

**DETERMINA DEL DIRETTORE GENERALE DELLA
AST DI FERMO**

N. 773/AST_FM DEL 07/12/2023

**Oggetto: DEFINIZIONE E NOMINA DEL GRUPPO OPERATIVO DELLA
CYBERSICUREZZA AZIENDALE DELL'AST DI FERMO**

**IL DIRETTORE GENERALE DELLA
AST DI FERMO**

- -

VISTO il documento istruttorio qui approvato e riportato in calce alla presente determina di cui costituisce parte integrante e sostanziale e dal quale si rileva la necessità di provvedere a quanto in oggetto specificato;

RITENUTO, per i motivi riportati nel predetto documento istruttorio, di adottare il presente atto;

ACQUISITI i pareri favorevoli del Direttore Amministrativo e del Direttore Sanitario sottoscritti in calce

VISTA l'attestazione del Responsabile dell'U.O.S.D. Controllo di Gestione;

- D E T E R M I N A -

1) di nominare, in riferimento all'obiettivo 30N per l'anno 2023 indicato dalla Regione Marche, "Definizione di una organizzazione per la Cybersicurezza dei servizi a catalogo", quali responsabili del gruppo operativo dei tecnici informatici per la cybersicurezza aziendale i seguenti tecnici informatici attualmente in carico all'UOC SIA che effettuano la reperibilità H 24/7:

- Ing. Jr. Roberto Rogante: collaboratore informatico cat. D (con posizione organizzativa), con funzione di coordinamento del gruppo della cybersicurezza aziendale;
- Ing. Demis Corazza: collaboratore informatico cat. D;
- P.ind. Paolo Silenzi: programmatore informatico cat. C;
- P.inf. Leonardo Caciorgna: programmatore informatico cat. C

i quali dovranno gestire tale attività aziendale in stretta collaborazione con la struttura della cybersicurezza regionale, presente nel Settore Transizione Digitale e Informatica della Regione Marche, nei limiti della responsabilità contrattuale propria dell'inquadramento contrattuale di ogni dipendente;

- 2) di definire, come anche indicato dalla Dirigente del Settore Transizione Digitale e Informatica della Regione Marche, per quanto possibile, all'interno del team di lavoro per la cybersicurezza, anche un'articolazione in riferimento alle diverse principali tematiche informatiche/informative aziendali, come di seguito indicato:
 - Ing. jr Roberto Rogante: rete dati, data center e cluster server aziendale, sito extranet/intranet e posta aziendale;
 - Ing. Demis Corazza: rete dati, data center e cluster server aziendale;
 - P. ind. Paolo Silenzi: sito extranet/intranet e posta aziendale;
 - P.inf. Leonardo Caciorgna: data center e cluster server aziendale;
- 3) di definire che il gruppo operativo, ed in particolare, il coordinatore del gruppo, sarà l'interfaccia diretta nella gestione operativa della cybersicurezza aziendale dell'AST di Fermo, in situazioni di normalità e d'urgenza, del gruppo della cybersicurezza regionale;
- 4) di definire che la responsabilità organizzativa e di programmazione della cybersicurezza dell'AST di Fermo, risulta in capo al Direttore dell'UOC SIA;
- 5) di attestare che dalla presente determina non deriva alcun onere di spesa a carico del Bilancio dell'AST di Fermo;
- 6) di richiedere al Settore Transizione Digitale e Informatica della Regione Marche la partecipazione del gruppo della cybersicurezza ai corsi di formazione specifici convenzionati con le Università e gli enti di competenza;
- 7) di trasmettere il presente atto al Settore Transizione Digitale e Informatica della Regione Marche e ai componenti del gruppo della cybersicurezza nominati nella presente determina;
- 8) di trasmettere il presente atto al Collegio Sindacale a norma dell'art. 28 della L.R. 19 del 08.08.2022 e s.m.i.;
- 9) di dichiarare che il presente atto è efficace dal giorno di pubblicazione nell'albo pretorio informatico dell'AST di Fermo, ai sensi del comma 8 dell'art.39 della L.R. n.19/2022;

Il Direttore Amministrativo
Dott. Alberto Carelli

Il Direttore Sanitario
Dott.ssa Simona Bianchi

Il Direttore Generale
Dr. Gilberto Gentili

Per il parere infrascritto:

U.O.S.D. SUPPORTO ALL'AREA CONTROLLO DI GESTIONE

Sulla base di quanto dichiarato dal Direttore dell'UOC SIA-RTD si attesta che dal presente atto non derivano oneri a carico del Bilancio di questa Azienda Sanitaria Territoriale

Il Responsabile
U.O.S.D. Supporto all'Area Controllo di Gestione
Dott. Daniele Rocchi

La presente determina consta di n. 8.

- DOCUMENTO ISTRUTTORIO -
(UOC SIA AST FM)

Normative e atti di riferimento:

- **Direttiva UE 2016/1148** - nota come *Direttiva NIS:* " *Sicurezza delle reti e dei sistemi informativi*";
- **D.lgs. n.65 del 18 maggio 2018:** " *Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*";
- **DL n.105/2019:** " *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica (e di disciplina dei poteri speciali nei settori di rilevanza strategica)*;
- **DL n.162 /2019:** " *Disposizioni urgenti in materia di proroga di termini legislativi, di organizzazione delle pubbliche amministrazioni, nonché di innovazione tecnologica*";
- **DL n.82 del 14 giugno 2021:** " *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*", convertito in
- **Legge n.10 del 4 agosto 2021:** " *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*";
- **Legge Regionale n.19 del 08/08/2022:** " *Organizzazione del Servizio Sanitario Regionale*".

Premesso che:

Considerata la vulnerabilità delle reti informatiche, dei sistemi informativi e dei servizi informatici, considerata la necessità ed urgenza di adottare e realizzare importanti infrastrutture tecnologiche, la direttiva dell'Unione europea (UE) 2016/1148, nota come Direttiva NIS, recepita in Italia con il decreto legislativo n. 65 del 2018, ha introdotto disposizioni volte a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi nell'Unione Europea. L'obiettivo della Direttiva è quello di definire un'unica linea strategica tra i vari Stati dell'Unione europea, per fronteggiare il rischio di incidenti ai danni delle reti informatiche e dei sistemi informativi, attuando delle strategie al fine di assicurare la gestione dei rischi informatici e la protezione contro i cyber attacchi, recando misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

Considerato come il dominio cibernetico costituisca un terreno di confronto con riflessi sulla sicurezza nazionale è necessario un coordinamento tra le varie regioni al fine di rendere il Paese più sicuro e resiliente anche nel dominio digitale.

Considerata la necessità e l'urgenza di tale tematica, la Regione Marche ha inserito tra gli obiettivi degli anni 2023-2024 per tutte le Aziende Sanitarie Territoriali, due obiettivi, rispettivamente indicati con 29N e 30N, relativi all'implementazione/definizione di un'organizzazione per ogni Azienda, che si occupi della gestione della cybersicurezza del sistema informatico/informativo aziendale e che sviluppi un iniziale assesment dei principali servizi/sistemi utilizzati da ogni Azienda sanitaria e che lavori in sinergia con la Regione Marche.

In particolare, l'obiettivo 29N: "Assesment della Cybersicurezza con definizione del catalogo servizi", richiede la percentuale di servizi e relativi processi interessati dall'assesment sul totale, mentre il 30N: "Definizione di una organizzazione per la Cybersicurezza dei servizi a catalogo" per cui si richiede la "Presenza di un'organizzazione di responsabili per la cybersicurezza di servizi e relativi processi".

Tale obiettivi sono di particolare importanza per la sicurezza dei dati informatici aziendali e per la continuità dei servizi informatici aziendali.

In data 15/11/2023 il Settore Transizione Digitale e Informatica della Regione Marche ha organizzato una call con le Aziende Sanitarie Territoriali al fine d'illustrare gli obiettivi regionali dati e per comunicare l'intero progetto della cybersicurezza regionale, della quale ogni Azienda sanitaria dovrà costituire una parte.

La Dirigente del Servizio ha evidenziato l'estrema necessità di definire un gruppo di tecnici responsabili della cybersicurezza per ogni Azienda Territoriale, che in un lavoro congiunto e di sinergia con i responsabili della cybersicurezza regionale dovranno implementare una rete regionale, al fine di lavorare in collaborazione e in parallelo, in modo tale da poter agire tempestivamente in caso di attacchi informatici ed arginare la situazione di pericolo.

I gruppi tecnici, svolgendo un ruolo di importanza rilevante, è opportuno che siano formati adeguatamente, e a tal d'uopo la Regione Marche ha attivato con l'Università Politecnica delle Marche, UNIVPM, e l'Università degli Studi Di Camerino, UNICAM, delle convenzioni per l'erogazione di corsi formativi specifici.

In coerenza con il riordino del SSR di cui alla LR. 19/2022 ed in considerazione delle sopravvenute esigenze riorganizzative regionale/aziendali, la neocostituita Azienda Sanitaria

Territoriale di Fermo non ha un sistema informatico/informativo autonomo, infatti, alcune parti del sistema informativo aziendale (data center regionale dedicato agli applicativi delle aziende sanitarie utilizzati, navigazione verso internet, gestione firewall, antivirus aziendali ,Active directory,...) sono gestiti centralmente con gestione provvisoria in capo all'AST AN (contratti unici ex ASUR), e dalla Regione Marche.

Quindi, una volta definito il gruppo di tecnici per la cybersicurezza nell'AST di Fermo, esso avrà un range di azione limitata per quanto riguarda le azioni di intervento all'ambito locale, in virtù di quanto sopra evidenziato.

Altro aspetto di fondamentale importanza sono le risorse finanziarie per acquistare ed implementare strumenti di sicurezza, che offrono una maggiore resilienza del sistema informatico, nei confronti degli attacchi cibernetici.

In considerazione di quanto stabilito dalla Regione Marche, per definire un team di responsabili per la cybersicurezza, l'UOC SIA dell'AST di FM può attualmente utilizzare n.4 tecnici informatici, cat. D e C, che effettuano, oltre alle normali attività tecniche di manutenzione/gestione del sistema informatico/informativo aziendale, anche un servizio di reperibilità H24/7 per emergenze relative alla continuità del sistema informativo aziendale.

Tali tecnici, attualmente in carico all'UOC SIA che effettuano la reperibilità, sono:

- Ing. Jr. Roberto Rogante: collaboratore informatico cat. D (con posizione organizzativa);
- Ing. Demis Corazza: collaboratore informatico cat. D;
- P.ind. Paolo Silenzi: programmatore informatico cat. C;
- P.inf. Leonardo Caciorgna: programmatore informatico cat. C.

Per quanto sopra esposto e motivato,

SI PROPONE

che il Direttore Generale dell'AST di Fermo determini:

- 1) di nominare, in riferimento all'obiettivo 30N per l'anno 2023 indicato dalla Regione Marche, "Definizione di una organizzazione per la Cybersicurezza dei servizi a catalogo", quali

responsabili del gruppo operativo dei tecnici informatici per la cybersicurezza aziendale i seguenti tecnici informatici attualmente in carico all'UOC SIA che effettuano la reperibilità H 24/7:

- Ing. Jr. Roberto Rogante: collaboratore informatico cat. D (con posizione organizzativa), con funzione di coordinamento del gruppo della cybersicurezza aziendale;
- Ing. Demis Corazza: collaboratore informatico cat. D;
- P.ind. Paolo Silenzi: programmatore informatico cat. C;
- P.inf. Leonardo Caciorgna: programmatore informatico cat. C;

i quali dovranno gestire tale attività aziendale in stretta collaborazione con la struttura della cybersicurezza regionale, presente nel Settore Transizione Digitale e Informatica della Regione Marche, nei limiti della responsabilità contrattuale propria dell'inquadramento contrattuale di ogni dipendente;

2) di definire, come anche indicato dalla Dirigente del Settore Transizione Digitale e Informatica della Regione Marche, per quanto possibile, all'interno del team di lavoro per la cybersicurezza, anche un'articolazione in riferimento alle diverse principali tematiche informatiche/informative aziendali, come di seguito indicato:

- Ing. jr Roberto Rogante: rete dati, data center e cluster server aziendale, sito extranet/intranet e posta aziendale;
- Ing. Demis Corazza: rete dati, data center e cluster server aziendale;
- P. ind. Paolo Silenzi: sito extranet/intranet e posta aziendale;
- P.inf. Leonardo Caciorgna: data center e cluster server aziendale

3) di definire che il gruppo operativo, ed in particolare, il coordinatore del gruppo, sarà l'interfaccia diretta nella gestione operativa della cybersicurezza aziendale dell'AST di Fermo, in situazioni di normalità e d'urgenza, del gruppo della cybersicurezza regionale;

4) di definire che la responsabilità organizzativa e di programmazione della cybersicurezza dell'AST di Fermo, risulta in capo al Direttore dell'UOC SIA;

5) di attestare che dalla presente determina non deriva alcun onere di spesa a carico del Bilancio dell'AST di Fermo;

- 6) di richiedere al Settore Transizione Digitale e Informatica della Regione Marche la partecipazione del gruppo della cybersicurezza ai corsi di formazione specifici convenzionati con le Università e gli enti di competenza;
- 7) di trasmettere il presente atto al Settore Transizione Digitale e Informatica della Regione Marche e ai componenti del gruppo della cybersicurezza nominati nella presente determina;
- 8) di trasmettere il presente atto al Collegio Sindacale a norma dell'art. 28 della L.R. 19 del 08.08.2022 e s.m.i.;
- 9) di dichiarare che il presente atto è efficace dal giorno di pubblicazione nell'albo pretorio informatico dell'AST di Fermo, ai sensi del comma 8 dell'art.39 della L.R. n.19/2022;

:

**Il Direttore dell'UOC SIA-RTD
Ing. Stefano Intorbida**

- ALLEGATI -

Nessun allegato