



Regione Umbria

Giunta Regionale

DELIBERAZIONE DELLA GIUNTA REGIONALE

N. 998 SEDUTA DEL 28/09/2022

OGGETTO: Avviso ACN per la realizzazione di interventi di potenziamento della resilienza cyber a valere sul PNRR, Missione 1 - Componente 1 - Investimento 1.5 Cybersecurity. Partecipazione della Regione Umbria.

		PRESENZE
Tesei Donatella	Presidente della Giunta	Assente
Morrone Roberto	Vice Presidente della Giunta	Presente
Agabiti Paola	Componente della Giunta	Presente
Coletto Luca	Componente della Giunta	Presente
Fioroni Michele	Componente della Giunta	Presente
Melasecche Germini Enrico	Componente della Giunta	Presente

Presidente: **Roberto Morrone**

Segretario Verbalizzante: Cristina Clementi

Atto firmato digitalmente ai sensi delle vigenti disposizioni di legge

L'atto si compone di 7 pagine

LA GIUNTA REGIONALE

Visto il documento istruttorio concernente l'argomento in oggetto: “**Avviso ACN per la realizzazione di interventi di potenziamento della resilienza cyber a valere sul PNRR, Missione 1 - Componente 1 - Investimento 1.5 Cybersecurity. Partecipazione della Regione Umbria.**” e la conseguente proposta di 'Assessore Michele Fioroni

Preso atto:

- a) del parere favorevole di regolarità tecnica e amministrativa reso dal responsabile del procedimento;
- b) del parere favorevole sotto il profilo della legittimità espresso dal Dirigente competente;
- c) del parere favorevole del Direttore in merito alla coerenza dell'atto proposto con gli indirizzi e gli obiettivi assegnati alla Direzione stessa;

Vista la legge regionale 1 febbraio 2005, n. 2 e la normativa attuativa della stessa;

Visto il Regolamento interno di questa Giunta;

A voti unanimi espressi nei modi di legge,

DELIBERA

per le motivazioni contenute nel documento istruttorio che è parte integrante e sostanziale della presente deliberazione

- 1) di demandare al servizio “*Servizio Sistemi informativi sanitari, sanità digitale e innovazione*” la predisposizione di quanto necessario alla partecipazione, con un progetto per il sistema sanitario regionale, all'avviso ACN per la realizzazione di interventi di potenziamento della resilienza cyber a valere sul PNRR, Missione 1 - Componente 1 - Investimento 1.5 Cybersecurity;
- 2) di demandare al servizio “*Servizio Sistema informativo regionale, Infrastrutture digitali*” la predisposizione di quanto necessario alla partecipazione, con un progetto per il sistema regionale non-sanitario, all'avviso ACN per la realizzazione di interventi di potenziamento della resilienza cyber a valere sul PNRR, Missione 1 - Componente 1 - Investimento 1.5 Cybersecurity;
- 3) di istituire un “comitato tecnico per la cybersicurezza” che comprende i responsabili dei sistemi informativi delle singole aziende sanitarie, e progressivamente delle altre agenzie/partecipate regionali, le strutture ICT della regione con competenze sulla sicurezza informatica e i rappresentanti di PuntoZero Scarl cui compete la sicurezza del cloud ibrido/data center regionale e della rete RUN, demandando a tale comitato l'attuazione delle progettualità di cui all'avviso ACN e la definizione degli accordi necessari tra gli enti per rendere operativi i progetti, coordinare gli affidamenti necessari e implementare l'unità locale di cybersicurezza su scala regionale;
- 4) di demandare al servizio “*Servizio Sistema informativo regionale, Infrastrutture digitali*” i successivi atti necessari all'avvio ed alla gestione del “comitato tecnico per la cybersicurezza”;
- 5) di dare atto che il presente provvedimento è soggetto a pubblicazione nel sito istituzionale ai sensi dell'art.12 e dell'art.26, comma 1, del d.lgs. n.33/2013.

DOCUMENTO ISTRUTTORIO

Oggetto: Avviso ACN per la realizzazione di interventi di potenziamento della resilienza cyber a valere sul PNRR, Missione 1 - Componente 1 - Investimento 1.5 Cybersecurity. Partecipazione della Regione Umbria.

Visto l'avviso n.3/2022 dell'Agenzia per la cybersicurezza nazionale (ACN) per la presentazione di proposte per la realizzazione di interventi di potenziamento della resilienza cyber a valere sul PNRR "Missione 1 - Componente 1 - Investimento 1.5 Cybersecurity", sono state elaborate, dalle strutture ICT regionali e da PuntoZero Scarl, delle proposte progettuali da realizzare nell'ambito del sistema regionale:

- analisi della postura di sicurezza e piano di potenziamento;
- miglioramento dei processi e dell'organizzazione di gestione della cybersecurity;
- miglioramento della consapevolezza delle persone;
- progettazione e sviluppo di nuovi sistemi per la mitigazione del rischio cyber;

I quadri economici complessivi ipotizzati per tali progettualità sono i seguenti, ma potranno essere soggetti a variazione in fase di presentazione/progettazione esecutiva:

1. Potenziamento della resilienza cyber della sanità umbra fino ad un budget massimo pari ad € 1.000.000,00, con il seguente quadro economico:

TIPOLOGIA INTERVENTO	TOTALE (al netto di IVA)	TOTALE IVA¹	IMPORTO FINANZIAMENTO RICHiesto
Analisi della postura di sicurezza e piano di potenziamento	0		0
Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	0		0
Miglioramento della consapevolezza delle persone	327.869	72.131	400.000
Progettazione e sviluppo di nuovi sistemi e servizi per la mitigazione del rischio cyber	491.803	108.197	600.000

2. Innalzamento livello di Sicurezza dell'infrastruttura tecnologica regionale Umbra fino ad un budget massimo pari ad € 1.000.000,00, con il seguente quadro economico:

TIPOLOGIA INTERVENTO	TOTALE (al netto di IVA)	TOTALE IVA²	IMPORTO FINANZIAMENTO RICHiesto
Inserimento componente di sicurezza attivo con analisi del comportamento dei sistemi e non su "firme" – contrasto agli 0-Day ed agli Internals;	€ 368.032,79	€ 80.967,21	€ 449.000,00
Attivazione del processo di controllo continuo delle vulnerabilità e della superficie d'attacco	€ 285.655,74	€ 62.844,26	€ 348.500,00
Dotazioni tecnologiche dedicate all'attività di CyberSecurity (Potenza computazionale e storage);	€ 81.967,21	€ 18.032,79	€ 100.000,00
Analisi Reputazionale per identificare obiettivi esposti e falle di sicurezza da condurre su dark e deep web;	€ 42.213,11	€ 9.286,89	€ 51.500,00
Servizi per l'implementazione degli interventi progettuali svolti dall'in-house	€ 51.000,00	€ 0	€ 51.000,00

Il sistema regionale costituito dalla Regione Umbria e dalle 4 Aziende sanitarie ha già investito notevoli risorse in sicurezza informatica negli ultimi anni, ma nel complesso permangono delle criticità nelle capacità di gestione del rischio cyber da parte dei singoli Enti. Anche in presenza di strumenti software e hardware di recente implementazione, risulta scarso il numero di risorse umane specializzate dedicate alla sicurezza informatica e al presidio dei sistemi. Questo non permette di sfruttare appieno le potenzialità degli strumenti e strutturare processi operativi stabili nel tempo.

Ne deriva inoltre un livello di sicurezza non uniforme nei vari enti e nei vari casi applicativi, il che rappresenta una problematica aggiuntiva per il "sistema regione" nel suo complesso vista la presenza di numerosi sistemi inter-aziendali e di stretta collaborazione tra i vari Enti che negli anni hanno portato avanti molte iniziative congiunte sul lato infrastrutturale ed applicativo, anche con il supporto della società in house regionale.

La Regione intende gestire il progetto mediante la società in-house Puntozero scarl già affidataria dei progetti in materia di cybersicurezza in corso di attuazione e gestore del data center regionale (DCRU e cloud ibrido regionale) e della rete pubblica regionale RUN in particolare tramite interventi di aumento della sicurezza del DCRU, hardening delle sedi regionali, progettazione e realizzazione di un SOC. La Regione Umbria, altresì, ha sempre svolto il ruolo di coordinamento dei sistemi informativi sanitari delle aziende sanitarie pubbliche e la società in house Puntozero svolge il ruolo di centrale acquisti per la sanità sia per l'Ente Regione che per le Aziende sanitarie che partecipano al progetto. Ciò consente la gestione unitaria del progetto sia per le componenti comuni che per quelle di competenza delle singole aziende sanitarie.

Alla luce di quanto sopra descritto appare quindi necessario effettuare una attività di analisi della postura di sicurezza, attività già avviata, sia a livello regionale sui sistemi condivisi che a livello di singola azienda sanitaria, per poi implementare un piano di potenziamento strategico su scala regionale che coinvolga anche gli aspetti specifici della sicurezza a livello aziendale, proprio per risolvere le

criticità di sistema sopra evidenziate ed uniformare la postura di sicurezza complessiva. Il progetto presentato punta alla costituzione e avvio di una "unità locale di cybersicurezza" condotta dalla società in house PuntoZero Scarl che si farà carico di tutte le attività di coordinamento delle difese della Regione e delle Aziende sanitarie, per fare fronte comune contro gli attacchi, presidiare la sicurezza dei sistemi condivisi inter-aziendali, sfruttare ogni possibile sinergia tra i servizi di sicurezza facendo comunicare i vari SOC sia in fase di monitoraggio/difesa che in fase di eventuale risposta a incidenti di sicurezza, studio delle opportunità di rafforzamento delle configurazioni di sicurezza perimetrale e monitoraggio degli enti, attività per uniformare le procedure di sicurezza e individuare le buone pratiche comuni a livello regionale.

L'unità locale di cybersicurezza è una iniziativa di supporto operativo che si affianca, in modo sinergico, alle iniziative per i CERT/CSIRT regionali già in corso di progettazione/realizzazione.

Il coinvolgimento delle aziende sanitarie, e progressivamente delle altre agenzie/partecipate regionali, nel progetto avverrà attraverso la stesura di apposito accordo tra regione e gli altri soggetti nonché con la costituzione di un "comitato tecnico per la cybersicurezza" che comprenderà i responsabili dei sistemi informativi delle aziende, gli uffici ICT della regione con il supporto della stessa PuntoZero Scarl.

Infine, va sottolineato come la realizzazione di interventi tesi ad innalzare il livello di cybersicurezza del sistema sanitario regionale è necessario anche per l'attuazione degli interventi di digitalizzazione previsti nel PNRR missione 6 di cui alla DGR n.516/2022, anche alla luce di quanto previsto nel "Piano sanitario regionale PSR Umbria 2022-2026" adottato con DGR n.793/2022.

Tutto ciò premesso si propone alla Giunta regionale:

1. di demandare al servizio "*Servizio Sistemi informativi sanitari, sanità digitale e innovazione*" la predisposizione di quanto necessario alla partecipazione, con un progetto per il sistema sanitario regionale, all'avviso ACN per la realizzazione di interventi di potenziamento della resilienza cyber a valere sul PNRR, Missione 1 - Componente 1 - Investimento 1.5 Cybersecurity;
2. di demandare al servizio "*Servizio Sistema informativo regionale, Infrastrutture digitali*" la predisposizione di quanto necessario alla partecipazione, con un progetto per il sistema regionale non-sanitario, all'avviso ACN per la realizzazione di interventi di potenziamento della resilienza cyber a valere sul PNRR, Missione 1 - Componente 1 - Investimento 1.5 Cybersecurity;
3. di istituire un "comitato tecnico per la cybersicurezza" che comprende i responsabili dei sistemi informativi delle singole aziende sanitarie, e progressivamente delle altre agenzie/partecipate regionali, le strutture ICT della regione con competenze sulla sicurezza informatica e i rappresentanti di PuntoZero Scarl cui compete la sicurezza del cloud ibrido/data center regionale e della rete RUN, demandando a tale comitato l'attuazione delle progettualità di cui all'avviso ACN e la definizione degli accordi necessari tra gli enti per rendere operativi i progetti, coordinare gli affidamenti necessari e implementare l'unità locale di cybersicurezza su scala regionale;
4. di demandare al servizio "*Servizio Sistema informativo regionale, Infrastrutture digitali*" i successivi atti necessari all'avvio ed alla gestione del "comitato tecnico per la cybersicurezza";
5. di dare atto che il presente provvedimento è soggetto a pubblicazione nel sito istituzionale ai sensi dell'art.12 e dell'art.26, comma 1, del d.lgs. n.33/2013.

PARERE DI REGOLARITÀ TECNICA E AMMINISTRATIVA

Ai sensi del vigente Regolamento interno della Giunta: si esprime parere favorevole in ordine alla regolarità tecnica e amministrativa del procedimento e si trasmette al Dirigente per le determinazioni di competenza.

Perugia, lì 27/09/2022

Il responsabile del procedimento
Mirco Marcagnani

FIRMATO

Firma apposta digitalmente ai sensi
delle vigenti disposizioni di legge

PARERE DI LEGITTIMITÀ

Ai sensi del vigente Regolamento interno della Giunta;

Visto il documento istruttorio;

Atteso che sull'atto è stato espresso:

- il parere favorevole in ordine alla regolarità tecnica e amministrativa reso dal responsabile del procedimento;

Si esprime parere favorevole in merito alla legittimità dell'atto

Perugia, lì 27/09/2022

Il dirigente del Servizio
Sistema informativo regionale,
infrastrutture digitali

Graziano Antonielli

FIRMATO

Firma apposta digitalmente ai sensi
delle vigenti disposizioni di legge

PARERE DEL DIRETTORE

Il Direttore, ai sensi e per gli effetti degli artt. 6, l.r. n. 2/2005 e 13 del Regolamento approvato con Deliberazione di G.R., 25 gennaio 2006, n. 108:

- riscontrati i prescritti pareri del vigente Regolamento interno della Giunta,
- verificata la coerenza dell'atto proposto con gli indirizzi e gli obiettivi assegnati alla Direzione, esprime parere favorevole alla sua approvazione.

Perugia, lì 27/09/2022

IL DIRETTORE
DIREZIONE REGIONALE SVILUPPO
ECONOMICO, AGRICOLTURA, LAVORO,
ISTRUZIONE, AGENDA DIGITALE
Luigi Rossetti
Titolare

FIRMATO
Firma apposta digitalmente ai sensi
delle vigenti disposizioni di legge

PROPOSTA ASSESSORE

L'Assessore Michele Fioroni ai sensi del vigente Regolamento della Giunta regionale,

propone

alla Giunta regionale l'adozione del presente atto

Perugia, lì 27/09/2022

Assessore Michele Fioroni
Titolare

FIRMATO
Firma apposta digitalmente ai sensi
delle vigenti disposizioni di legge
