CONSORZIO UNIVERSITARIO PICENO

CONSORZIO UNIVERSITARIO PICENO

RELAZIONE SULLA PERFORMANCE ANNO 2019
(art. 10 c.1 lett. b D. Lgs. 150/2009)

RISULTATI OBIETTIVI: arch. Alessandra Bovara, Responsabile Area Amministrativo-Istituzionale, titolare di Posizione Organizzativa (a partire dall'8/05/2019)

L'Arch. Alessandra Bovara, Responsabile Area Amministrativo-Istituzionale del C.U.P., titolare di Posizione Organizzativa (a partire dall'8/05/2019),

PREMESSO che:

- con deliberazione del Consiglio di Amministrazione n. 10 del 2 febbraio 2019 è stato approvato il Piano obiettivi, Piano Esecutivo di Gestione e ciclo della performance del Consorzio Universitario Piceno - Esercizi finanziari 2019-2021 così come da proposta del Direttore, contenente gli obbiettivi affidati al Direttore medesimo per il primo quadrimestre 2019 e ai titolari di Posizione Organizzativa per il restante periodo;
- con la deliberazione di cui sopra sono state attribuite al Direttore e ai Responsabili di Area le necessarie risorse umane e finanziarie per il raggiungimento degli obiettivi consortili definiti dal C.d.A. per l'anno 2019 in stretto raccordo con gli obiettivi strategici riportati nel Documento Unico di programmazione 2019-2021;
- il Direttore successivamente, con proprio provvedimento, ha affidato gli obiettivi ai Responsabili di area e dei servizi dell'Ente;

REDIGE, di seguito, la RELAZIONE SULLA PERFORMANCE ANNO 2019.

La struttura della presente relazione riproduce un'analisi dei risultati conseguiti mediante un esame degli obiettivi, tenendo conto che per l'anno 2019 gli obiettivi sono non solo quelli individuali assegnati con il PEG per il periodo maggio-dicembre 2019 ma anche quelli assegnati dal Direttore dell'Ente ai responsabili di Area e di Servizio (obiettivi di struttura).
Si fa rilevare, inoltre, che come Responsabile di Area sono state implementate o completate alcune attività assegnate con il PEG al Direttore per il primo quadrimestre 2019 e che a far data dal 19 luglio 2019 al Responsabile dell'Area Amministrativo-Istituzionale è stato conferito anche il ruolo di Responsabile anticorruzione dell'Ente.

A. OBIETTIVI INDIVIDUALI 2019 assegnati con PEG. (periodo 8/05/2019 – 31/12/2019). PESO 100%

MACRO OBIETTIVO ANNUALE (1): definizione dell'offerta formativa del sistema universitario relativamente all'offerta formativa dell'Anno Accademico 2019/2020 del Piceno (analisi e approvazione). **Peso 10%**

Risultato raggiunto (punti 10/100)
Il presente obiettivo rappresenta il c.d. "core business" del Consorzio Universitario Piceno in relazione alle attività di gestione e programmazione delle attività universitarie relativamente all'esercizio 2019 e relativamente all'A.A. 2019/2020.
I tavoli di lavoro permanenti sono stati convocati e sono stati redatti i relativi verbali. L'offerta formativa è stata analizzata dal Consiglio di Amministrazione.

ATTIVITA' ANNUALE: analisi dell'offerta formativa A.A. 2019/2020 da parte del Consiglio di Amministrazione del CUP sulla base degli atti definiti in sede di T.L.P..

Processo:

- in data 18 ottobre 2019 è stato approvato dal Consiglio di Amministrazione il verbale del Comitato Paritetico tra UNIVPM e CUP con atto deliberativo n. 42.
- in data 6 dicembre 2019 è stato approvato dal Consiglio di Amministrazione il verbale del Comitato Misto tra UNICAM e CUP con atto deliberativo n. 53.

MACRO OBIETTIVO ANNUALE (2): studio delle performance quantitative e qualitative del sistema universitario del Piceno. **Peso 90%**

Risultato raggiunto (punti 90/100)

Al fine di ottenere risultati riguardo la modalità di percezione dell'università nell'area del Piceno e dare valutazioni ai soci del C.U.P. circa l'opportunità di procedere con il progetto di rilancio di un sistema universitario unico del territorio, è stato promosso uno studio complessivo che ha analizzato le performance quantitative e qualitative del sistema universitario del Piceno e ne ha delineato lo stato dell'arte in termini di percepito. Per la realizzazione dello studio (da parte di uno spin off universitario) è stata necessario effettuare attività di ricerca di documenti e informazioni anche presso enti consorziati che sono confluiti in uno specifico ulteriore documento sull'Università del Piceno, contenente anche gli investimenti da parte del territorio, a partire dalla fondazione del C.U.P. nel 1976. Lo studio sulle performance è stato diffuso con i canali istituzionali e all'interno del convegno organizzato per la presentazione del documento di fine mandato del Consiglio di Amministrazione, per il quale è stato realizzato un apposito documento contenente le prospettive di sviluppo del sistema universitario.

ATTIVITA' ANNUALE: promozione e divulgazione dei risultati dello studio complessivo che analizzi le performance quantitative e qualitative del sistema universitario del Piceno.

Processo:

- raccolta documentazione e informazioni anche presso enti consorziati necessari alla realizzazione dello studio sulle performance e realizzazione del documento specifico sull'Università del Piceno in termini di investimenti da parte del territorio. Documento realizzato nel rispetto dei tempi pervisti. Messa a disposizione di copie da distribuire durante riunioni o convegni di rilievo.
- diffusione dello studio sulle performance quantitative e qualitative del sistema universitario (realizzato dallo spin-off universitario) attraverso la realizzazione del documento *Dalla relazione di fine mandato 2013-2018 alle prospettive di sviluppo del sistema universitario del Piceno,* che ha implementato al suo interno lo studio sulle performance, e all'interno del convegno di presentazione del rapporto di fine mandato 2013-2018 del Consiglio di Amministrazione dell'Ente, nel rispetto dei tempi previsti.
- diffusione dei risultati dello studio attraverso i canali istituzionali (sito web, etc.).

B. OBIETTIVI DI STRUTTURA

B1. ATTIVITA' assegnate al Direttore per il primo quadrimestre 2019.

MACRO OBIETTIVO (1): Definizione dell'offerta formativa del sistema universitario relativamente all'offerta formativa dell'Anno Accademico 2019/2020 del Piceno (programmazione offerta formativa e definizione aspetti economici).

ATTIVITA': Università degli studi di Macerata. Definizione dei rapporti economici in essere.
I rapporti economici in essere con UNIMC non sono stati definiti nei tempi previsti (30.04.2019) per inerzia da parte dell'Università di Macerata, nonostante i solleciti.

Processo:

- il Consiglio di Amministrazione con delibera n. 27 del 19.07.2019 "Rapporti economici CUP/UNIMC" richiamata la nota n. 17386 del 4.06.2019 pervenuta dall'Università di Macerata e i precedenti scambi tra le parti, ha approvato di avviare azione legale nei confronti di UNIMC per il recupero del credito vantato dal CUP, dando mandato al Responsabile del Servizio Finanziario di affidare l'incarico ad un avvocato di fiducia, previa acquisizione di preventivi di spesa da parte di una pluralità di professionisti;
- Successivamente, ai fini dell'affidamento in argomento, il Presidente del Consiglio di Amministrazione ha proposto l'approvazione di un regolamento per la formazione di un elenco di Avvocati del Libero Foro per il conferimento di incarichi di rappresentanza e difesa in giudizio in favore dell'Ente, ai sensi degli artt. 4 e 17, c.1, lett. d) del D. Lgs. 50/2016 e ss.mm.ii., presentato al Consiglio di Amministrazione in data 31.01.2020 e approvato con delibera n. 3.
  Il Regolamento è in attesa di approvazione da parte dell'Assemblea dell'Ente in una prossima seduta.

MACRO OBIETTIVO (2): implementazione ricerca fonti di finanziamento locale ed internazionale.

ATTIVITA': espletamento selezione di personale da dedicare a ricerca fondi e progetti strategici.
Relativamente alla selezione di personale da dedicare a ricerca fondi e progetti, le procedure sono state avviate con determinazione dirigenziale n. 12 del 26.02.2019, mentre la selezione è stata espletata successivamente al periodo previsto per necessità di modificare il Regolamento dei Servizi dell'Ente.

Processo:

- Con determina n. 46 del 26.07.2019 è stata nominata la commissione esaminatrice, sono stati ammessi ii candidati ed è stata stabilità la data della prova selettiva (è stato svolto il ruolo Presidente di commissione);
- Con determina n. 48 del 31 luglio 2019 è stato affidato il servizio di n. 4 esperti linguistici per l'accertamento della conoscenza delle lingue straniere previste dal bando;
- Con determina n. 56 del 7 ottobre 2019 sono stati approvati i verbali e la graduatoria finale e si è stabilito di procedere con l'assunzione del vincitore.
- Con comunicazione del 9 ottobre 2019 è stata comunicata l'assunzione a decorrere dal 18 novembre 2019;
- È stato predisposto il contratto di lavoro tra il C.U.P. e il vincitore della selezione firmato tra le parti in data 17 ottobre 2019.

B2. ATTIVITÀ ANTICORRUZIONE E TRASPARENZA.
(Responsabile anticorruzione e trasparenza dal 19 luglio 2019, inizialmente non previsto con il PEG 2019-2021).

CONSORZIO UNIVERSITARIO PICENO

1. Aggiornamento del Piano Triennale di Prevenzione della Corruzione e della trasparenza 2019/2021.

Processo:

- il Piano Triennale per la Prevenzione della Corruzione e per la Trasparenza 2019-2021 adottato in precedenza dal CdA viene pubblicato dall'11 al 26 giugno 2019 allo scopo di raccogliere suggerimenti ed osservazioni che consentano di addivenire ad un documento definitivo condiviso con chiunque intenda fornire suggerimenti ed osservazioni.
- Il Consiglio di Amministrazione con delibera n. 32 del 19 luglio 2019 approva il Piano triennale di prevenzione della corruzione e per la trasparenza 2019 – 2021 redatto dal Responsabile per la Prevenzione della Corruzione e per la Trasparenza Dr. Pierluigi Raimondi, e delibera:
    - di modificare il Regolamento dei servizi dell'ente, art. 22, laddove prevede che "Al Segretario è attribuito il ruolo di Responsabile per la prevenzione della corruzione e per la trasparenza".
    - di nominare quale nuovo Responsabile per la prevenzione della corruzione e per la trasparenza, l'Arch. Alessandra Bovara, Responsabile dell'Area amministrativo-istituzionale;
    - di pubblicare il Piano sul sito istituzionale dell'Ente aggiornato con il nome del nuovo RPCT.
- In data 19.12.2020 viene effettuato il monitoraggio sulle misure previste dal piano.

2. Assolvimento degli obblighi di pubblicazione ai sensi della Legge 190/2012 e smi. e implementazione del nuovo sito istituzionale dell'ente.

Dal monitoraggio effettuato in data 31/12/2019 si evince che sono state pubblicate sostanzialmente tutte le informazioni disponibili relative all'anno 2019. I dati mancanti si riferiscono a documentazione non prodotta o non presente presso l'Ente.

Processo:

- In data 31/07/2019 è stato effettuato dal Responsabile del Servizio Università, Orientamento, Comunicazione ed elaborazione dati il monitoraggio relativo alla pubblicazione dei dati sul sito istituzionale-area amministrazione trasparente (ns. prot. n. 728 del 31/07/2019);
- In data 31/12/2019 è stato effettuato dal Responsabile del Servizio Università, Orientamento, Comunicazione ed elaborazione dati il monitoraggio relativo alla pubblicazione dei dati sul sito istituzionale-area amministrazione trasparente (ns. prot. n. 19 del 7/01/2020).

B3. OBIETTIVI AREA AMMINISTRATIVO – ISTITUZIONALE AFFIDATI DAL DIRETTORE CON DETERMINA N. 15 DEL 28 FEBBRAIO 2019

Obiettivi Unità di Staff – Segreteria Generale. Il Responsabile dell'Area Amministrativo-Istituzionale ad interim è anche Responsabile della Segreteria Generale.

MACROPROGETTO: attività di segreteria (struttura di riferimento).
Obiettivo che contribuisce direttamente alla realizzazione degli obiettivi del Direttore/Resp. di Area PEG 2019.

Azione (1): supporto alla Direzione/Resp. di Area per la gestione dei rapporti con CDA e Assemblea.

Azione (2): predisposizione delle deliberazioni adottate dal Consiglio di Amministrazione e dall'Assemblea, in collaborazione con Servizio Finanziario per quelle relative al servizio finanziario.

Azione (3): smistamento della posta in entrata.

Azione (4): supporto alla Direzione/Resp. di Area per la gestione dei rapporti con le Università di riferimento del Consorzio.

Azione (5): supporto alla Direzione/Resp. di Area nella predisposizione delle proposte del Consiglio di Amministrazione.

Indicatori azione (1):
- predisposizione convocazioni e ordini del giorno;
- predisposizione in bozza di tutti i verbali delle sedute di Assemblea e di Consiglio di Amministrazione;

Indicatore azione (2): predisposizione in bozza di tutte le deliberazioni adottate dal Consiglio e dall'Assemblea, in collaborazione con Servizio Finanziario.

Indicatore azione (3): assegnazione posta in entrata Presidente, Direttore, Aree e Servizi.

Indicatori azione (4): predisposizione convocazioni, ordini del giorno e atti relativi ai rapporti con le università di rifermento;

Indicatore azione (5): predisposizione in bozza su indicazione della Direzione di proposte da sottoporre al Consiglio di Amministrazione e all'Assemblea dei soci.

Peso: 20% degli obiettivi strategici.

(1) Sono state predisposti gli ordini del giorno e inviate tutte le convocazioni relative alle adunanze anno 2019.
Sono stati predisposti in bozza tutti i verbali delle n. 4 sedute dell'Assemblea e delle n. 6 sedute del Consiglio di Amministrazione dell'anno 2019.
Sono stati convocati, in base alle convenzioni vigenti, i TLP ed è stato seguito l'iter che ha portato all'approvazione dei verbali dei TLP da parte del Consiglio di Amministrazione entro l'anno.

(2) Sono state predisposte tutte le deliberazioni dell'Assemblea e del Consiglio di Amministrazione anno 2019, in collaborazione con il Servizio Finanziario e il Sevizio Università, Orientamento, Comunicazione ed elaborazione dati per quelle attinenti i servizi stessi.

(3) E' stata regolarmente vistata e smistata la posta in arrivo.

(4) In merito all'Università di Camerino e all'Università Politecnica delle Marche sono stati predisposti in bozza i verbali delle sedute dei Comitati oltre lettere, convocazioni e tutto quanto richiesto dal Presidente o dal Direttore.

(5) Sono state predisposte su indicazione del Direttore le proposte di deliberazione da sottoporre al Consiglio di Amministrazione e all'Assemblea dei soci. Da maggio 2019 le proposte sono presentate in qualità di Responsabile di Area.

Inoltre, sono state regolarmente predisposte tutte le determine affidate alla Segreteria Generale dalla Direzione nel primo quadrimestre 2019. Successivamente le determine sono state adottate come Responsabile di Area.

MACROPROGETTO: supporto gestione del personale.

Azione (1): supporto alla Direzione/Resp. di Area per le attività di coordinamento delle attività del Consorzio e del personale coinvolto.

Azione (2): supporto alla Direzione/Resp. di Area per la predisposizione dei bandi relativi alla selezione del personale o dei collaboratori.

Azione (3): supporto alla Direzione/Resp. di Area per le attività dell'Ufficio Procedimenti Disciplinari.

Indicatore azione (1): predisposizione convocazioni e partecipazione alle riunioni convocate dalla Direzione/Resp. di Area per organizzazione attività.

Indicatore azione (2): predisposizione bandi resisi necessari nel corso dell'anno relativi alla selezione del personale o dei collaboratori.

Indicatore azione (3): verbalizzazione incontri resisi necessari nel corso dell'anno.

Peso: 30% degli obiettivi strategici.

(1) Sono state predisposizione le convocazioni e indette le riunioni richieste dalla Direzione per organizzazione attività e comunicazioni al personale nel primo quadrimestre.

(2) Sono state predisposte le determine relative alla selezione di personale e il relativo bando.

(3) E' stata supporta la Direzione nelle attività dell'UPD, sono stati redatti in bozza convocazioni, verbali, atti relativi. Dall'8 maggio 2019 come Responsabile di Area Amministrativo-Istituzionale viene ricoperto anche il ruolo di Presidente dell'UPD.

Inoltre, sono stati predisposti il Piano triennale di fabbisogno di personale, la relazione e il monitoraggio della performance.
E' stato supportato il Servizio Finanziario relativamente al Conto annuale del personale anno 2018.

MACROPROGETTO: supporto gestione rapporti con Organizzazioni sindacali e attività connesse al nuovo CCNL (struttura di riferimento).

Azione (1): supporto alla Direzione/Resp. di Area per le trattative con le organizzazioni sindacali.

Azione (2): supporto alla Direzione/Resp. di Area per la determinazione e gestione dei fondi di contrattazione decentrata integrativa, in collaborazione con Servizio Finanziario.

Indicatore azione (1): predisposizione di tutti i verbali sindacali relativi alle sedute che vengono svolte nel corso dell'esercizio.

Indicatore azione (2): predisposizione delle Relazioni Illustrativa e Tecnico-finanziaria relative ai fondi per la contrattazione decentrata integrativa, in collaborazione con il Servizio Finanziario.

Peso: 10% degli obiettivi strategici.

(1) Sono stati predisposti in bozza i verbali degli incontri con le OO.SS. e il CCI 2016-2018 dell'Ente.
(2) Sono state predisposte, con il Servizio finanziario, le relazioni illustrative e tecnico finanziarie relative alla costituzione dei fondi dirigente e dipendenti anno 2018, da sottoporre all'Organo di Revisione dell'Ente.

Inoltre, è stata predisposta, con il Servizio Finanziario, la determina del Direttore per la costituzione dei fondi per la contrattazione integrativa decentrata anno 2019 dipendenti e dirigente.

Come Presidente della delegazione trattante di parte pubblica è stato definito l'accordo per la contrattazione del salario accessorio dei dipendenti anno 2019.

MACROPROGETTO: Anticorruzione e trasparenza (struttura di riferimento).
Obiettivo che contribuisce direttamente alla realizzazione degli obiettivi del Direttore/Resp. anticorruzione PEG 2019.

Azione (1): Supporto al Responsabile anticorruzione e per la Trasparenza nella redazione del Piano Triennale di Prevenzione della Corruzione e per la Trasparenza 2019/2021.

Azione (2): Collaborazione con il Responsabile del Servizio Università, Orientamento, Comunicazione ed Elaborazione Dati all'individuazione dei singoli dati da mettere in pubblicazione e trasmissione di quelli attinenti la Segreteria Generale (trasmissione ascrivibile a personale di supporto).

Azione (3): supporto alla Direzione/Resp. di Area/Presidente CdA per i rapporti con l'Organismo di Valutazione.

Indicatore azione (1): collaborazione con il Responsabile anticorruzione alla predisposizione del Piano Triennale di Prevenzione della Corruzione 2019/2021.

Indicatore azione (2): Trasmissione dati individuati attinenti la Segreteria Generale al Servizio Università, Orientamento, Comunicazione ed Elaborazione Dati.

Indicatori azione (3): trasmissione all'OV degli atti che necessitano della sua valutazione.

Peso: 25% degli obiettivi strategici.

(1) E' stato supportato il Responsabile anticorruzione nell'elaborazione del Piano Triennale di Prevenzione della Corruzione e per la trasparenza 2019/2021.

(2) Sono stati individuati con il Responsabile del Servizio Università, Orientamento, Comunicazione ed Elaborazione Dati i singoli dati per la pubblicazione in *Amministrazione trasparente* e sono stati regolarmente trasmessi i dati attinenti la Segreteria generale.

(3) Sono stati trasmessi all'OV gli atti necessari che necessitano di una sua valutazione.

MACROPROGETTO: controlli interni.

Azione (1): supporto al Direttore/Segretario dell'Ente per le procedure relative al controllo successivo di regolarità amministrativa.

Indicatore azione (1): svolgimento sessioni di controllo quadrimestrale secondo le indicazioni del Direttore/Segretario.

Peso: 10% degli obiettivi strategici.

E' stato supportato il Segretario dell'Ente nello volgimento di 3 sessioni di controlli interni.

MACROPROGETTO: adempimenti Legge 190/2012 art. 1, comma 32
Obiettivo che contribuisce direttamente alla realizzazione degli obiettivi del Direttore/Resp. di Area PEG 2019.

Azione (1): predisposizione file riassuntivo CIG.

Indicatore azione (1): predisposizione file riassuntivo CIG entro 31.12.2019 (compilazione ascrivibile personale di supporto).

Target: avvenuta pubblicazione sul sito istituzionale del file xml entro i termini disposti dalla normativa.

Peso: 5% degli obiettivi strategici.

E' stato predisposto il file riassuntivo CIG entro 31.12.2019. La pubblicazione sul sito istituzionale del file xml è avvenuta a gennaio 2020 entro i termini disposti dalla normativa.

In qualità di datore di lavoro sono stati affidati i servizi relativi al medico competente e al Responsabile del Servizio di Prevenzione e Protezione, è stato organizzato un corso sulla sicurezza per tutti i dipendenti, e corsi specifici per gli addetti antincendio e per il Responsabile dei Lavoratori per la Sicurezza.

Sono stati coadiuvati il Presidente del Consiglio di Amministrazione e il Responsabile per la protezione dei dati per gli adempimenti connessi alla *privacy.*

Con riguardo agli **obiettivi affidati per l'anno 2019 dal Direttore agli altri Responsabili di servizio dell'Area amministrativo – Istituzionale**, la struttura ha complessivamente raggiunto tutti gli obiettivi assegnati.

Afferiscono all'Area Amministrativo-Istituzionale i Servizi indicati nella tabella seguente.

CONSORZIO UNIVERSITARIO PICENO

Organizzazione dell'Area Amministrativo-Istituzionale:

Ufficio	**Cognome e Nome**	**Tempo**	**Giur**	**Econ**	**Profilo Professionale**	**Tot. R.U.**
Responsabile AREA AMMINISTRATIVO-ISTITUZIONALE	Arch. Bovara A.	T.I.	D1	D2	Istruttore direttivo P.O.	4
Segreteria generale	ad interim Arch. Bovara A.					
Servizio Finanziario	-	T.P.D 33,33%	D1	D4	Istruttore direttivo	
Servizio Univ. Orient. Comunic. Elabor. dati	-	T.P.I. 83,33%	D1	D1	Istruttore direttivo	
Servizio ricerca fondi e progetti strategici	-	T.D. (da nov. 2019)	D1	D1	Istruttore direttivo	

PERSONALE DI SUPPORTO ALLE AREE dell'ente	-	T.I.	C1	C2	Istruttore amministrativo	4
	-	T.P.I. 83,33%	B1	B3	Addetta area amministr.	
	-	T.P.I. 69,44%	B1	B1	Addetta area istituzionale	
	-	T.I.	B3	B5	Guardia giurata non armata	

Tutta la documentazione relativa alle attività svolte è a disposizione presso la Segreteria Generale del Consorzio Universitario Piceno.

Il Responsabile di Area Amministrativo-Istituzionale
F.to Arch. Alessandra Bovara

CONSORZIO UNIVERSITARIO PICENO

CONSORZIO UNIVERSITARIO PICENO

RELAZIONE SULLA PERFORMANCE ANNO 2019
(art. 10 c.1 lett. b D. Lgs. 150/2009)

RISULTATI OBIETTIVI: Ing. Loris Pierbattista, Responsabile Area Acquisti Telematici, Appalti e Contratti part time 12 ore

L'ing. Loris Pierbattista, Responsabile Area Acquisti Telematici, Appalti e Contratti del C.U.P.

PREMESSO che:
- con deliberazione del Consiglio di Amministrazione n. 10 del 2 febbraio 2019 è stato approvato il Piano obiettivi, Piano Esecutivo di Gestione e ciclo della performance del Consorzio Universitario Piceno - Esercizi finanziari 2019-2021 così come da proposta del Direttore, contenente gli obiettivi affidati al Direttore medesimo per il primo quadrimestre 2019 (successivamente il direttore, con proprio provvedimento, ha affidato gli obiettivi ai Responsabili di area e dei servizi dell'Ente) e ai titolari di Posizione Organizzativa per il restante periodo.
- nello stesso tempo, sono state attribuite al Direttore e ai Responsabili di Area le necessarie risorse umane e finanziarie per il raggiungimento degli obiettivi consortili definiti dal C.d.A. per l'anno 2019 in stretto raccordo con gli obiettivi strategici riportati nel Documento Unico di programmazione 2019-2021;

REDIGE, di seguito, la RELAZIONE SULLA PERFORMANCE ANNO 2019.

La struttura della presente relazione riproduce un'analisi dei risultati conseguiti mediante un esame degli obiettivi per il periodo sopra indicato, tenendo conto che per l'anno 2019 gli obiettivi sono non solo quelli individuali assegnati con il PEG ma anche quelli in precedenza assegnati dal Direttore dell'Ente ai responsabili di Area e di Servizio (denominati obiettivi di struttura).

A. OBIETTIVI INDIVIDUALI 2019 assegnati con PEG. (periodo 8/05/2019 – 31/12/2019). PESO 100%

MACRO OBIETTIVO ANNUALE (1): transizione al digitale. **Peso 100%**

Breve descrizione dell'obiettivo

Il Codice dell'Amministrazione Digitale è stato di recente ampiamente modificato. il processo di riforma pone in capo ad ogni amministrazione pubblica la funzione di garantire l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione, centralizzando in capo ad un ufficio unico il compito di conduzione del processo di transizione alla modalità operativa digitale ed altresì dei correlati processi di riorganizzazione, nell'ottica di perseguire il generale obiettivo di realizzare un'amministrazione digitale e aperta, dotata di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità.

ATTIVITA' ANNUALE: analisi del contesto e avvio processo.

Target: relazione sullo stato di attuazione della modalità digitale nell'ente e programmazione attività necessarie per il perseguire il generale obiettivo di realizzare un'amministrazione digitale e aperta, dotata di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità. Entro 31.12.2019.

Risultato raggiunto (punti 100/100)

Processo:

Allo scopo di assicurare piena attuazione alla trasformazione digitale dell'Amministrazione, il Consorzio Universitario Piceno (di seguito per brevità denominato anche Consorzio o CUP) ha individuato nell'Area acquisti telematici, appalti e contratti, l'area cui attribuire i compiti per la transizione digitale declinati dal comma 1 dell'art. 17 del Codice dell'Amministrazione Digitale (CAD), adottato con d.lgs. 7 marzo 2005, n. 82 e nel sottoscritto, Ing. Loris Pierbattista, il Responsabile per la transizione al digitale del Consorzio.

Ciò premesso, si descrive lo sviluppo del processo che innegabilmente ha avuto come punto di partenza la verifica dello stato di attuazione della "*modalità digitale*" all'interno dell'Amministrazione e la programmazione delle attività necessarie per garantire una corretta e completa transizione al digitale. Si precisa che tutte le attività sono state svolte in collaborazione con un dipendente part time in somministrazione categoria C1.

Il processo è stato sviluppato sulla base delle linee guida AGID "Misure minime di sicurezza ICT per le pubbliche amministrazioni**"** che indicano le misure minime di sicurezza ICT emanate dall'AgID, e rappresentano un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti.

INVENTARIO DELLE RISORSE INFORMATICHE UTILIZZATE DAL C.U.P.

Come già detto, l'analisi non poteva prescindere da un inventario delle risorse hardware e software utilizzate dal CUP e per raggiungere questo scopo è stato utilizzato uno strumento automatico denominato "*lansweeper",* vale a dire un'applicazione sempre attiva in grado di individuare e monitorare con continuità le risorse che l'Amministrazione effettivamente utilizza.

Questa applicazione permette inoltre di identificare le risorse hardware e software non ancora censite ogni qualvolta fossero collegati in rete dei nuovi dispositivi, registrando la versione del sistema operativo utilizzato, le applicazioni installate ed il cosiddetto livello di patch.

Tutti i sistemi collegati alla rete (ad es.: PC, stampanti, server) e i dispositivi di rete (ad es.: switch e access point) sono stati registrati con il proprio indirizzo IP con indicazione dei nomi e della funzione delle macchine, dell'utilizzatore della risorsa e del servizio/ufficio di appartenenza, specificando inoltre la tipologia di dispositivo se portatile o fisso.

Si segnala inoltre che, con periodicità quotidiana, il "*lansweeper"* unitamente al firewall perimetrale Watchguard t35 installato esegue la discovery dei dispositivi collegati alla rete con segnalazione di allarme nel caso fossero individuate eventuali anomalie.

Si precisa che il firewall è in grado di qualificare tutti i sistemi connessi alla rete attraverso l'analisi del loro traffico dati.

Si è inoltre provveduto a redigere l'elenco dei software autorizzati in uso ai diversi uffici/servizi del CUP e le versioni necessarie per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi realizzando una vera e propria "*White List*" delle applicazioni autorizzate.

Si sottolinea che, come ulteriore sistema di controllo, l'applicazione "*Lansweepper*" verifica l'integrità dei file accertando che le applicazioni nella "*White list*" non siano state modificate; vengono, cioè, eseguite regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzati.

Per uniformarsi alle linee guida AGID sull'accessibilità degli strumenti informatici una maggiore sicurezza si utilizzano macchine virtuali "*Air-Gapped*" ovverosia fisicamente isolate dalla rete dell'Amministrazione e in cui eseguire applicazioni necessarie per operazioni strategiche o critiche, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.

SICUREZZA DELLE CONFIGURAZIONI

Allo scopo di garantire un'adeguata protezione delle configurazioni hardware e software si è deciso di impiegare una configurazione standard per le workstation, i server e gli altri tipi di sistemi usati dall'Amministrazione.

Al fine di assicurare il ripristino dei P.C. nel caso in cui essi dovessero essere compromessi si è proceduto ad installare il software - open source - FOGProject che ne garantisce il *recovery* utilizzando una configurazione standard; il ripristino dei server avviene, se necessario, tramite il restore del sistema di virtualizzazione PVE (Proxmox Virtual Envirement).

Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati; è utile precisare che tutte le operazioni di amministrazione di server, workstation, dispositivi di rete e analoghe apparecchiature possono avvenire da remoto per mezzo di connessioni protette.

Vengono inoltre eseguiti periodici controlli dell'integrità dei file per assicurare che i file critici del sistema non siano stati alterati.

GESTIONE VULNERABILITÀ

Per garantire un'adeguata gestione delle vulnerabilità si è adottato un sistema SIEM (Security Information and Event Management) open-source denominato "*OSSIM*" che in maniera automatica in caso di modifica significativa della configurazione dell'infrastruttura esegue una ricerca delle vulnerabilità su tutti i sistemi in rete e fornisce un report con indicazioni delle vulnerabilità più critiche.

Il SIEM viene regolarmente aggiornato con tutte le più rilevanti vulnerabilità di sicurezza.

Server e client sono in active directory con aggiornamento automatico di antivirus, sistema operativo e software microsoft.

È stato inoltre predisposto un DRP (*Disaster Recovery Plan*) di seguito descritto nel dettaglio.

L'applicazione delle patch viene eseguita in automatico entro 24h dall'informativa su tutti i PC; tuttavia per le patch sul server si prevede un'attesa di 2 o 3 settimane prima dell'installazione per verificare l'efficacia e l'affidabilità delle patch stesse.

GESTIONE UTENZE E PRIVILEGI

Si è fatto in modo che le utenze siano dotate di credenziali forti (Es. per VPN password di 16 caratteri composti da una sequenza di numeri, simboli e lettere maiuscole e minuscole) e vengano sostituite ogni mese con password sempre nuove.

E' stata inoltre creata una distinzione tra utenze privilegiate e non privilegiate ed è garantito che a ciascuna utenza sia riconducibile una ed una sola persona.

PROTEZIONE DAI MALWARE

È installato su tutti i dispositivi connessi alla rete l'antivirus Bitdefender che viene aggiornato automaticamente; viene eseguita, inoltre, una scansione anti-malware dei supporti rimuovibili ogniqualvolta vengano connessi.

Si precisa che Bitdefender ha inoltre la funzione di firewall personale. Tutti gli eventi rilevati sono inviati ad un repository centrale (syslog server) dove sono stabilmente archiviati.

Bitdefender è gestito e controllato da una "console cloud" e pertanto non è consentito agli utenti alterarne la configurazione.

Solo dalla console centrale riservata all'amministratore di sistema è possibile forzare manualmente l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale mentre l'analisi dei potenziali malware è effettuata su infrastruttura cloud.

Si è proceduto inoltre ad installare e configurare un Firewall perimetrale Watchguard t35 che opera sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host; il firewall monitora, analizza ed eventualmente blocca gli accessi a indirizzi che abbiano una "cattiva reputazione", filtra il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, anche con strumenti antispam e filtra anche il contenuto del traffico web.

Sia Bitdefender che il firewall Watchguard t35 utilizzano strumenti anti-malware che sfruttano, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.

COPIE DI SICUREZZA

Massimo una volta a settimana viene effettuata una copia di sicurezza delle informazioni strettamente necessarie per il completo ripristino del sistema.

Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure riguardano il sistema operativo, le applicazioni software e la parte dati e per i server l'intera macchina virtuale.

Vengono inoltre effettuati backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di ripristino.

OBIETTIVI DA REALIZZARE

Dato atto che il Piano Triennale per l'Informatica nella Pubblica Amministrazione detta indirizzi precisi sull'adozione di soluzioni Cloud e SAAS rispetto alle soluzioni "*on premise*" (in sede) obiettivo primario dell'amministrazione è quello di prevedere un piano strutturato in fasi successive da attivare nel 2020 che preveda la migrazione delle procedure gestionali su servizio SAAS e delle copie su spazio backup in cloud "GDPR compliant" su datacenter europei.

Si procederà inoltre al rinnovo del sito web istituzionale adeguandolo agli standard previsti in materia di trasparenza e accessibilità utilizzando dei "*template*" certificati a tale scopo.

DISASTER RECOVERY PLAN DEL CONSORZIO UNIVERSITARIO PICENO

Il piano di *Disaster Recovery* (DRP) fornisce una procedura per recuperare dati e sistemi in caso di calamità, include gli obiettivi di continuità operativa dell'ente, elenca gli strumenti ed i piani che sono stati attuati per far funzionare l'Amministrazione al più presto in caso di un'emergenza "IT" e garantisce l'efficiente passaggio di consegne di informazioni.

Di seguito sono descritti le seguenti informazioni:

1. definizione degli obiettivi;

2. le priorità;

3. la strategia di backup e ripristino di emergenza.

DEFINIZIONI DEGLI OBIETTIVI

RPO Recovery Point Objective

Determina il tempo che intercorre tra l'ultimo backup creato e il momento del disaster.

RTO Recovery Time Objective

Determina il tempo massimo tra il momento del disastro e quando il sistema è completamente ripristinato e avviato.

WRT Working Recovery Time

Definisce quanto tempo impiegherà il responsabile IT per rendere operativi gli utenti dell'ente dopo che il ripristino del sistema e dei dati è stato eseguito.

MTD Maximum Tolerable Downtime

Rappresenta il tempo di arresto totale accettabile tra il momento del disastro e il momento in cui gli utenti possono lavorare di nuovo in modo produttivo.

DEFINIZIONE DELLE PRIORITÀ

Il Datacenter è realizzato su sistema cluster ad alta affidabilità virtualizzato

Le Virtual Machine del CUP contenenti i dati sono quattro:

1. vSRVfs (server File + gestionale);
2. MasterDC (Domain controller);
3. vSRVkerio (server Mail);
4. vSRVweb (server web).

Nella tabella seguente sono stabilite in funzione delle priorità e delle criticità i tempi di RPO, RTO, WRT e MTD stabiliti.

server	criticità	RPO	RTO	WRT	MTD
vSRVfs	molto alta	24h	3h	5min	3h e 5min
MasterDC	alta	4gg	15min	5min	20min
vSRVkerio	alta	12h	2,5h	5min	2h e 35min
vSRVweb	media	4gg	20min	5min	25min

BACKUP AND DISASTER RECOVERY STRATEGY

È stata utilizzata una strategia di backup e Disaster Ricovery che fosse un giusto compromesso tra il budget a disposizione e le priorità sopra descritte.

Sono stati implementati:

1. Backup automatici e frequenti.
2. Backup protetti da password e/o completamente crittografati.
3. Autorizzazioni per limitare l'accesso ai file di backup solo a un numero limitato di persone autorizzate.
4. Monitoraggio di tutte le attività di backup.
5. Metodologie per ripristinare velocemente i file di backup.

É in programma di effettuare copie dei file in posizione esterna su spazio backup in cloud “GDPR compliant” su datacenter europei.

Per ogni VM (macchina virtuale) sono di seguito elencate le azioni intraprese in conformità all'articolo 32 del GDPR:

Virtual server		**Frequenza BACKUP**	**Protezione BACKUP**	**LOCAL BACKUP STORAGE**	**OFFSITE BACKUP**	**BACKUP TESTS**	**MONITORING**	**RECOVERY**
vSRVfs	VM	4gg	vzdump format + NFS solo su IP del server fisico	NAS QNAP	Non attivo	1 anno	mail con report	restore VM
	DATI	24H	formato zip, criptato					restore dati
Master DC	VM	4gg	vzdump format + NFS solo su IP del server fisico	NAS QNAP	Non attivo	1 anno	mail con report	restore VM
vSRVkerio	VM	4gg	vzdump format + NFS solo su IP del server fisico	NAS QNAP	Non attivo	1 anno	mail con report	restore VM
	DB mail	12h	formato zip, criptato					restore db
vSRVweb	VM	4gg	vzdump format + NFS solo su IP del server fisico	NAS QNAP	Non attivo	1 anno	mail con report	restore VM

CONSORZIO UNIVERSITARIO PICENO

1. **GLI OBIETTIVI DI STRUTTURA ASSEGNATI CON DETERMINA N. 15 del 2019 SONO:**

Con riguardo agli obiettivi affidati dal Direttore al Responsabile dell'Area Area Acquisti Telematici, Appalti e Contratti, essi sono stati complessivamente raggiunti.

MACRO PROGETTO: Formazione del personale dipendente del Consorzio, anno 2019
Azione (1): Erogazione al personale dipendente del Consorzio di corsi relativi alle procedure di affidamento di servizi e forniture.
Indicatore azione (1-a): Corso: *Tracciabilità dei flussi finanziari e richiesta CIG.*
Indicatore azione (1-b): Corso: *Ruolo del RUP*.
Indicatore azione (1-c): Corso: *Esempi pratici MePA*.
Indicatore azione (1-d): Corso: *Aggiornamenti del Codice dei contratti pubblici in materia di procedure sotto soglia.*
Peso: 50% degli obiettivi strategici.

Al fine di garantire un'adeguata formazione su tutti i temi richiesti, è stato progettato un percorso formativo articolato in tre moduli al fine di fornire la strumentazione concettuale e normativa essenziale per consolidare le competenze di base nella gestione dei procedimenti di acquisto

1. In particolare i primi due temi, vale a dire «*la tracciabilità dei flussi finanziari e richiesta CIG*» e «*il ruolo del RUP*», viste i molteplici collegamenti sono stati fusi in un unico momento formativo che il sottoscritto ing. Loris Pierbattista ha tenuto il 5 giugno del 2019 e a cui hanno partecipato alcuni fra i dipendenti del C.U.P. e precisamente: la Responsabile dell'Area Amministrativa Istituzionale, la Responsabile del Servizio Università Orientamento Comunicazione ed Elaborazione dati, la Responsabile del Servizio Finanziario unitamente ad un istruttore amministrativo del medesimo servizio.

Sono stati sviluppati i seguenti temi:

- *I concetti fondamentali dei contratti pubblici;*
- *i principi comunitari e nazionali;*
- *il principio di concorrenza: l'obbligo della gara, il suo fondamento e le deroghe consentite;*
- *il principio di economicità e il "danno alla concorrenza" nella giurisprudenza giuscontabile;*
- *il principio di rotazione;*
- *il responsabile del procedimento: profili essenziali.*
- *Linee Guida ANAC n. 3 - Nomina, ruolo e compiti del responsabile unico del procedimento per l'affidamento di appalti e concessioni;*
- *il calcolo del valore dell'appalto: l'importo a base di gara e le "opzioni";*

- *la tracciabilità dei flussi finanziari– Casi particolari rientranti nel perimetro della Tracciabilità;*
- *Sistema informativo Monitoraggio gare di ANAC;*
- *La disciplina dei CIG e degli Smart CIG con particolare riguardo agli acquisti effettuati tramite Consip S.p.A..*

2. Il 24 settembre 2019 il sottoscritto ha tenuto un corso a cui hanno partecipato esclusivamente la Responsabile dell'Area Amministrativa Istituzionale e la Responsabile del Servizio Università Orientamento Comunicazione ed Elaborazione dati avente ad oggetto *Aggiornamenti del Codice dei contratti pubblici a seguito della conversione in legge del D.L. "Sblocca cantieri" con particolare riferimento alle procedure di acquisti per importi inferiori alla soglia di rilievo comunitario.*

   Nel modulo formativo sono state affrontate le novità del Decreto "Sblocca Cantieri", tracciandone il quadro normativo generale, per poi approfondire temi come le procedure sotto soglia, i criteri di aggiudicazione, il subappalto ed altro ancora.

   Sono stati trattati i seguenti temi:

- *Il quadro normativo dopo la Legge di conversione del Decreto "sblocca cantieri";*
- *La sospensione di alcune norme fondamentali del Codice fino al 31 dicembre 2020;*
- *Le procedure sotto-soglia e i criteri di aggiudicazione*
- *La commissione giudicatrice;*
- *La verifica dei requisiti generali e speciali;*
- *Il subappalto;*
- *Le offerte anomale*

3. Infine il 18 dicembre 2019 il sottoscritto ha tenuto un corso relativo agli acquisti tramite gli strumenti telematici del MEPA a cui hanno partecipato alcuni funzionari del Consorzio Universitario Piceno e precisamente*:* la Responsabile dell'Area Amministrativa Istituzionale, la Responsabile del Servizio Università Orientamento Comunicazione ed Elaborazione dati e un istruttore direttivo del Servizio ricerca fondi e progetti strategici.

   Sono stati oggetto di trattazione i seguenti temi:

- Gli strumenti di Consip: Convenzioni Quadro, Accordi Quadro, SDAPA e MEPA.
- *La struttura del MEPA.*
- *Convenzioni Consip e strumenti di acquisto;*
- *Definizione di:*
  - *Ordine diretto di acquisto (ODA);*
  - *Trattativa diretta (TD);*
  - *Richieste di offerte (RdO).*
- *Analisi particolareggiata di categorie di abilitazione MEPA di particolare interesse per il Consorzio.*
- *Gli acquisti di beni e servizi informatici e di connettività.*
- *L'Ordine diretto di acquisto (ODA) e i cataloghi del MEPA:*
  - *la ricerca degli operatori economici;*
  - *la dei beni e dei servizi;*
  - *l'estrazione dei dati;*
  - *l'inserimento a carrello e l'acquisto.*
- *La Trattativa diretta (TD) sul MEPA:*
  - *le procedure utilizzabili;*
  - *la ricerca degli operatori economici;*
  - *contratti a corpo e a misura nell'ambito di una TD;*
  - *documentazione da richiedere;*
  - *i termini della TD.*
- La gestione dell'attività contrattuale ripetitiva: la conclusione di accordi quadro nell'ambito del MEPA.
- *Il sistema dei controlli sui requisiti di partecipazione:*
  - *la verifica a campione da parte dei gestori dei mercati elettronici;*
  - *i principi stabiliti dall'ANAC nelle Linee guida sugli appalti sottosoglia.*
- *Simulazioni operative.*

2. MACRO PROGETTO: Supporto contrattuale agli obiettivi della Direzione/ Area amministrativo-istituzionale.

Azione (1): attività di supporto contrattuale.
Indicatore azione (1): supporto nella predisposizione contratti MePA e determinazioni di affidamento.
Peso: 50% degli obiettivi strategici.

Di seguito viene riportato l'elenco di tutte le iniziative per le quali, nel corso del 2019, il Responsabile dell'Area Acquisti Telematici, Appalti e Contratti del C.U.P. ha garantito il proprio Supporto alla Direzione del CUP e all'Area Amministrativa Istituzionale nella predisposizione dei contratti e delle determinazioni di affidamento.

Supporto alla Direzione del CUP nella predisposizione dei seguenti T.D. nell'ambito del MePA

#		Codice	Nome	Stato	Data stato	Bando/Categoria
1	○	890681	Affidamento per tre mesi del servizio di pulizia ordinaria dei locali della Facoltà di Economia "G. Fuà" sede di S. Benedetto del Tronto	Stipulata	18/04/2019	SERVIZI
2	○	888433	Affidamento per tre mesi del servizio di pulizia ordinaria dei locali della Facoltà di Economia "G. Fuà" sede di S. Benedetto del Tronto	Deserta	15/04/2019	SERVIZI
3	○	862626	Richiesta di preventivo propedeutica all'affidamento diretto ai sensi dell'art. 36 comma 2 lettera a) del D.Lgs. 50/2016 e s.m.i. a favore del Consorzio Universitario Piceno del servizio professionali fiscali e tributari.	Stipulata	29/03/2019	SERVIZI
4	○	862612	Richiesta di preventivo propedeutica all'affidamento diretto ai sensi dell'art. 36 comma 2 lettera a) del D.Lgs. 50/2016 e s.m.i. a favore del Consorzio Universitario Piceno di servizi professionali di consulenza del lavoro per l'anno 2019.	Stipulata	29/03/2019	SERVIZI

Supporto alla Direzione del CUP nella predisposizione delle seguenti R.d.O. nell'ambito del MePA

Supporto alla Direzione del CUP nella predisposizione dei seguenti O.D.A nell'ambito del MePA

N. OdA	Comunicazione da leggere	Autore	Descrizione	Data Stato	Strumento
4749813		APUNI0009	Affidamento per la durata di 2 mesi del servizio di assistenza tecnica informatica a favore del CUP	27/05/2019	Mercato Elettronico
4877206		APUNI0009	Adesione alla piattaforma di invio massivo mail per una durata di 24 mesi a far data dalla sottoscrizione dell'ODA	29/04/2019	Mercato Elettronico
4849355		APUNI0009	Acquisizione del canone annuale di licenza d'uso update Kerio Connect Mail Server. Periodo 31.03.2019-30.03-2020	20/03/2019	Mercato Elettronico
4761346		APUNI0009	Affidamento del servizio di connettività della sede consortile anno 2019	05/02/2019	Mercato Elettronico

Supporto alla Direzione del CUP nella predisposizione dei seguenti O.D.A nell'ambito delle Convenzioni Consip

N. OdA	Comunicazione da leggere	Autore	Descrizione	Fornitore	Totale (IVA incl.)	Stato	Data Stato
4885962		APUNI0009	Migrazione da Convenzione Telefonia Mobile 6 a telefonia Mobile 7 e ordine telefoni	TELECOM ITALIA S.P.A.	N.A.	Evaso dal Fornitore	17/05/2019
4876920		APUNI0009	Affidamento del servizio sostitutivo di mensa mediante buoni pasto cartacei non nominativi per un anno a seguito di adesione alla Convenzione Consip Buoni Pasto n. 8 - lotto 8	REPAS LUNCH COUPON	2.052,96	Accettato dal Fornitore	05/04/2019
4872429		APUNI0009	Fornitura annuale di energia elettrica per la sede del Consorzio Universitario Piceno	A2A ENERGIA SPA	N.A.	Accettato dal Fornitore	02/04/2019

CONSORZIO UNIVERSITARIO PICENO

Supporto alla Responsabile dell'Area Amministrativa Istituzionale nella predisposizione delle seguenti RdO

IDT	Nome	Lotto	Stato	Data pubblicazione	Data aggiudicazione	Data stipula
2470414	Richiesta esplorativa di preventivi propedeutica all'affidamento diretto ai sensi dell'art. 36, co. 2, lett. a) del D.Lgs. 50/2016 del servizio relativo alla predisposizione del dossier richiesto dalla procedura per l'accreditamento del Consorzio Universitario Piceno come struttura formativa della Regione Marche.	1	Stipulata	10/12/2019 09:11:00	20/12/2019 10:25:38	20/12/2019 10:29:15
2446463	Richiesta esplorativa di preventivi propedeutica all'affidamento diretto ai sensi dell'art. 36 comma 2 lettera a) del D.Lgs. 50/2016 e s.m.i. a favore del Consorzio Universitario Piceno del servizio di somministrazione di lavoro a tempo determinato part time di n.1 unità di personale nell'ambito dell'orientamento universitario.	1	Stipulata	14/11/2019 13:43:00	03/12/2019 15:57:40	03/12/2019 16:00:24

	2425315	Richiesta esplorativa di preventivi propedeutica all'affidamento diretto ai sensi dell'art. 36 comma 2 lettera a) del D.Lgs. 50/2016 e s.m.i. del servizio di stampa e consegna di prodotti di comunicazione a favore del Consorzio Universitario Piceno.	1	Scaduta	23/10/2019 13:16:00	-	-
	2412367	Richiesta esplorativa di preventivi propedeutica all'affidamento diretto ai sensi dell'art. 36 comma 2 lettera a) del D.Lgs. 50/2016 e s.m.i. del servizio di stampa e consegna di prodotti di comunicazione a favore del Consorzio Universitario Piceno.	1	Scaduta	11/10/2019 09:18:00	-	-
	2378205	Richiesta esplorativa di preventivi propedeutica all'affidamento diretto ai sensi dell'art. 36 comma 2 lettera a) del D.Lgs. 50/2016 e s.m.i. del servizio di progettazione grafica, consulenza in comunicazione, adeguamento, gestione e popolamento sito internet e gestione social media a favore del Consorzio Universitario Piceno	1	Stipulata	30/08/2019 15:11:00	26/09/2019 09:42:50	26/09/2019 09:46:56

CONSORZIO UNIVERSITARIO PICENO

Supporto alla Responsabile dell'Area Amministrativa Istituzionale nella predisposizione delle seguenti RdO

N. OdA	Comunicazione da leggere	Autore	Descrizione	Fornitore
4970368		BVRLSN001	Affidamento servizio assistenza software - 2019	HALLEY INFORMATICA S.R.L.

Tutta la documentazione relativa alle attività svolte è a disposizione presso la Segreteria Generale del Consorzio Universitario Piceno.

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

Il Responsabile di Area
Acquisti Telematici, Appalti e Contratti

F.to Ing. Loris Pierbattista

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Ok (LanSweeper)
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Ok (LanSweeper)
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	Ok (LanSweeper)
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	OK (Firewall watchguard)
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	OK (Domain Controller)
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	OK (Domain Controller)
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Ok (LanSweeper)
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Ok (LanSweeper)
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.	Ok (LanSweeper)
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.	Ok (LanSweeper)
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	no
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	no

1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	no

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
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.	Ok (LanSweeper)
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.	Ok (LanSweeper)
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	no
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Ok (LanSweeper)
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Ok (LanSweeper)
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.	Ok (LanSweeper)
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	Ok (LanSweeper)
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o	Ok (Proxmox)

				critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	OK Ogni sistema è provvisto di antivirus Bitdefender continuamente aggiornato e il traffico monitorato dal firewall, per ogni client
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.	no
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	no
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Ok (Fog server e backup Proxmox VM)
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Ok (Fog server e backup Proxmox VM)
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	OK solo per i server VM
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	NO manca HARDWARE da acquistare
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	NO manca HARDWARE

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).	OK Il collegamento sul firewall e sull'hypervisor avviene solo ed esclusivamente tramite HTTPS, utilizzando un filtro a livello di ip pubblico autorizzato impostato sul firewall ad aprire la connessione,accesso alla rete da VPN tramite autenticazione di username e password complesse.
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.	OK (bitdefender)
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	NO
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	NO
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	NO
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	NO
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	NO

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
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.	NO (manca software SIEM) verrà implementato a partire da settembre

4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	NO
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	NO
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	NO
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	NO
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	NO
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.	NO
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.	NO
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	NO (manca software SIEM)
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	NO
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	OK Server e client sono in active directory ; è stato impostato l'aggiornamento automatico di antivirus, SO e software microsoft.
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.	OK Non ci sono dispositivi esclusi dalla connettività internet presenti nella struttura.

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.	NO
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.	OK nViene effettuato dall'amministratore di sistema dopo segnalazione firewall/antivirus
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.	NO
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.).	NO chi lo deve stilare?
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.	OK L'applicazione delle patch viene fatta in automatico appena disponibili, per le patch sul server si attende 2 o 3 settimane prima dell'installazione in caso di eventuali fix alle patch stesse. Siamo in costante contatto tramite i mezzi informativi con Microsoft e watchguard per comunicazioni di patch di criticità elevata, al momento della ricezione le patch vengono applicate entro 24h dall'informativa
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.	OK Viene effettuato dall'amministratore di sistema
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.	OK È stato creato un ambiente di test vistualizzato su cluster PROXMOX

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
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.	OK Può operare con privilegi amministrativi solo l'amministartore di sistema
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	OK Ogni accesso di un utenza amministrativa ad ogni server viene automaticamente registrato nei vari log previsti.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	OK (active directory)
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	NO
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	OK Esiste una sola utenza amministrativa ed è utilizzata dall'amministratore di sistema
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	NO
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.	SI è la normale prassi
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	NO
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	NO
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	NO
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	OK (active directory)
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	NO

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).	OK Password amministrativa è complessa e sostituita ogni 50gg)
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	OK (active directory Password policy)
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	OK (active directory Password policy)
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	OK (active directory Password policy)
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	OK (active directory Password policy)
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	OK (active directory Password policy)
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.	NO, soluzione implementata solo su sistemi LINUX
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	NO
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	OK (active directory)
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	OK (active directory) utenze amministrative utilizzate solo dall'amministratore di sistema
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.	OK (active directory) utenze amministrative utilizzate solo dall'amministratore di sistema
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).	NO

5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	OK Credenziali amministrative di gestione di dominio e root sono consegnate dentro busta chiusa
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	OK Non è implementato l'accesso ai sistemi tramite certificati digitali

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
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.	OK Presente bitdefender in tutti i server e pdl della struttura
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	OK Presente bitdefender in tutti i server e pdl della struttura
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	NO (manca software SIEM)
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.	OK GravityZone di bitdefender
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.	OK GravityZone di bitdefender
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	OK GravityZone di bitdefender
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	OK Ogni dispositivo esterno, ha bisogno di credenziali per utilizzare risorse in rete
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	OK LANswepper
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	OK attiva in ogni windows
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	OK bitdefender

8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	OK FIREWALL watchguard
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	OK bitdefender
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	OK FIREWALL watchguard
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	OK active directory policy
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	OK configurato su office 2013
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Ok configurato su outlook 2013 e Kerio client
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Ok configurato su outlook 2013 e Kerio client
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	OK Funzionalità attualmente attiva tramite bitdefender
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.	OK Funzionalità attualmente attiva tramite bitdefender
8	9	2	M	Filtrare il contenuto del traffico web.	OK Funzionalità attualmente attiva tramite bitdefender e firewall watchguard
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).	OK Funzionalità attualmente attiva tramite bitdefender e firewall watchguard
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	OK Funzionalità attualmente attiva tramite bitdefender
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	Ok Funzionalità attualmente attiva tramite bitdefender

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID	Livello	Descrizione	Modalità di implementazione

10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	OK E' presente un backup completo delle macchine virtuali server una volta a settimana.
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	OK backup configurato sia su VM dei server (so e applicazioni)tramite funzionalità di Proxmox e dei dati tramite funzionalità NAS qnap separatamente
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	OK backup configurato sia su VM dei server (so e applicazioni)tramite funzionalità di Proxmox e dei dati tramite funzionalità NAS qnap separatamente
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	NO (non sono stati programmati test di disaster recovery
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.	NO (manca HW o contratto cloud) da acquiare
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.	NO (manca HW o contratto cloud) da acquistare

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
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	OK GDPR gap analysis effettuata
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	NO
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non	OK Firewall Watcguard

				autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	NO
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	NO
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	NO
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	NO
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	NO manca siem
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	NO
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	SI firewall
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	NO