evidenza dei dati analizzati;
- in caso siano rilevate anomalie, il report deve dettagliare la problematica e assegnare un livello di severità;
- nel report prodotto dall'analisi, per ogni problema rilevato, sia suggerita una soluzione/rimedio.

b. Servizio di Vulnerability Assessment / Penetration Test

Lo stato di sicurezza dei sistemi/apparati/servizi applicativi deve essere verificato attraverso continue valutazioni di sicurezza (Vulnerability Assessment – VA e Penetration Test – PT).

Il servizio di VA dovrà garantire di:

- realizzare verifiche sia su una base temporale prestabilita (una volta ogni sei mesi complessivo su tutti i sistemi/apparati/componenti applicative) o a richiesta dall'Ente;
- realizzare verifiche sia complessive su tutti i sistemi/apparati/componenti applicative (ad esempio application server), sia su una parte dell'infrastruttura;
- aggiornare continuamente la knowledge·base delle vulnerabilità da accertare permettendo sempre il rilevamento delle ultime minacce;
- gestire centralmente le scansioni;

- non degradare le prestazioni delle reti o provocare instabilità (sia a livello di sistema e sia a livello di rete);
- classificare le vulnerabilità rilevate in base sia alla severità della minaccia, sia al contesto di riferimento del sistema/servizio verificato;
- generare un report dettagliato dei risultati (personalizzabile su richiesta) a completamento di ciascuna verifica entro 5 giorni lavorativi;
- dettagliare nell'apposito report le remediation da attuare;
- per ciascuna vulnerabilità accertata il report suggerisca una soluzione/rimedio da applicare.

Lo scopo della funzione di PT è di verificare se le vulnerabilità, accertate o potenziali, individuate col Vulnerability Assessment possano realmente essere sfruttate per un attacco informatico contro gli elementi componenti la server farm e le web application/service e proporre ad LI eventuali azioni correttive.

L'accertamento sarà svolto utilizzando tecniche avanzate di Ethical Hacking, utilizzando tecniche automatizzate e/o manuali per lo sfruttamento delle minacce.

Il servizio di PT dovrà garantire di:

- essere svolto secondo una precisa metodologia di riferimento (preferibilmente utilizzando la metodologia OSSTMM o la CEH per i test infrastrutturali e la metodologia OWASP per i test sulle Web Application/Service) in modo che i risultati siano verificabili e riproducibili;
- non apportare modifiche ai dati contenuti nei sistemi oggetto dei test, ma solo visualizzazioni allo scopo di dimostrare l'esistenza di vulnerabilità;
- evitare il blocco delle user-id dei sistemi/servizi gestiti;
- evitare accuratamente tutte le procedure che possano arrecare disservizi o saturazione alle reti della server farm;
- essere svolto garantendo la continuità operativa dei sistemi, dei servizi e delle infrastrutture oggetto di test;
- non eseguire attacchi di tipo DoS (o DDoS);
- custodire le informazioni e i dati acquisiti durante lo svolgimento dei test esclusivamente per il tempo necessario alla redazione del report e comunque non oltre 40 giorni solari dalla loro acquisizione.

L'attività di VA/PT si completa con la redazione di un report in cui si documentano tutte le informazioni acquisite attraverso la discovery, l'identification e la loro dettagliata analisi.

Il VAPT dovrà con frequenza semestrale (anche fuori dall'orario lavorativo) coprire tutte le componenti infrastrutturali e applicative (sistemi/apparati/ componenti applicative) secondo una pianificazione che ARIASPA dovrà concordare con i referenti del l'Ente entro 6 mesi dall'avvio contrattuale.

Tale pianificazione potrà ovviamente essere soggetta a modifiche a seguito di richieste dell'Ente o valutazioni da parte di ARIASPA per modifiche infrastrutturali (ovviamente accettate e concordate con l'Ente).

Nella fase di presa in carico, ARIASPA concorderà con l'Ente le specifiche tecniche del Servizio e produrrà il documento relativo alle *Regole di Ingaggio* (*Rules of Engagement, o RoE*) che saranno lo standard per le attività di esecuzione delle attività. Nelle RoE saranno definite ad esempio le seguenti informazioni:

- le reti e/o gli indirizzi IP in cui sono attestati i sistemi/servizi e apparati della server farm;
- le reti e/o indirizzi IP che dovranno essere esclusi dai test;
- le URL delle web application/service da testare;
- quali sistemi/servizi devono essere testati in modalità black-box (senza alcuna informazione fornita dall'Ente) o gray-box (con parziali informazioni fornite dall'Ente);
- le fasce temporali in cui testare determinati sistemi/servizi/applicazioni.

Gli esiti saranno accuratamente documentati e consegnati all'Ente per indirizzare le eventuali azioni correttive.

I risultati dei test dovranno essere presentati all'Ente entro 5 giorni dal completamento dell'attività con la redazione di un report sintetico ed uno analitico.

- **Report Sintetico** (da denominare "Executive Report") deve riassume la situazione analizzata e le vulnerabilità riscontrate; per ogni sistema/servizio è sintetizzata la situazione complessiva e il numero delle vulnerabilità riscontrate e classificate per livello di rischio; la descrizione dei possibili miglioramenti che potrebbero essere applicati all'infrastruttura oggetto dei test, insieme all'elenco delle soluzioni

tecnologiche da adottare per incrementare il livello di security (Proposta di Adeguamento). Il reporting delle vulnerabilità sfruttate dovrà essere contestualizzato rispetto alla localizzazione del sistema/servizio nella server farm, alle misure di sicurezza di rete implementata e gli skill necessari per realizzare l'attacco.

- **Report Analitico** (da denominare "Technical Report") deve riportare integralmente tutte le informazioni validate ottenute dalla scansione.

L'Ente potrà:

- effettuare direttamente, o per il tramite di Fornitori terzi, attività di VAPT informando preventivamente ARIASPA che dovrà fornire tutto il necessario supporto;
- richiedere ad ARIASPA un numero massimo di 20 VAPT annui sulle piattaforme applicative che ARIASPA dovrà eseguire con le stesse tempistiche dei VAPT standard.

c. Servizio di Security Incident Management

Il servizio consiste nelle seguenti attività:

- monitorare tutte le infrastrutture gestite, su tutti gli incident di sicurezza. Nello specifico è richiesto ad ARIASPA di valutare la portata di un eventuale incidente di sicurezza in termini di impatto rispetto ai dati personali e all'erogazione dei servizi.
- fornire una reportistica dettagliata di tutti eventi con report aggregati e di dettaglio
- fornire una reportistica dettagliata sul servizi/o impattati/o dall'incident di sicurezza
- implementazione delle remediation indicate dall'Ente

7.1.7 Servizio di monitoraggio applicativo

Il servizio di monitoraggio dovrà integrare il servizio di security monitoring oltre a permettere la gestione in tempo reale dell'ubicazione geografica dei sistemi, delle componenti applicative, dei dati e dell'infrastruttura, indipendentemente dalla

tipologia degli stessi (sicurezza, network, sistemi, database, ...). Dovranno essere predisposte almeno le seguenti tipologie di dashboard:

- per servizio applicativo;
- per tipologia infrastrutturale;
- per tipologia di componente;
- per tipologia di dati trattati;

Inoltre, devono essere realizzate opportune allarmistiche configurabile per ogni componente di sicurezza e sistemi di reportistica online e schedulabili per le diverse tipologie di dashboard

Anche in questo caso si dovrà sottostare al principio del minor privilegio.

7.1.8 Servizio di Identity Access Management

Il servizio di identity management realizzato tramite soluzioni leader di mercato consentirà ad ogni cambio di privilegi sulle utenze che accedono ai diversi ambienti, di essere registrato in tempo reale sui sistemi di logging.

In particolare, le attività degli amministratori di sistema saranno registrate per un tempo minimo di 6 mesi online ed ulteriori 6 mesi fuori linea.

7.1.9 Servizio di logging

Dovranno essere registrate tutte le informazioni atte a garantire la normativa attualmente in vigore e successive modifiche e il rispetto delle linee guida AGID. Il logging dovrà essere attivato per tutti gli strumenti, apparati e sistemi in ambito e dovrà essere garantito in tempo reale verificando eventuali problemi e collegando automaticamente nuovi apparati. È in carico di ARIASPA l'attività di capacity di tale soluzione nonché l'adeguamento delle risorse a fronte di aumenti dei volumi relativi agli eventi registrati.

7.1.10 Servizio di protezione delle Basi Dati

La soluzione di protezione dei database consiste in una soluzione realizzata tramite soluzioni leader di mercato, attivabile/installabile su ogni singola istanza DB, in modo

da non pregiudicare le performance ne richiedere upgrade hardware per il corretto funzionamento.

Il monitoraggio (o eventuale blocco) viene effettuato in tempo reale anche per alti carichi transazionali monitorando tutte le transazioni, comprese le operazioni della rete, i quantitativi (query result) delle operazioni svolte e anche le transazioni intra-database.

A richiesta dell'Ente potranno essere previste analisi sulle attività svolte tramite meccanismi di machine learning (ad es. per consentire la verifica di utenze compromesse). È prevista una gestione centralizzata, che possa gestire fino a mille istanze database da una singola postazione. La soluzione è totalmente scalabile e non richiede risorse hardware per la gestione di ulteriori database.

Nella soluzione è prevista la possibilità di verificare il DB per le vulnerabilità, individuare i dati sensibili, tipologia di campi specifici e rilevare i difetti di configurazione, il tutto gestibile dalla stessa Dashboard di gestione cantralizzata usata per il monitoraggio.

Le tipologie di database sono Oracle, mySql, Postgres, MongoDb, Ms Sql Server. Qualora l'Ente ritenesse necessaria l'introduzione di nuove tipologie di db dovranno essere verificate da ARIASPA le compatibilità ed eventualmente implementare soluzioni alternative se i DB non fossero supportati.

7.1.11 Servizio di Anti-DDOS

La soluzione è in grado di rispondere ad attacchi mirati alla saturazione dei canali di connettività e/o di risorse dei sistemi/servizi esposti.

Qualora l'esposizione di Servizi avvenisse tramite il piano di indirizzamento di ARIASPA, la soluzione potrà essere realizzata anche per la proposta IaaS.

Le soluzioni tecnologiche permettono la risoluzione di varie tipologie di attacchi DDoS quali ad esempio:

a. Syn-flood

Il termine Syn Flooding, letteralmente tradotto con "inondazione di pacchetti di tipo Syn", nasce dal fatto che tutte le volte che un utente fa click su di un link di una pagina web richiede l'apertura di una connessione (di tipo TCP) verso quel sito; questo avviene

seguendo una serie di passi, il primo dei quali consiste nell'invio di un pacchetto TCP che richiede l'apertura di una connessione. Tutte le regole di funzionamento del protocollo TCP esigono che il sistema risponda allocando alcune risorse (in pratica memoria) per la connessione. Programmando opportunamente un semplice PC, è possibile richiedere l'apertura di diverse migliaia di connessioni al secondo, che "inondando" il server e ne consumano rapidamente tutta la memoria, bloccandolo o mandandolo in crash.

Il punto debole di questo tipo di attacco è che il computer attaccante deve essere in grado di mandare il flusso di pacchetti attraverso la connessione ad Internet fino al server attaccato.

Diversamente, l'utente malintenzionato deve poter fornire delle "credenziali" di accesso valide per usufruire della vulnerabilità insorta nel sistema operativo e portare a termine, efficacemente, l'attacco al sito bersaglio.

I pacchetti dannosi predisposti con un indirizzo IP falsificato (cioè modificato rispetto a quello originale), procureranno al computer "vulnerabile" una situazione temporanea di Denial of Service; tuttavia, poiché le connessioni che sono normalmente disponibili sono lente per tutti (per soggetti ben intenzionati così come per soggetti malintenzionati), questo tipo di attacco diventa impraticabile, nel senso che non dà il risultato atteso (cioè appunto la congestione del server).

b. DNS Amplification

Il DNS Amplification Attack o DNS Reflector attack è un classico attacco di tipo Distributed Denial of Service (DDoS) che abusa di server DNS open resolver e ricorsivi (recursive) inviando a questi ultimi pacchetti contenenti informazioni falsificate sull'IP di provenienza (IP spoofing). Lo studio di questo attacco ha portato la consapevolezza che per la sua completa riuscita è necessario soddisfare due fondamentali precondizioni:

- Un nome di dominio valido con record di risorsa di tipo SOA e TXT che supporti EDNS
- Una query personalizzata al cui interno sia contenuto l'indirizzo Ip della vittima a cui sarà successivamente destinata la risposta. Questa tecnica prende il nome di IP spoofing.

Il primo punto sta alla base del meccanismo di amplificazione, il secondo si riferisce invece alla rifrazione dell'attacco. Il concetto di amplificazione ha base sul fatto che query (richieste) molto piccole possono generare risposte molto più grandi, ad esempio una query UDP di 60 byte può generare una risposta di 512, cioè 8.5 volte più grande della richiesta. Chi sferra quest'attacco solitamente si avvale di una rete di computer dislocati sulla rete internet (ad esempio una Botnet) utilizzata inconsapevolmente allo scopo d'inviare una moltitudine di richieste a diversi server DNS open resolver. Questo primo aspetto dell'amplificazione viene successivamente potenziato per mezzo di diverse query, precostruite manualmente, atte ad interrogare i diversi record di risorsa dei domini sfruttati.

c. ICMP Flood

Il ping flood è un semplice attacco di tipo denial of service dove l'utente malevolo sommerge il sistema oggetto dell'attacco per mezzo di pacchetti ICMP Echo Request (ping). Ha successo soltanto se l'utente che compie l'attacco dispone di molta più banda rispetto al sistema attaccato (per esempio un attacco eseguito con una linea ADSL verso un sistema collegato con un modem dial-up). Colui che compie l'attacco spera che il sistema risponda con pacchetti ICMP Echo Reply, consumando quindi banda in uscita, oltre a quella già utilizzata per i pacchetti in arrivo

7.1.12 Servizio di detection e blocking di attacchi APT

A seguito del costante aumento degli attacchi ad infrastrutture tecnologiche, veicolati da server, PC e componenti IoT compromesse pilotati dall'esterno, che portano a termine attacchi mirati al furto di informazioni, è prevista la disponibilità di una soluzione basata su tecnologia dedicata leader di mercato in grado di identificare e (opportunamente configurata se richiesto dall'Ente) bloccare questi tipi di attacchi ed eventualmente i sistemi compromessi.

Questo tipo di soluzione sarà implementata nelle reti del vDC in Cloud utilizzato dall'Ente per esporre i servizi tramite piano di indirizzamento di ARIASPA.

7.1.13 Servizio di monitoraggio infrastruttura

Gli accessi amministrativi all'infrastruttura potranno avvenire solo tramite soluzioni che ne garantiscano

- l'enforcement degli accessi (autenticazione a due fattori e controllo di quali azioni possono o non possono essere eseguite da utenti privilegiati nell'ambiente anche in caso di amministratori),
- il monitoraggio (tracciamento e logging di tutte le attività degli utenti privilegiati e delle azioni svolte),
- la compliance delle impostazioni di sicurezza definite (ad esempio complessità delle password),
- il reporting (evidenza di quanto è stato svolto o è stato tentato di svolgere**)**

7.1.14 Servizio di IPS/IDS

Il servizio è dedicato alle analisi del traffico di rete in grado di rilevare e bloccare attacchi informatici a livello rete e applicativo. Le analisi del traffico avverranno mediante l'utilizzo di firme predefinite, analizzando i flussi di traffico e confrontandoli con campioni noti, che il produttore della soluzione rilascia periodicamente.
Il sistema mette a disposizione dell'analista dell'Ente (o a richiesta di ARIASPA) i risultati delle analisi in forma grafica fornendo la possibilità di, creare report di dettaglio relativi agli eventi rilevati, consentendo di catturare e riutilizzare i campioni di traffico per ulteriori analisi di approfondimento. Ovviamente sarà possibile la configurazione del sistema per analisi puntuali di quanto è in fase di analisi.

7.1.15 Servizio di threat emulation

Il servizio è dedicato alle analisi del traffico di rete al fine di rilevare e bloccare malware principalmente veicolati all' interno di connessioni HTTP, FTP, SMTP, CIFS, SMB, IRC etc... Le analisi del traffico avvengono senza l'utilizzo di firme predefinite, ma analizzando i flussi di traffico e replicandoli automaticamente in ambiente protetto, senza la necessità di comunicare con l'esterno, in modo da poter rilevare anche i tipi di attacco ancora non noti. Le analisi del traffico vengono eseguite su una piattaforma di virtualizzazione (che il malware non deve identificare come tale) e deve utilizzata consentendo l'analisi del codice con sistemi operativi diversi (in particolare diverse

versioni di Windows, con diversi livelli di aggiornamento, e diverso equipaggiamento software) in modo da rilevare malware che hanno come obiettivo sistemi con particolari dotazioni software. Il malware oggetto di rilevamento può essere di diverso tipo (ad esempio Zero Day Browser Exploit, Zero Day Application Exploit, Rootkits) e il sistema consente la produzione di report di dettaglio e aggregati per consentire le analisi necessarie al traffico prodotto dal malwalre. Inoltre, è possibile la configurazione di whitelist e/o blacklist per le attività sia di configurazione che di analisi.

7.1.16 Servizio Web Application Firewall

Il servizio analizza ogni accesso utente alle applicazioni web critiche e proteggere le applicazioni e i dati da attacchi informatici.
La soluzione prevede tra l'altro modalità di auto-apprendimento dal comportamento "normale" delle applicazioni (riduzione falsi positivi) e la contemporanea correlazione con le minacce provenienti da tutto il mondo e aggiornato in tempo reale. Inoltre, prevede le funzionalità di reputation services (filtraggio del traffico basato sulla più recente reputazione in tempo reale), protezione da bot (rileva i client botnet e gli attacchi DDoS applicativi) meccanismi di fraud prevention (presenza di soluzioni di prevenzione delle frodi), protezione "virtual patching" per le web applications per proteggere i servizi esposti e ridurre i tempi delle emergenze.
Allo stesso tempo sono previsti report automatici e manuali forniti a seguito di condivisione con l'Ente.

7.2 Software di sicurezza dell'Ente

Tutti i software installati, acquistati o realizzati dall'Ente e le relative personalizzazioni dovranno essere accettati da ARIASPA e dovranno garantire i requisiti di sicurezza e privacy richiesti da ARIASPA per tutti gli ambienti previsti.

7.3 Misure di sicurezza per la gestione dei servizi

Nell'ambito delle attività di documentazione e monitoraggio di tutti i cambiamenti apportati alle strutture di elaborazione delle informazioni e ai sistemi, il fornitore deve mettere in atto tutti gli accorgimenti necessari per:

- tracciare tutte le modifiche ai programmi, ai sistemi ed ai parametri di sicurezza e di configurazione, siano essi relativi ai sistemi che all'infrastruttura;
- assicurare che per tutte le modifiche, comprese quelle in emergenza, siano implementate e documentate idonee ed efficaci procedure di roll-back.

Non fa ambito della presente proposta di sicurezza la progettualità di un'attività di insourcing di sicurezza.

Eventuali richieste di configurazioni non a norma per gli aspetti di sicurezza da parte di sicurezza saranno formalizzate all'Ente tramite una reportistica condivisa.

In caso di accettazione da parte dell'Ente di tali configurazioni, l'Ente stesso sarà responsabile di quanto potrà accadere sul servizio in ambito o su quelli ad esso correlabili.

Inoltre, ARIASPA assicura:

- l'integrità e l'inalterabilità dei log relativi ai sistemi ed alle infrastrutture di supporto;
- che i log relativi ai sistemi ed alle infrastrutture di supporto siano inviati in tempo reale al sistema di logging;
- di non installare software senza autorizzazione da parte dell'Ente ed attuare procedure per rilevare e prevenire l'uso di software non autorizzato;
- di mantenere costantemente aggiornata la documentazione della configurazione corrente dei sistemi e degli apparati;
- di effettuare periodicamente test di verifica sulla sicurezza dei sistemi e dei dati ivi contenuti (VA/PT), comprendendo anche i sistemi di protezione perimetrale.

7.4 Sicurezza e protezione dei dati

ARIASPA si impegna a adottare ragionevoli misure idonee a proteggere il Contenuto dell'Ente da perdite, accessi o divulgazioni accidentali o illegittimi.

ARIASPA non potrà accedere ai Contenuti dell'Ente né utilizzarli, salvo ove necessario ai fini della manutenzione o prestazione dei Servizi Offerti, o allo scopo di rispettare una legge o un provvedimento vincolante di una pubblica autorità.

ARIASPA si impegna a non:

- divulgare i Contenuti dell'Ente a enti pubblici o terzi
- spostare i Contenuti dell'Ente, salvo, in ogni caso, ove fosse necessario per ottemperare a una norma di legge o a un provvedimento vincolante di una pubblica autorità.

ARIASPA si impegna a comunicare all'Ente l'eventuale sussistenza delle norme di legge sopra indicate o di eventuali provvedimenti vincolanti, fermo restando che tale comunicazione non violi una legge o un provvedimento vincolante di una pubblica autorità.

L'Ente acconsente a tale utilizzo per le Informazioni dell'Account esclusivamente nel rispetto dell'Informativa Privacy. L'Informativa Privacy non si applica ai Contenuti dell'Ente.

7.5 Requisiti relativi agli aspetti organizzativi

ARIASPA, per quanto di competenza, verrà nominata Responsabile del trattamento dei dati personali dai singoli Titolari del trattamento.

7.6 Misure derivanti dal provvedimento sugli Amministratori di sistema e s.m.i.

L'Autorità Garante per la protezione dei dati personali ha stabilito specifiche misure di sicurezza e di verifica relativamente alle attività svolte da parte degli Amministratori di Sistema sui sistemi da loro gestiti.

ARIASPA provvederà:

- identificare come Amministratori di Sistema le figure professionali finalizzate alla gestione ed alla manutenzione degli impianti di elaborazione e sue componenti

e altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati personali;

- attribuire le funzioni di Amministratore di Sistema previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;
- effettuare la designazione quale Amministratore di Sistema individualmente, allegando l'elenco degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- riportare in un apposito documento, da mantenere aggiornato e disponibile ai diversi Titolari in caso di loro richiesta e al Garante in caso di accertamenti, gli estremi identificativi delle persone fisiche Amministratori di Sistema, con l'elenco delle funzioni ad essi attribuite;
- adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) da parte degli Amministratori di Sistema e degli utenti che accedono direttamente ai sistemi.

In particolare, le registrazioni degli accessi devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate;

- conservare le registrazioni degli accessi per un congruo periodo, non inferiore a sei mesi;

7.7 Data breach

ARIASPA dovrà tempestivamente comunicare, ogni violazione dei dati o di incedenti informatici con un impatto significativo sui dati personali contenuti nelle banche dati, secondo le procedure previste da ARIASPA nel rispetto di quanto previsto dall'Autorità Garante per la Protezione dei dati personali.

8. Componenti del progetto di razionalizzazione e consolidamento del ced dell'Ente

Il progetto complessivo è costituito dalle componenti di seguito dettagliate.

8.1 Analisi e Realizzazione delle infrastrutture, erogazione delle attività di Moving

Prevede la realizzazione delle attività di razionalizzazione e consolidamento del CED dell'Ente Comunale utilizzando i servizi cloud offerti da ARIASPA.

Le attività è organizzata nelle seguenti fasi:

- progettazione e predisposizione della rete dati geografica (WAN) per l'interconnessione tra l'Ente e le piattaforme cloud;
- Assessment: in questa fase, ripetuta per ogni servizio da migrare, si analizzano dal punto di vista tecnico i server che erogano il servizio e le loro componenti (DB, AppSvr, Flussi, etc.);
- Progettazione: in questa fase, ripetuta per ogni servizio da migrare, si studia come ridisegnare il servizio seguendo le linee guida architetturali previste e si studia una possibile strategia di migrazione che si condivide con l'Ente;
- Realizzazione: in questa fase, ripetuta per ogni servizio da migrare, si predispongono, all'interno del DataCenter o Cloud di ARIASPA, le VM così come previsto dalla progettazione e si consegnano alle Software House per il rilascio della parte software e per i test pre-migrazione;
- Migrazione: in questa fase, ripetuta per ogni servizio da migrare, si concorda con l'Ente data, ora e durata del fermo per la migrazione del servizio; a seguito saranno effettuati tutti i test di collaudo per certificare l'avvenuta migrazione.

8.2 Erogazione continuativa dei servizi

Dalla conclusione delle attività previste nel paragrafo precedente, i servizi degli EE.LL rientrano nella gestione ordinaria dell'erogazione e di tutti i processi descritti in precedenza nel capitolo '*5 Processi Operativi*'.

8.3 Coordinamento del progetto

Tale componente, erogata parallelamente alle precedenti, copre l'intero ciclo di vita del progetto e consiste nel:

- controllare l'attuazione della strategia generale di consolidamento e razionalizzazione e gli avanzamenti generali durante le fasi realizzative e di esecuzione;
- verificare gli avanzamenti delle attività presso i singoli Enti;
- evidenziare punti di attenzione e criticità definendo azioni correttive;
- definire e ratificare azioni nei termini dell'accordo di collaborazione.

9. Cloud e modalità di gestione – Cloud Management Platform (CMP)

La gestione del VDC messo a disposizione avverrà tramite uno strumento di gestione denominato "CMP" (Cloud Management Platform): una soluzione web-based (costituita da pannelli e/o console) che racchiude al suo interno tutti i processi per la gestione dell'infrastruttura On e Off Premises, rendendo di fatto la gestione di tale infrastruttura trasparente per gli utenti.

La CMP permetterà la fruizione dei servizi infrastrutturali in completa autonomia in modalità multi-tenant, nel rispetto dei requisiti di sicurezza e di rispondenza normativa adottati in ARIASPA.

9.1 Funzionalità offerta IaaS

In caso di Servizio IaaS del VDC, la CMP rende disponibili una serie di funzionalità per l'attivazione, gestione, configurazione e monitoraggio del VDC. L'utente, attraverso un

catalogo unico, potrà effettuare il provisioning delle VM e aree storage in totale autonomia.

Inoltre, saranno messe a disposizione le seguenti funzionalità:

- possibilità di ridimensionare le risorse approvvigionate;
- possibilità di connettere/scollegare in autonomia le VM dalla rete pubblica (internet) e/o dalla rete interna;
- possibilità di attivare e disattivare la VM in autonomia;
- possibilità di effettuare operazioni schedulate (singole o ricorrenti), tra cui ad esempio l'accensione e lo spegnimento delle VM;
- richieste relative alla gestione e configurazione delle altre risorse base previste in fase di attivazione del VDC (es. Virtual Network, V-Firewall, V- Load Balancer) mediante funzionalità di self-ticketing.

9.2 Funzionalità offerta Full Managed

Nella modalità di Servizio Full Managed, la CMP mette a disposizione degli utenti degli enti una serie di funzionalità composta da cruscotti specializzati e personalizzabili al fine del governo del proprio VDC.

Le principali funzionalità previste sono:

- reportistica delle componenti del VDC, nello specifico VM e aree storage;
- dashboard che offrono visioni sintetiche e di dettaglio dello stato delle performance delle infrastrutture;
- Service Portal per la gestione dei processi ITSM (tra cui change, request, incident).

10. Reference architecture

Parte integrante dell'accordo di collaborazione è rappresentato dal documento "reference architecture", atto a definire le componenti architetturali di un nuovo sistema o per le evoluzioni tecnologiche di architetture esistenti, elaborato ed aggiornato da ARIASPA. La Reference Architecture elenca le tecnologie di riferimento

a cui gli applicativi utilizzati dall'Ente devono aderire, per poterne garantire la gestione Full Managed ed il rispetto dei livelli di servizio riportati nel capitolo "Livelli di servizio". Nella RA sono riportate le tecnologie riferite alle componenti architetturali approvate utilizzando i driver relativi alla standardizzazione delle infrastrutture, all'ottimizzazione dei processi di gestione e agli aspetti di sicurezza/normative. L'obiettivo è quello di definire delle "componenti di servizio" a cui sono associate le "caratteristiche del servizio" che definiscono gli OLA e gli SLA con cui il servizio deve essere erogato.

10.1 Modalità Gestione dei sistemi non in reference architecture

In presenza di applicativi dell'Ente con difformità rispetto alla reference architecture ARIASPA potrà offrire il servizio IaaS supportando l'Ente nella valutazione della fattibilità tecnica di migrazione dei sistemi nel VDC messo a disposizione.

11. Formazione

ARIASPA è tenuta ad erogare, senza costi aggiuntivi, formazione di tipo sistemistico ad almeno due professionisti ICT interni all'Ente rendendoli autonomi nell'ambito del dominio di competenza dei sistemi, quindi nella gestione del Tenant e nell'ambito delle funzionalità del CMP (Cloud Manager Platform). La formazione sarà fornita subito dopo la configurazione del Tenant e nei tempi necessari al raggiungimento dell'effettiva autonomia, e con modalità da concordare (da remoto o presso l'Ente).