CAPITOLATO TECNICO

ACQUISIZIONE SERVIZI IT RELATIVI ALL'HOSTING DEL PORTALE "REGISTRO REVISORI LEGALI"

INDICE

1.1. GLOSSARIO

Consip	La società che, in qualità di stazione appaltante della presente fornitura, affida la fornitura oggetto del presente Capitolato, e fruisce della fornitura oggetto del presente capitolato.
Fornitore	La società affidataria della presente procedura d'acquisto
Contratto	Il contratto che verrà stipulato tra Consip ed il Fornitore dove sono enunciate le regole giuridiche alle quali si dovrà conformare la fornitura.
Fornitura	Il complesso delle attività descritte nel presente capitolato tecnico.
Malfunzionamento	Qualsiasi anomalia funzionale del software e, in ogni caso, ogni difformità del prodotto in esecuzione rispetto alla relativa documentazione tecnica e manualistica d'uso.
Approvazione	Validazione dei prodotti intermedi di fornitura, previa verifica di merito.
Task	Una o più attività o interventi volta a soddisfare specifiche esigenze di Consip.

1.2. INTRODUZIONE

DESCRIZIONE DEL PORTALE

Il sistema implementa il Portale unico di accesso, con componenti pubbliche e private, per la pubblicazione e gestione del Registro dei Revisori Legali, compresi i Tirocinanti".

L'applicazione è integrata con:

- sistemi esterni, per il reperimento, l'immagazzinamento o lo scambio di dati relativi

ai Revisori e ai Tirocinanti;

- sistemi informativi del MEF, ed in particolare con il sistema di Protocollo e di Gestione documentale al fine di de-materializzare completamente il flusso di gestione della modulistica.

- Il nodo pubblico dei pagamenti "PagolaPA"

- Sistemi di PEC, firma digitale qualificata remota automatica e verifica firma

Il Portale, attraverso tutte le sue componenti software, è in grado di gestire le seguenti macro funzionalità:

- alimentazione del Registro attraverso il caricamento dati nella base informativa;

- aggiornamento in modifica da parte degli utenti (Revisori/Tirocinanti);

- modifica della base dati da parte dei funzionari dell'Amministrazione/Consip per quanto attiene ai diversi "stati" dei Revisori e dei Tirocinanti sulla base dell'applicazione della normativa vigente;

- modifica dei contenuti delle pagine web pubbliche e private, attraverso funzioni tipiche di content management;

- pubblicazione di documenti di interesse pubblico (normative, decreti, comunicati stampa, ecc.) o specifico (moduli per Revisori e Tirocinanti);

- funzionalità relative alla pubblicazione delle informazioni verso Internet, in modo tale che sia il Registro dei Revisori che quello dei Tirocinanti siano pubblici e consultabili.

- Creazione e gestione di tutte le pratiche amministrative inerenti l'albo

- Gestione degli incarichi

- Pagamenti on-line

- Bollo virtuale

-Gestione workflow approvativi per le singole pratiche

- Gestione massiva delle pratiche

-Cruscotti di monitoraggio e reportistica sullo stato delle pratiche

UTENTI

Si individuano le seguenti tipologie di utenti:

- il pubblico, per operazioni di consultazione dei dati pubblici del registro;

- i Revisori, per le attivazioni delle pratiche, la consultazione e l'aggiornamento dei propri dati;

- i Tirocinanti, per le attivazioni delle pratiche, la consultazione e l'aggiornamento dei propri dati;

- i "gestori" ovvero l'Ispettorato Generale Finanza della Ragioneria Generale dello Stato (MEF) o personale da questo delegato (Consip) che utilizzeranno le funzioni di backoffice del portale per aggiornare il contenuto informativo del Registro e la gestione delle pratiche.

ARCHITETTURA DELLA SOLUZIONE

L'architettura delle applicazioni è basata sul modello a tre livelli: presentation, business, dati.

Il livello presentation contiene le classi che producono il codice html da inviare al browser utilizzando template HTML-JavaScript da completare con i dati, il livello di business fornisce i dati elaborati alle classi di presentazione e il livello dati effettua gli accessi al DB.

L'installazione del software applicativo è effettuata unicamente sui server web; i client intranet o internet dovranno disporre unicamente di un browser.

L'applicazione è scalabile orizzontalmente (load balancing) e verticalmente.

Il RDBMS utilizzato è Oracle 11g in alta affidabilità (in modalità RAC).

Il portale si basa sulla piattaforma OPENCMS v. 8.0.3, per quanto attiene alla componente di Content Management, e su un'applicazione gestionale di backoffice in tecnologia J2EE.

SOFTWARE DI BASE

- Application Server: Tomcat

- DBMS: Oracle 11g

- S.O: Linux.

ARCHITETTURA DI SISTEMA

L'architettura di sistema è organizzata su tre livelli.

I servizi sono erogati da server di front-end inseriti in strati differenti: lo strato più esterno (Front End) contiene i server esposti sulla rete Internet; tra lo strato di front-end e la rete internet è interposto il primo strato dell'infrastruttura di sicurezza. Il secondo strato comprende i server applicativi, separato dal primo attraverso un ulteriore strato di sicurezza. Il terzo strato comprende tutti i server che erogano i servizi di back-end, protetto da un ulteriore strato di sicurezza che consentirà l'accesso ai soli server applicativi.

La figura seguente mostra l'architettura generale del sistema.

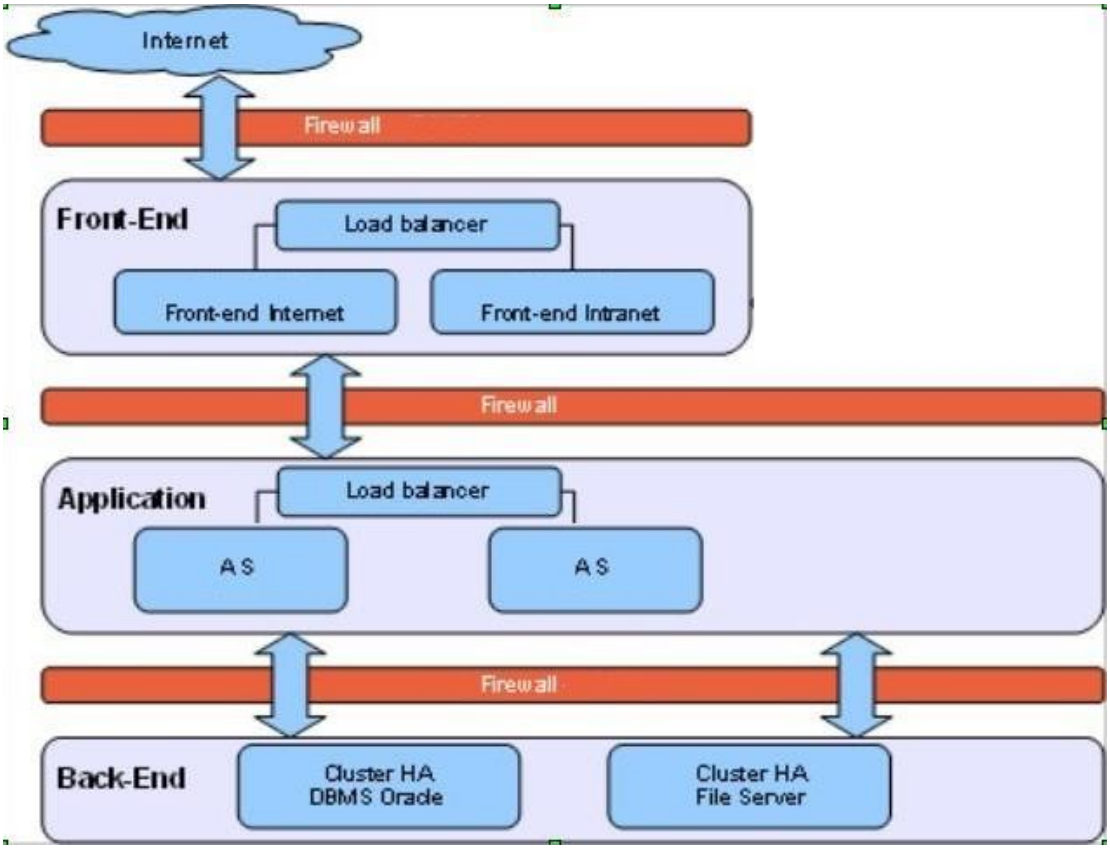

Figura 1: Architettura portale

ARCHITETTURA FISICA

L'architettura fisica è basata su piattaforma virtuale che utilizza il pool di risorse hardware disponibile per realizzare servizi applicativi in cluster:

Più dettagliatamente sono implementati:

- un primo livello di clustering in cui tutti i nodi fisici sono attivi e rendono disponibili le proprie risorse in un unico pool di risorse (CPU,RAM,etc.);
- un secondo livello di clustering in cui due o più server virtuali sono messi in configurazione HA.

Questo tipo di architettura garantisce una altissima affidabilità poiché:

- il pool di risorse è fisicamente dislocato su più macchine ciascuna delle quali con caratteristiche di elevata affidabilità (grazie alla doppia alimentazione, alla RAM con correzione di errore, alle CPU con RAM dedicata, al doppio BUS di comunicazione ed altro);
- i server virtuali che si trovano al livello superiore sfruttano risorse indipendenti dalla macchina fisica su cui realmente sono disponibili;
- i server virtuali sono messi in configurazioni HA di tipo attivo-attivo o attivo-passivo a seconda del tipo di servizio che devono erogare.

I server in load balancing che forniscono la connettività web verso internet sono costituiti da macchine fisiche per isolarle ulteriormente dall'ambiente applicativo virtuale.

Il cluster Oracle (Oracle RAC), per ragioni prestazionali, è costituito da una serie di nodi fisici opportunamente configurati.

1.3. OGGETTO E DURATA

Acquisizione servizi it relativi all'hosting del Portale unico di accesso, con componenti pubbliche e private, per la pubblicazione e gestione del Registro dei Revisori Legali per il periodo dal 1/1/2018 al 31/12/2018

1.4. EROGAZIONE DEL SERVIZIO DI HOSTING

COMPETENZE HELP DESK

Gli operatori del servizio di assistenza devono essere adeguatamente formati e con significativa esperienza nel settore. Lo skill garantito comprende:

- Conoscenza del processo di assistenza
- Conoscenza del profilo di fornitura (componenti HW/SW, SLA contrattuali, priorità, ecc)
- Conoscenze approfondita di strumenti informatici di produttività individuale e comunicazione

Il livello di formazione è in grado di garantire una risposta immediata in merito a richieste sulle informazioni principali e dubbi e difficoltà inerenti i servizi e le procedure.

Il processo di gestione risorse umane, al fine di garantire l'efficienza sul servizio mantiene un piano di miglioramento dello skill attraverso piani formativi periodici e incontri di allineamento su nuovi rilasci e/o aggiornamenti del servizio.

DIMENSIONAMENTO

Il dimensionamento dell'infrastruttura in hosting e della connettività sarà adeguato al carico di lavoro previsto:

Utenti: 250.000, con incremento successivo de10%;

Banda minima: 100 Mbps per il traffico internet e 100 Mbps per la connettività con il CED dell'Amministrazione.

STANDARD DI RIFERIMENTO E RELATIVE CERTIFICAZIONI

Per quanto attiene alle attività di gestione dei servizi, il Fornitore adotta lo standard ITIL v3, gestendo i seguenti processi:

- Demand Management; Pianificazione delle attività di erogazione del servizio e delle risorse da allocare (fase di Service Strategy);
- Service Level Management; Capacity Management, Availability Management, IT Service Continuity Management, Information Security Management, Supplier Management (fase di Service Design);

- Transition Planning and Support, Change Management, Service Asset and Configuration Management, Release and Deployment Management, Knowledge Management (fase di Service Transition);
- Event Management, Incident Management e codifica delle richieste pervenute al Service Desk, Escalation Management, Request Fulfillment Management, Access Management, Problem Management e definizioni delle priorità da assegnare alle richieste di assistenza da condividere con l'Amministrazione (fase di Service Operation);
- Gestione delle attività di aggiornamento della knowledge base di self assistance;
- Gestione delle FAQ e delle sezioni web dedicate all'autodiagnosi dei problemi;
- Gestione del flusso informativo derivanti da attività di assistenza e loro condivisione con tutti i possibili servizi "impattati".

DESCRIZIONE DEL DATA CENTER PER L'EROGAZIONE DEL SERVIZIO DI HOSTING

Il Fornitore eroga i propri servizi di hosting attraverso un Data Center all'interno del quale sono collocati i sistemi e gli apparati elettronici di proprietà dello stesso.

Il Data Center si trova presso la sede operativa del Fornitore. Il sito di Disaster Recovery è ubicato presso altra sede ed è connesso al Data Center del Fornitore tramite un doppio collegamento dedicato da 1 Gigabit Ethernet in fibra ottica.

MONITORAGGIO DEI SISTEMI

Il Data Center del Fornitore è gestito seguendo le best practice suggerite dall'ITIL (Information Technology Infrastructure Library). A livello organizzativo è presente una struttura di Service Desk la quale agisce come SPOC (Single Point Of Contact) per problemi relativi all'erogazione dei servizi. Le strumentazioni di controllo sono state implementate su progetti open source come il Nagios, tramite il quale si realizza il monitoraggio completo dei servizi di business offerti dal Fornitore.

Nello specifico, il Fornitore utilizza il prodotto Wuerth Phoenix Net-eye per il monitoraggio e controllo di sistemi e servizi e il prodotto S3 Virtual User per le navigazioni automatiche relative ai servizi stessi.

Il processo di Incident Management si avvale di una robusta infrastruttura di Event Management, nella quale i controlli Nagios sulle risorse vengono integrati e correlati con navigazioni web che testano il servizio in tutta la sua catena infrastrutturale. Gli eventi rilevati sono correlati alle mappe di servizio, registrate nel sistema di gestione della configurazione (CMDB – Configuration Management Database). Tramite queste fonti di informazione gli operatori del Service Desk sono in grado di operare con una soluzione di 1° livello, qualora l'evento sia già presente nel known error database, oppure di scalare la malfunzione verso il 2° livello inserendo tutte le informazioni necessarie ed attivando il corretto gruppo di supporto mediante un sistema di gestione del Workflow.

PROCEDURA DI INCIDENT MANAGEMENT

Il processo di Incident Management si avvale di una robusta infrastruttura di Event Management, nella quale i controlli Nagios sulle risorse vengono integrati e correlati con navigazioni web che testano il servizio in tutta la sua catena infrastrutturale. Gli eventi rilevati sono correlati alle mappe di servizio, registrate nel sistema di gestione della configurazione (CMDB – Configuration Management Database). Tramite queste fonti di informazione gli operatori del Service Desk sono in grado di operare con una soluzione di 1° livello, qualora l'evento sia già presente nel known error database, oppure di scalare la malfunzione verso il 2° livello inserendo tutte le informazioni necessarie ed attivando il corretto gruppo di supporto mediante un sistema di gestione del Workflow.

Le console operative del Data Center sono controllate dagli operatori durante l'orario di presidio. Sulle console operative vengono riportati, per ogni singolo server oggetto di controllo, tutte le informazioni raccolte dagli agenti e che richiedono l'attenzione degli operatori. Al di fuori di tali orari è previsto un servizio di reperibilità degli operatori del Service Desk che vengono avvisati in caso di anomalie dai sistemi di controllo automatici, tramite un sistema di notifica automatica SMS.

Il 2° livello di supporto sistemistico è composto da un team di Sistemisti di Base e Sistemisti di Rete.

Il gruppo degli specialisti di sistemi, che include esperti in sistemi operativi, middleware, data base e reti, è responsabile delle attività di installazione, configurazione e gestione di tutti sistemi, i middleware, i data base, i firewall e gli

apparati di rete utilizzati per l'erogazione dei servizi. Il personale inoltre è responsabile della gestione e risoluzione di eventuali problemi che dovessero verificarsi sulle componenti infrastrutturali, oltre che dell'aggiornamento ordinario dei software inclusa l'installazione di patch.

Il personale non si collega direttamente al singolo server, ma opera attraverso l'utilizzo di un sistema, sviluppato dalla funzione aziendale che sovraintende alla sicurezza informatica, che prevede la verifica delle credenziali di accesso personali anche attraverso l'utilizzo di certificati di autenticazione. Gestisce inoltre la profilazione e le autorizzazioni di ciascun utente e provvede a loggare le attività svolte sui vari sistemi da ogni singolo operatore.

L'assegnazione di un Ticket al supporto specialistico dell'area sistemistica è finalizzata ad usufruire di competenze/conoscenze/strumenti specialistici in grado di analizzare e risolvere la richiesta che si rileva particolarmente complessa e che richiede un intervento sistemistico sulle infrastrutture HW/SW dei sistemi di base e/o di rete.

Il processo di gestione degli incidenti, condotto secondo le raccomandazioni delle Best Practices ITIL, si focalizza sulle modalità di gestione e di ripristino tempestivo degli incidenti di carattere sistemistico. La funzione del Fornitore coinvolta in tale processo è il Service Desk che opera anche come interfaccia per gli altri processi, quali il Change Management, il Problem Management e il Configuration Management.

Il modello organizzativo prevede che il supporto specialistico sistemistico sia fornito dalla funzione di Service Desk (SD) che gestisce il ciclo di vita dell'incidente con lo strumento PSM e che si avvale della collaborazione di tutte le strutture aziendali coinvolte.

Il processo si declina nei seguenti passi procedurali:

FASE	Descrizione
Rilevazione e Registrazione	In questa fase l'operatore provvede a classificare l'incidente sulla base della tipologia di servizio tecnologico/prodotto a cui la segnalazione si riferisce. L'urgenza viene assegnata in base alla seguente scala qualitativa: Alta,Media,Bassa.

Diagnosi	In questa fase si provvede ad un'analisi preliminare dell'incidente e alla verifica dell'esistenza di errori noti (con relativa soluzione) associati a quel dato incidente e servizio tecnologico di riferimento. Nel caso in cui il SD non sia in grado di definire la soluzione da adottare per risolvere l'incidente, il ticket passa allo stato "Routed" e viene assegnato ad un gruppo di risoluzione.
Risoluzione e Ripristino	Nel caso in cui l'incidente sia risolvibile al 1° livello, il Service Desk InfoCert stabilisce la soluzione da adottare (workaround) e provvede, nel caso non sia necessario un gruppo di risoluzione, alla risoluzione dell'incidente (stato "running"). Nel caso in cui sia richiesto l'utilizzo di un gruppo di risoluzione si procede con lo stabilire le soluzioni da adottare e provvede alla risoluzione dell'incidente (stato "running") richiedendo, eventualmente anche il coinvolgimento di altre strutture. A seguito della risoluzione dell'incidente il ticket passa allo stato "Completed".
Chiusura	Scopo della fase di "Chiusura " è quello di confermare il buon esito della risoluzione dell'incidente. Il Service Desk provvede ad informare gli attivatori della segnalazione i quali verificano l'effettiva risoluzione dell'incidente e, in caso positivo, si procede con la chiusura dell'incidente.

Il Service Desk provvede ad informare gli attivatori della segnalazione i quali verificano l'effettiva risoluzione dell'incidente e, in caso positivo, si procede con la chiusura dell'incidente.

PROBLEM MANAGEMENT

La gestione del Problem Management è inserita nel processi "PR455-Incident Management"governata dalla istruzione tecnica specifica "PR455/IT–Problem Management Data Center".

L'attività di Problem Management mira a ridurre gli impatti negativi a seguito di incidenti che possono essere provocati da errori/malfunzioni nelle infrastrutture IT e a prevenire il verificarsi e il ripetersi di tali errori. A tale scopo il Problem Management cerca di individuare la causa degli incidenti e e ne attua le opportune azioni preventive, correttive e/o migliorative.

La gestione dei problemi può essere sia reattiva che proattiva. Reattiva quando vengono risolti problemi a seguito di uno o più incidenti. La gestione proattiva riguarda invece l'identificazione e la risoluzione di problemi prima che si verifichino degli incidenti.

Il processo si declina nei seguenti passi procedurali:

FASE	Descrizione
Classificazione del Problem	Questa fase prevede la classificazione del Problem con l'individuazione del Servizio Tecnologico impattato e del livello di urgenza (direttamente correlato con il concetto di priorità di intervento) e la relativa associazione del Problem agli eventuali incident esistenti. Il Problem Owner è responsabile della gestione del Problem per la parte di Investigazione e Diagnosi. Tale attività viene sottoposta a verifica da parte del Responsabile area Sistemi in sede di riunione del Comitato Tecnico.[Ticket Problem "*Opened*"]
Investigazione e diagnosi	Questa fase prevede l'attività di investigazione e diagnosi finalizzata ad identificare le cause associate al problema. Il Problem Owner ha la possibilità di aprire attività specifiche di analisi assegnabili al medesimo gruppo o a gruppi differenti. Al termine di tale fase è possibile definire il Problem come Known Error e dar seguito alla gestione del Problem stesso. Tale attività viene sottoposta a verifica da parte del Responsabile area Sistemi in sede di riunione del Comitato Tecnico.[Ticket Problem "*Under Diagnosis*"]
Gestione del Problem	Questa fase prevede la classificazione del problema come "Known Error" e la definizione delle cause associate; se possibile vengono avviate le attività del relativo workaround. In funzione di valutazioni tecnico/economiche il Service Manager valuta la necessità di aprire un Change, di mantenere un record dello stato del "Known Error" oppure la possibilità di risolvere il problem direttamente (in questo caso sarà comunque necessario disporre di un workaround accettabile). Nel caso di cambiamento richiesto, il Service Manager apre un record correlato al Change e la fase successiva di completamento del Change seguirà il processo specifico.[Ticket Problem "*Risolved*"]
Chiusura	In questa fase il problem potrà essere chiuso dal Service Manager oppure riaperto. Tale attività viene sottoposta a verifica da parte del Responsabile area Sistemi in sede di riunione del Comitato Tecnico.[Ticket Problem "*Closed*"]

1.5. SICUREZZA FISICA ED AMBIENTALE

Lo stabile del Fornitore è sorvegliato da personale specializzato 24 ore al giorno; la sala CED, dove si trovano i dispositivi hardware e software dei diversi sistemi del Fornitore, la sala di controllo dell'alimentazione elettrica, del sistema idraulico, del condizionamento e la sala di monitoraggio dei sistemi di sicurezza installati, è accessibile solo mediante utilizzo di badge autorizzato ed è controllato da un sistema TVCC; le porte sono dotate di allarmi a contatti magnetici; le stanze dell'area sono controllate mediante rivelatori combinati microonde e infrarossi.

Le zone interne sono tenute sotto controllo tramite allarmi a contatti magnetici su

finestre ed ingressi, sensori piezodinamici per la rilevazione della rottura dei vetri, rivelatori volumetrici a microonde/infrarossi e rivelatori antiallagamento nel sottopavimento. La difesa del perimetro esterno dello stabile è assicurata da una cancellata che delimita l'intera area, da barriere a raggi infrarossi per segnalare il superamento della barriera fisica e da un controllo perimetrale dell'edificio e degli accessi con sistema TVCC.

Le contromisure mirano a prevenire accessi non autorizzati, danni ed interferenze con il servizio offerto e rispondono ai seguenti principi:

- Controllo centralizzato delle apparecchiature e della sicurezza fisica: Le sedi del Fornitore sono costantemente monitorate da impianto di allarme antintrusione con sensori ottici, microonde e volumetrici distribuiti in tutti i locali esposti a pericolo. Il personale della Sala Controllo è dotato di un sistema di supervisione di alimentazione elettrica, degli apparati idraulici, del condizionamento e della sicurezza dotato di console grafiche che evidenziano con allarmi sonori e visivi eventuali malfunzioni o allarmi.
- Controllo degli accessi: L' accesso ai locali con apparecchiature tecnologiche sensibili è consentito mediante riconoscimento individuale tramite impianto di controllo accessi
- Continuità elettrica e generatori supplementari
- Condizionamento e controllo automatizzato della temperatura
- Rilevazione e soppressione incendi: Le sedi sono costantemente monitorate da impianto di allarme rivelazione fumi
- controllo accesso agli Edifici
- Sicurezza dell'area CED
- Protezione dei locali adibiti a ospitare i sistemi per l'erogazione del servizio.
- Protezione dei locali tecnici della sede di DR

CONTINUITÀ ELETTRICA E GENERATORI SUPPLEMENTARI

Tutte le apparecchiature del Data Center sono collegate alla rete elettrica attraverso gruppi di continuità che consentono di mantenere l'alimentazione in caso di interruzione dell'erogazione dell'energia elettrica. In caso di assenza dell'alimentazione per pochi cicli, intervengono automaticamente delle batterie tampone in grado di mantenere la continuità elettrica; per dare un'indicazione del

dimensionamento delle batterie, queste sono in grado di sopportare l'attuale carico complessivo di tutte le apparecchiature per circa un'ora. Se l'assenza di alimentazione si protrae per più di pochi secondi, vengono automaticamente avviati dei gruppi elettrogeni che iniziano a fornire l'alimentazione al gruppo di continuità.

CONDIZIONAMENTO E CONTROLLO AUTOMATIZZATO DELLA TEMPERATURA

Tutte le apparecchiature del Data Center sono collocate in locali dotati di condizionamento e controllo automatizzato della temperatura; il sistema di condizionamento viene gestito centralmente dalla Sala Controllo, la quale può intervenire tempestivamente a fronte di variazioni impreviste di temperatura.

RILEVAZIONE E SOPPRESSIONE INCENDI

I locali del Data Center sono tenuti sotto controllo tramite rivelatori ottici di fumo, i quali, qualora ve ne sia la necessità, provvedono ad innescare un sistema di spegnimento incendi a NAFS3.

PROTEZIONE DEI LOCALI CA

I sistemi destinati specificamente alla firma per la PEC, alla CA, alla firma e marcatura temporale sono collocati nei locali utilizzati per il servizio di Certificazione, all'interno dell'area CED.

Particolare cura è stata posta nel realizzare i collegamenti tra gli apparati presenti in quest'area: tutte le connessioni (cavi, bridge, router) sono allocate in maniera non direttamente accessibile. Per accedere al sito bisogna essere in possesso di un badge autorizzato e PIN personale di accesso.

L'ingresso al locale CA è protetto da bussola che consente l'ingresso di una sola persona autorizzata per volta.

All'interno del sito sono realizzate cinque salette, il cui accesso è protetto da una porta la cui apertura richiede nuovamente l'utilizzo del badge. Solo le persone autorizzate ad entrare nella specifica sala sono abilitate.

Tutte le porte sono dotate di allarmi a contatti magnetici. Il locale CA usufruisce del

sistema di rilevazione antincendio previsto per l'intero stabile, del sottosistema di spegnimento e dei rivelatori antiallagamento previsti per l'area CED. Nei locali all'interno di quest'area è presente il sottosistema di spegnimento incendi e nel sottopavimento sono installati i rivelatori antiallagamento.

Tutti i locali e le porte di accesso al locale CA sono controllati tramite sistema TVCC e rivelatori combinati microonde e infrarossi.

Per permettere l'accesso al personale esterno esistono specifici badge temporanei rilasciati dal servizio di sicurezza.

Usufruiscono del livello di protezione, sopra descritto, alcune postazioni degli operatori, la Sala Telecomunicazioni, la Saletta Sicurezza e la Sala di controllo e monitoraggio. In particolare:

SALETTA SICUREZZA

All'interno di questa sala vengono registrati gli accessi al locale CA.

Il controllo degli accessi viene effettuato tramite badge.

Sala Telecomunicazioni

L'area si trova in locali non direttamente accessibili.

SALA DI CONTROLLO E MONITORAGGIO

Per accedere all'area è necessario essere in possesso dell'apposito badge.

SICUREZZA DELLE RETI: PROTEZIONE DA INTRUSIONI

I sistemi e le reti sono connessi ad Internet in modo controllato da sistemi firewall che consentono di suddividere la connessione in aree a sicurezza progressivamente maggiore: rete Internet, reti DMZ (Demilitarized Zone) o Perimetrali, Reti Interne. Tutto il traffico che fluisce tra le varie aree è sottoposto ad accettazione da parte del firewall, sulla base di un set di regole stabilite. Le regole definite sui firewall vengono progettate in base ai principi di "default deny" (quanto non è espressamente permesso è vietato di default, ovvero, le regole consentiranno solo quanto è strettamente necessario al corretto funzionamento dell'applicazione) e "defense in

depth" (vengono organizzati livelli successivi di difesa, prima a livello di rete, tramite successive barriere firewall, ed infine a livello di sistema, (hardening))

La definizione delle politiche di accesso relativamente ai siti del Cliente saranno concordate, nel rispetto dei vincoli imposti dalle politiche stabilite dall'Area Sistemi di Sicurezza Informatica.

La gestione e l'implementazione delle regole di sicurezza dei firewall sono assicurate dalla struttura tecnica. I sistemi firewall sono in alta affidabilità (HA) e in bilanciamento di carico. Si tratta, infatti, di cluster Firewall realizzati con coppie di appliance indipendenti e collegati tra loro. Tali apparecchiature sono gestite, tramite appositi software, in modo che in caso di guasto di una delle macchine il traffico venga dirottato sul secondo nodo attivo del cluster in maniera trasparente per i servizi erogati.

I servizi di posta elettronica certificata esposti in internet sono sottoposti regolarmente a verifiche di intrusione software da parte di fornitori esperti in tematiche di intrusione e sicurezza.

I risultati delle verifiche sono analizzati dal Responsabile della Sicurezza e sono gestiti per mezzo di eventuali azioni correttive/adeguative/preventive/migliorative assegnate ai responsabili dei singoli servizi e monitorate.

BACKUP E DISASTER RECOVERY PLAN

Le politiche di backup prevedono salvataggio su nastro dei contenuti dei dischi dei sistemi server con frequenza settimanale e salvataggio incrementale giornaliero. La periodicità potrà essere aumentata in caso di necessità. Il tempo di ritenzione di un salvataggio sarà quindicinale per le copie settimanali e settimanale per gli incrementali giornalieri e potrà essere eventualmente adattato a esigenze particolari. Il servizio comprende la possibilità di restore di file system a fronte di problemi.

I media sono conservati in una sala adibita a tale compito e ricavata in spazi attigui alla sala macchine. Per quanto riguarda le condizioni di temperatura, umidità e sicurezza della nastroteca sono le medesime specificate per la sala macchine.

Il Fornitore, applicando le procedure standard internazionali, ha redatto un piano, composto da processi e da tecnologie, che consente di prevenire che eventi

disastrosi blocchino definitivamente ed irreparabilmente il proprio business. I dati e le applicazioni ritenuti essenziali e strategici per il fornitore vengono replicati giornalmente, grazie ad un doppio collegamento in fibra ottica. Con cadenza annuale, come previsto dal processo di gestione della Disaster Recovery, avvengono i test per verificare l'effettivo funzionamento dell'infrastruttura.

SLA

Si riportano nel seguito i parametri di Service Level Agreement sottoposti a controllo e monitoraggio su base mensile:

PARAMETRO	SLA TARGET
Disponibilità del servizio	99,5%
Tempo di attesa per l'accesso ad una pagina (esclusi download e upload documenti)	<= 5 secondi nel 95% dei casi
Tempo di ripristino	• Disservizi di severità 1: o entro 8 ore nel 100% dei casi Disservizi di severità 2: • o entro 16 ore nel 100% dei casi. • Disservizi di severità 3: o entro 4 giorni.
Percentuale di accessi alle pagine non riusciti	<= 3%
Percentuale di richieste di accesso da parte dell'Amministrazione per aggiornamento in remoto del sito che vanno a buon fine	> = 98%
Numero massimo di infrazioni dolose al sito tollerate	= 0

Ai fini della valutazione dei livelli di cui sopra si intende:

- livello di Severità 1 – Critical Business Impact, cioè un malfunzionamento che causa il blocco del sistema e l'interruzione delle attività;
- livello di Severità 2 – Significant Business Impact, cioè un malfunzionamento che causa la mancata disponibilità di features importanti, senza interruzione del servizio;
- livello di Severità 3 – Minor Business Impact, cioè richieste relative a caratteristiche e funzionalità ovvero un malfunzionamento che causa la mancata disponibilità di caratteristiche poco significative, in assenza di workaround.

1.6. ADEMPIMENTI PER LA SICUREZZA

Il Fornitore si impegna a porre in essere quanto necessario per garantire l'esecuzione delle attività in piena aderenza con le disposizioni del D.Lgs. 81/2008 s.m.i. , cooperando e coordinandosi, in particolare, con i referenti del Committente, ai fini degli adempimenti di cui all'art. 26 del citato decreto.

1.7. MODALITÀ DI FATTURAZIONE

In relazione all'oggetto di fornitura di cui al paragrafo 3, le fatture dovranno essere prodotte applicando la disciplina indicata nelle condizioni contrattuali art. 15 comma 3 e più specificatamente come di seguito indicato:

- Ai fini del pagamento del corrispettivo indicato nel presente contratto, il Fornitore potrà emettere fattura successivamente alla approvazione da parte della Committente del "consuntivo attività", contenente il dettaglio delle prestazioni erogate nel periodo di riferimento, nonché della verifica di conformità positiva. Nella fattura dovrà essere indicato il periodo temporale di riferimento.