AVVISO PUBBLICO DI INDAGINE ESPLORATIVA DEL MERCATO

OGGETTO: adeguamento della sicurezza informatica dei sistemi e macchinari dell'Ente al nuovo Codice dell'Amministrazione digitale di cui al D.Lgs. n. 217/17 del 13/12/2017 con sviluppo dei dettami tecnici previsti dalla CIRCOLARE AGID 18 aprile 2017, n. 2/2017, allegati 1 e 2 - Indagine esplorativa del mercato preliminare all'affidamento.

PREMESSA

L'Ente Regionale per il diritto allo Studio Universitario di Sassari (di seguito ERSU) intende affidare il servizio di adeguamento della sicurezza informatica dell'Ente al nuovo Codice dell'Amministrazione digitale di cui al D.Lgs n. 217/17 del 13/12/2017.

L'adeguamento predetto prevede lo sviluppo dei dettami tecnici previsti dalla CIRCOLARE AGID 18 aprile 2017, n. 2/2017, allegati 1 e 2, pubblicata sulla GU Serie Generale n. 103 del 05-05-2017 ed avente ad oggetto: "Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: <<Misure minime di sicurezza ICT per le pubbliche amministrazioni>>.

A tal fine, intende esperire una indagine esplorativa di mercato mediante il presente avviso teso ad individuare, nel rispetto dei principi di libera concorrenza, non discriminazione, trasparenza correttezza e pubblicità, idonei operatori economici da invitare a successiva procedura per l'affidamento diretto in appalto del servizio in oggetto, ove ricorrano le condizioni di cui all'art. 36, comma 2, lettera a), del D.Lgs. n. 50/2016 ("*Codice dei contratti pubblici*"), mediante ricorso al Mercato Elettronico della Regione Sardegna (piattaforma telematica SardegnaCAT), istituito con Deliberazione della Giunta Regionale n. 38/12 del 30/09/2014.

Il Mercato Elettronico della Regione Sardegna è accessibile all'URL https://www.sardegnacat.it/esop/ita-ras-host/public/web/login.jst o direttamente dal link presente nella home page della Regione Sardegna.

L'indagine di mercato di cui al presente avviso, pubblicato sul profilo di committente www.ersusassari.it (sezione ALBO PRETORIO > BANDI E GARE > BANDI DI GARA E PROCEDURE NEGOZIATE), sulla sezione dedicata ai *Servizi alle imprese* del sito istituzionale della Regione Sardegna www.regione.sardegna.it e nel portale del Ministero delle Infrastrutture e dei Trasporti (MIT) www.serviziocontrattipubblici.it (sezione *Avvisi),* ha il solo scopo di favorire la partecipazione e la consultazione di operatori economici, mediante acquisizione di manifestazione di interesse da parte degli stessi ad essere invitati a presentare offerta.

L'ERSU, al fine di garantire la più ampia contendibilità dell'appalto, non intende operare alcuna limitazione in ordine al numero di operatori economici che intendono partecipare alla presente procedura.

Atteso che in questa fase preliminare di progettazione della procedura di affidamento del servizio l'ERSU non dispone di elementi sufficienti per quantificare il valore dell'appalto e per valutare le misure e soluzioni più idonee offerte dal mercato per implementare e gestire la sicurezza nella rete informatica, gli operatori interessati dovranno allegare alla manifestazione di interesse una proposta tecnico-progettuale e la relativa quotazione economica secondo le modalità appresso indicate.

Il presente avviso non costituisce invito a partecipare a gara pubblica, né proposta contrattuale, ma è finalizzato unicamente ad esperire una indagine di mercato e, pertanto, non vincola in alcun modo l'ERSU che, in qualunque momento, potrà stabilire di non procedere all'affidamento diretto in appalto del servizio, ove non ricorrano le circostanze di cui all'art. 36, comma 2, lettera a), del D.Lgs. n. 50/2016 ovvero di affidare il servizio all'esito dell'esperimento di altre procedure disciplinate dal D.Lgs. n. 50/2016, finanche consultando più operatori iscritti nella categoria d'interesse nel Mercato Elettronico SardegnaCAT.

Pertanto, all'esito dell'indagine di mercato, previa valutazione delle proposte economiche e tecnico-progettuali presentate, ove comparabili, l'ente potrà procedere all'affidamento diretto del servizio appaltando, ove ricorrano le condizioni di cui all'art. 36, comma 2, lett. a) del D.Lgs. 50/2016, tramite Richiesta di Offerta (R.d.O.) nella predetta piattaforma telematica SardegnaCAT, all'operatore che abbia utilmente formulato la manifestazione d'interesse e presentato la migliore quotazione economica alla predetta indagine ed iscritto nella categoria merceologica d'interesse.

1 – CARATTERISTICHE DEL SERVIZIO, OGGETTO E DURATA DELL'APPALTO.

Al fine dell'adeguamento dei livelli di sicurezza informatica ai dettami di cui alla circolare AGID 2/17 allegati 1 e 2 del 18 aprile 2017, i Data Center dell'Ente dovranno essere adeguati, in termini di sicurezza e protezione, a quanto previsto dal Codice dell'Amministrazione digitale di cui al D.Lgs. n. 217/17 del 13/12/2017 ed a quanto previsto, in termini di protezione dati, dal Regolamento UE 679/16.

La seguente tabella visualizza le misure richieste, oltre a tutte le minime (M) dettate dalla circolare, sono anche previste alcune misure standard (S) e alcune alte (A) specifiche per le esigenze della struttura:

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Liv.	Descrizione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Liv.	Descrizione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Liv.	Descrizione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.

3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Liv.	Descrizione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.

4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Liv.	Descrizione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).

5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Liv.	Descrizione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.
8	9	2	M	Filtrare il contenuto del traffico web.
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Liv.	Descrizione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Liv.	Descrizione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.

A tal fine, dovrà essere garantita una proposta che implichi un'integrazione tra interventi tecnici, nuove Business Practice e processi che devono far leva su soluzioni altamente affidabili, flessibili, scalabili, che garantiscano la continuità dei servizi.
L'Ente provvederà alla fornitura di 2 Server, dislocati presso la propria sede, sui quali realizzare l'ambiente di Active Directory e di tutte le relative licenze (VMWare, Windows Server 2016, CAL per Active Directory).

Allo scopo di realizzare la proposta progettuale, si indica in circa 60 unità il numero totale delle utenze del personale ERSU che utilizza i Pc e di circa 530 studenti residenti presso gli alloggi i quali utilizzano la rete WiFi a loro riservata, distribuiti presso le sedi dell'Ente situate in Via Coppino (per circa 40 utenti e 240 studenti), via Manzella (circa 6 utenti e 100 studenti), Via dei Mille (circa 10 utenti), Via Verona (circa 3 utenti e 150 studenti) e Via La Marmora (1 utente e 40 studenti), ai quali si devono aggiungere una decina di apparati tra NAS e Server. La seguente tabella indica anche la tipologia della connessione ad Internet e fra le diverse sedi dell'Ente:

SEDE	**TIPOLOGIA DELLA CONNETTIVITA'**	**Utenti ERSU**	**Utenti Studenti**
Via Coppino n.4 (centro stella) Firewall SOPHOS XG210	Fibra 100 M – 100 M; ADSL 30720/3072 – 1024 (backup della fibra); Antenne per Via Manzella a 1Gb/s (Mikro Tik LHGG-60);	40	240
Via Manzella Firewall SOPHOS XG115	Antenne per Via Coppino a 1Gb/s (Mikro Tik LHGG-60); Antenne per Via dei Mille a 1Gb/s (Mikro Tik LHGG-60);	6	100
Via dei Mille n.102 Firewall SOPHOS XG115	Antenne per Via Manzella a 1Gb/s (Mikro Tik LHGG-60); ADSL 30720/3072 – 1024;	10	-
Via Verona n.9 Firewall SOPHOS XG115	ADSL 8192 – 4096;	3	150
Via La Marmora n.51 Firewall SOPHOS XG115	ADSL 8192/8192 – 4069;	1	40

Le sedi presso via Coppino, Via Manzella e via dei Mille sono collegate tramite ponte radio.
Gli appliance firewall SOPHOS XG115 e XG210, presenti in tutte le sedi, gestiscono la sicurezza, la rete Internet e le regole di accesso, NAT e PAT, rete LAN, le VPN fra le diverse sedi e con esterni, il captive portal, filtraggio dei contenuti, ecc.
Le postazioni di lavoro del personale di tutte le sedi sono dotate di torretta con 2 prese Lan collegate agli switch di piano (Netgear POE 48 porte).
Le postazioni di lavoro sono dotate di sistema operativo Windows7/8/10 Pro con antivirus su piattaforma Kasperky Security Center.
Al fine di ottimizzare le prestazioni e migliorare la sicurezza, sono presenti diverse VLan (uffici, studenti, timbratori, antenne, wireless, ecc.).
Per il backup sui server locali, andrà previsto uno spazio di circa 40 Gb / utente per cui 60 utenti X 40 Gb = 2.4 Tb.

L'operatore cui è affidato il servizio dovrà altresì:

- procedere alla rilevazione dei bisogni, con analisi dell'attuale contesto, per l'adeguamento richiesto ai dettami di cui alla circolare n. 2/17 allegati 1 e 2 ed al GDPR 679/16 in materia di protezione dati fornendo adeguata proposta;
- fornire l'elenco dettagliato delle attività che intende mettere in atto finalizzate al raggiungimento delle misure minime di sicurezza ICT per le pubbliche amministrazioni conformemente alla citata circolare AGID n. 2/17 ed attuazione delle misure tecniche necessarie a tale adeguamento sulla base di quanto previsto dal codice per l'amministrazione digitale di cui al **D.Lgs. n. 217/17 del 13/12/2017**;

A titolo meramente esemplificativo e non assolutamente esaustivo l'appaltatore dovrà altresì:

- configurare una piattaforma tecnologica basata su VMWare sulla quale creare 2 macchine virtuali Windows Server 2016, una per ogni server; successivamente provvedere **all'installazione e configurazione di un ambiente Active Directory su di un Domain Controller**; predisporre inoltre un ambiente secondario di

backup su cloud, allo scopo di mantenere attivo il Domain Controller nel caso in cui l'ambiente primario dovesse, per qualunque motivo, smettere di funzionare;
- fornire il Servizio BaaS – Backup as a Service: consiste in un servizio di backup allo scopo di effettuare il salvataggio dei dati presenti sul server i quali devono essere configurati per effettuare un backup periodico di una determinata cartella presente sui Pc degli utenti;
- provvedere alla creazione degli utenti, dei gruppi e dei permessi, alla configurazione del sistema delle autenticazioni e dei log, alla configurazione di 4 postazioni di lavoro per ogni diversa sede;
- **VMWare:** Supporto specialistico per l'installazione della piattaforma VMWare con l'installazione di macchine virtuali con sistema operativo Microsoft (Windows Server 2016, Windows 7 e superiore) e Linux.

Tutte le attività di cui sopra dovranno essere mirate a fornire una soluzione completa e funzionante, conforme alle direttive del D.Lgs. n. 217/17 del 13/12/2017, della predetta circolare e del GDPR n. 679/16 per quanto riguarda la protezione dei dati, il tracciamento degli accessi ai dati ed alle operazioni svolte su di essi.

NOTA BENE: tutte le attività descritte nella tabella sopra riportata e al seguito nel presente paragrafo 1 dovranno essere realizzate entro 8 mesi dalla stipula del contratto di appalto.
L'appalto prevede altresì le seguenti prestazioni che saranno realizzate nel corso dell'intera durata biennale del contratto:
- supporto specialistico per la durata di 24 mesi on site;
- formazione specialistica sulle attività svolte in maniera da rendere autonomo il personale dell'Ente interessato alle attività in appalto per un totale di n. 40 ore.

2 - CONDIZIONI DI PARTECIPAZIONE E CRITERI DI SELEZIONE DEGLI OPERATORI ECONOMICI.
Possono partecipare alla procedura per l'affidamento dell'appalto in oggetto gli operatori economici indicati nell'art. 45 del D.Lgs n. 50/2016 per i quali non sussistano:
a) i motivi di esclusione di cui all'art. 80 del D.Lgs n. 50/2016;
b) le condizioni di cui all'art. 53, comma 16-ter, del D.Lgs n. 165/2001 o di cui all'art. 35 del D.L. n. 90/2014, convertito con modificazioni dalla L. n. 114/2014, o che non siano incorsi, ai sensi della normativa vigente, in ulteriori divieti a contrattare con la pubblica amministrazione.

Tali operatori devono altresì soddisfare i seguenti criteri di selezione:
c) idoneità professionale - Iscrizione nel registro delle imprese della Camera di commercio, industria, artigianato e agricoltura per attività inerente il servizio oggetto dell'appalto;
d) Capacità tecnica e professionale per cui dovrà essere dimostrato:
   d.1) di aver configurato e rese operative negli ultimi 3 anni antecedenti il presente avviso, installazioni in ambienti data center con tecnologie cloud enabled presso enti pubblici e privati con più di 50 utenti;
   d.2) di disporre di risorse proprie certificate VMWare / Microsoft.

Poiché la procedura negoziata per l'affidamento diretto dell'appalto sarà interamente espletata sul Mercato Elettronico della Regione Sardegna (piattaforma telematica SardegnaCAT), è inoltre condizione necessaria per essere invitati a presentare offerta l'iscrizione al predetto Mercato, nella categoria "AD26 - SERVIZI DI ASSISTENZA INFORMATICA E DI SUPPORTO" e/o sottocategoria della stessa, alla data stabilita quale termine ultimo per la presentazione delle manifestazioni di interesse. La mancata iscrizione dell'operatore economico al Mercato Elettronico della Regione Sardegna nella predetta categoria, alla data stabilita quale termine ultimo per la presentazione delle manifestazioni di interesse, è causa di esclusione dalla procedura.

Gli operatori economici potranno dichiarare ai sensi e per gli effetti degli artt. 46 e 47 del D.P.R. n. 445/2000 l'assenza di condizioni ostative e il possesso dei requisiti di cui sopra avvalendosi del modello di *manifestazione di interesse* unito al presente avviso.
Per l'iscrizione al Mercato Elettronico della Regione Sardegna (SardegnaCAT) è necessario accedere al link https://www.sardegnacat.it/esop/ita-ras-host/public/web/servizi_imprese/registrazione.jst e seguire le istruzioni ivi riportate.

Si rappresenta che, ai fini dell'iscrizione, l'operatore economico dovrà essere dotato di firma digitale e di strumentazione tecnica e informatica adeguata ai requisiti minimi di sistema accessibili dalla home page del sito internet www.sardegnacat.it.
Si invitano gli operatori economici interessati a verificare attentamente che la procedura di iscrizione alla piattaforma SardegnaCAT sia stata regolarmente completata e che la stessa sia andata a buon fine.
Per chiarimenti sulle procedure di iscrizione e sulle modalità tecnico operative di uso della piattaforma SardegnaCAT, si segnalano le modalità e i canali di contatto indicati nella pagina web all'indirizzo https://www.sardegnacat.it/esop/ita-ras-host/public/web/contatti.jst.

3 – SOPRALLUOGO PRELIMINARE

Al fine di acquisire conoscenza delle attuali condizioni, hardware in uso, configurazioni e di qualunque altra informazione utile alla partecipazione alla presente procedura, è facoltà degli operatori interessati fissare un appuntamento per un sopralluogo da effettuare presso le diverse sedi dell'Ente. Si fa presente che ai fini della partecipazione alla presente procedura, il sopralluogo non è obbligatorio, ma meramente facoltativo.
Il sopralluogo potrà essere effettuato a partire dal giorno successivo alla data di pubblicazione del presente avviso, indicativamente dal lunedì al venerdì tutti i giorni dalle ore 9.00 alle ore 13.00, fino a due giorni prima della data indicata quale termine ultimo per la presentazione delle manifestazioni di interesse, previa richiesta indirizzata al referente tecnico informatico presso la Direzione generale, inoltrata via E-MAIL all'indirizzo a.nigra@ersusassari.it e successiva convocazione in giorno ed ora stabiliti dall'ERSU. Non saranno prese in considerazione richieste di sopralluogo non pervenute all'ERSU in tempo utile all'organizzazione dello stesso nel rispetto del termine sopra indicato. L'ERSU potrà accordare il sopralluogo unicamente al rappresentante legale o al direttore tecnico dell'operatore concorrente, nonché ai dipendenti muniti di delega. Al termine delle operazioni di sopralluogo l'ERSU, mediante proprio incaricato, rilascerà l'attestazione di avvenuto sopralluogo.

4 - PRESENTAZIONE DI MANIFESTAZIONE DI INTERESSE / RICHIESTA DI INVITO ALLA PROCEDURA DI GARA.

La manifestazione di interesse e la relativa proposta economica, redatte in conformità al modello allegato *"Manifestazione di interesse"*, dovrà pervenire **entro e non oltre il giorno 03/12/2018** esclusivamente a mezzo posta elettronica certificata all'indirizzo affarigenerali@pec.ersusassari.it con indicazione nell'oggetto della seguente dicitura ***"MANIFESTAZIONE DI INTERESSE PER L'AFFIDAMENTO DEL SERVIZIO DI ADEGUAMENTO DELLA SICUREZZA INFORMATICA DEI SISTEMI E MACCHINARI DELL'ENTE".***
La manifestazione di interesse dovrà essere redatta dal titolare o legale rappresentante dell'operatore economico, debitamente sottoscritta mediante firma digitale di cui all'art. 1, comma 1, lett. s) del D.Lgs. n. 82/2005 e corredata di un documento di identità in corso di validità del sottoscrittore stesso.
Nella manifestazione di interesse l'operatore economico dovrà:

- dichiarare i riferimenti dei soggetti di cui all'art. 80, comma 3, del D.Lgs. n. 50/2016 con riguardo ai quali deve essere verificata l'assenza di motivi di esclusione di cui allo stesso predetto art. 80, commi 1 e 2, del D.Lgs. n. 50/2016;
- dichiarare espressamente di non trovarsi in alcuna delle situazioni che configurano motivi di esclusione dalle procedure di affidamento di pubblici contratti;
- dichiarare espressamente di soddisfare i criteri di selezione secondo quanto indicato al precedente paragrafo 2 del presente avviso con riguardo all'idoneità professionale e alle capacità tecnico professionali, conformemente al modello di manifestazione di interesse allegato;
- comunicare l'indirizzo PEC al quale verranno indirizzate tutte le eventuali comunicazioni riguardanti la presente procedura di indagine;
- dichiarare, se ricorre il caso, la data in cui è stato eventualmente effettuato il sopralluogo preliminare (facoltativo) di cui al paragrafo 3 del presente invito [nota bene: in allegato alla manifestazione d'interesse nella stessa comunicazione inoltrata via PEC all'indirizzo sopra indicato dovrà essere allegata copia in formato digitale dell'*attestazione di avvenuto sopralluogo* rilasciata dall'ERSU in occasione della visita dei locali interessati al servizio di che trattasi];

- dichiarare di essere iscritto al Mercato Elettronico della Regione Sardegna (piattaforma SardegnaCAT) nella categoria merceologica di interesse, specificando esattamente la/le categorie in cui è iscritto;
- dichiarare di avere perfetta conoscenza delle norme generali e speciali che regolano l'appalto e di tutti gli obblighi derivanti dalle prescrizioni degli atti della presente procedura e accetta incondizionatamente tutte le clausole e le condizioni riportate nel presente avviso e nel Patto di integrità che ha esaminato con diligenza ed in modo adeguato avendo, pertanto, preso conoscenza di tutte le condizioni locali e circostanze che possono aver influito sulla determinazione dei prezzi e sulla quantificazione della proposta economica presentata;
- di acconsentire al trattamento dei dati personali trasmessi, anche con strumenti informatici, nel rispetto della disciplina dettata dal Regolamento UE n. 679/2016 e secondo quanto previsto dal D.Lgs. n.196/2003 ove compatibile con il predetto Regolamento ed esclusivamente per le finalità di cui alla presente procedura di indagine di mercato;

La manifestazione di interesse dovrà altresì essere corredata da un elaborato contenente la **PROPOSTA TECNICO-PROGETTUALE**, parimenti sottoscritta con firma digitale dal rappresentante legale dell'operatore concorrente, recante una descrizione dettagliata delle attività da svolgere, corredata da schemi e metodologie con giustificazione delle scelte tecnologiche adottate e gli obiettivi da raggiungere in riferimento alle prestazioni oggetto dell'appalto, nonché da tutte le informazioni utili per consentire all'ERSU di valutare le modalità con cui l'operatore intende implementare le misure di sicurezza ICT e realizzare le prestazioni di servizi indicate al paragrafo 1. del presente avviso. Inoltre, la proposta dovrà recare l'indicazione delle modalità di implementazione delle misure indicate negli schemi di tabella riportate al medesimo paragrafo 1 del presente avviso (misure contrassegnate dal codice ABSC1, 2, 3, 4, 5, 8, 10, 13). Tale proposta costituirà la base di riferimento per la redazione a cura dell'ERSU del modulo di implementazione di cui all'allegato 2 della circolare AGID 18 APRILE 2017, N. 2/2017.
L'elaborato dovrà altresì indicare l'espressa previsione da parte dell'operatore proponente di realizzare i servizi oggetto del progetto entro 8 mesi dalla stipula del contratto di appalto e l'impegno di fornire adeguato supporto specialistico in loco e garantire la formazione specialistica sulle attività svolte per un totale di n. 40 ore (in maniera da rendere autonomo il personale dell'Ente interessato alle attività in appalto) nel corso dell'intera durata biennale del contratto.

Inoltre, la proposta tecnico-progettuale dovrà indicare la quotazione (in cifre e in lettere) dell'offerta proposta al netto di IVA per le prestazioni oggetto del progetto.

Non saranno ammesse istanze incomplete, pervenute oltre il termine sopra indicato o non sottoscritte digitalmente, ovvero non saranno valutate nella presente procedura manifestazioni di interesse non corredate dalla proposta tecnico-progettuale articolata e completa dei contenuti sopra descritti o mancante dell'indicazione della quotazione dell'offerta proposta per le prestazioni oggetto del progetto.

5 - UNITÀ RESPONSABILE DEL PROCEDIMENTO.
Il Responsabile Unico del Procedimento è la dottoressa Ambra Giordano (tel. 0799940042) col supporto informatico del dott. Alessandro Nigra (079/9940032).
Eventuali chiarimenti sulla presente procedura di indagine di mercato potranno essere richiesti tramite PEC all'indirizzo affarigenerali@pec.ersusassari.it.

6 - TRATTAMENTO DEI DATI PERSONALI.
Con riferimento al trattamento dei dati si precisa quanto segue:

1. il soggetto attivo della raccolta e del trattamento dei dati richiesti, anche sensibili in quanto a carattere giudiziario, è l'E.R.S.U. in qualità di "Titolare del trattamento", in persona del legale rappresentante delegato dott. Antonio Arghittu tel. 079/9940020
   mail: **segreteria.direzione@ersusassari.it** - PEC affarigenerali@pec.ersusassari.it
2. il Responsabile della protezione dei dati ex art. 37 del Regolamento UE n. 679/16 è il dott. Alessandro Inghilleri PEC: rdp@pec.regione.sardegna.it
3. I dati sono richiesti e trattati dal Titolare in relazione ad obbligo di legge, con quanto conseguente;

4. I dati personali forniti dagli Operatori economici ai fini della partecipazione alla presente procedura saranno raccolti e trattati nell'ambito del medesimo procedimento e dell'eventuale, successiva stipula e sino alla fine della gestione del contratto, secondo le modalità e finalità di cui al Regolamento UE n. 679/2016 e secondo quanto previsto dal D.Lgs. n. 196/2003 ove compatibile con il predetto Regolamento.
5. I diritti spettanti all'interessato sono quelli di cui ai succitati riferimenti normativi al quale si fa espresso rinvio per tutto quanto non previsto dal presente paragrafo.

Il Direttore Generale
Antonello Arghittu

Atto pubblicato sul profilo di committente www.ersusassari.it in data 12/11/2018.