Simpresa
Azienda Speciale della CCIAA di Napoli

DELIBERA DELL'AMMINISTRATORE UNICO
N. ...68... DEL ...25/09/2018

Oggetto: Adempimenti in materia di Privacy aziendale

Vista la Legge n. 580/1993 recante "Riordinamento delle Camere di Commercio, Industria, Artigianato e Agricoltura", come modificata dal D. Lgs. n. 23/10 e successivo decreto legislativo n.219/2016;

Visto il Decreto del Presidente della Giunta Regionale Campania n. 58 del 03/03/2016, notificato all'Ente il 07/03/2016, con cui l'Avv. Girolamo Pettrone è stato nominato Commissario Straordinario della C.C.I.A.A. di Napoli, con il potere di sostituire, a tutti gli effetti, per i compiti e le funzioni, gli Organi (Presidente e C.d.A.) delle dipendenti Aziende Speciali ed adottare tutti gli atti ed i provvedimenti tipici di riferimento;

Vista la Determina Commissariale n. 85 del 06/07/2016, con cui il Commissario Straordinario ha approvato, con in poteri della Giunta Camerale, l'atto di fusione per incorporazione, con decorrenza 01/01/2016, nell'Azienda Speciale "Euro-sportello", rinominata "S.I. Impresa", delle sei Aziende Speciali dipendenti e cioè "Agripromos, Com.Tur, Eurosportello, Cesvitec, Proteus e Laboratorio Chimico Merceologico (L.C.M.)", per rogito del dott. Rizzo Francesco, notaio in Afragola (NA), registrato al Rep. n. 133, raccolta n. 88;

Considerato che, ai sensi dell'art. 6 del vigente Statuto di detta Azienda "S.I. Impresa", rientra tra gli atti tipici dell'Amministratore Unico, nella persona del suindicato Avv. Girolamo Pettrone, la rappresentanza legale dell'Ente e nello specifico la stipula di convenzioni;

Visto l'Organigramma funzionale dell'Azienda Speciale "S.I. Impresa", predisposto con provvedimento n.48 del 23.07.2018 dall'Amministratore Unico ed approvato con Determinazione del Commissario Straordinario con i poteri della Giunta Camerale, n. 101 del 31.07.2018, ex art. 4, comma 2°, dello Statuto della C.C.I.A.A.;

Vista la delibera n.16 del 05 marzo 2018, con cui è stato dato incarico al Consorzio Promos Ricerche di redazione del "Manuale sulle misure di sicurezza e organizzative in ambito Privacy", di consulenza e formazione in materia di Privacy;

Richiamata la delibera dell'amministratore n. 31 del 16 maggio 2018 con cui per l'Azienda è stato nominato Responsabile del trattamento dei dati personali la dr.sa Maria Rosaria Furgiuele;

Tenuto conto che in data 24 maggio 2018 l'Amministratore ha nominato la dr.sa Maria Rosaria Furgiuele, responsabile della protezione dei dati dandone comunicazione all'Autorità Garante per la protezione dei dati personali;

Il Dirigente Responsabile dell'Area Amministrativa e del Personale dell'Azienda Speciale, dott.ssa Maria Antonietta Polito, la quale svolte anche le funzioni di verbalizzante, e che ne attesta la regolarità del procedimento svolto, la correttezza ed i profili di competenza, la veridicità degli atti richiamati e la loro esistenza quale l'Ufficio Istruttore, avanza la seguente relazione:

Il Consorzio Promos ricerche così come incaricato dall'Azienda ha predisposto nei mesi scorsi il "Manuale sulle misure di sicurezza e organizzative in ambito Privacy (GDPR)".

Al fine di ottemperare alle disposizioni di cui al Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)» (di seguito RGPD), in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018, occorre individuare alcune figure professionali interne cui va conferito incarico formale per il trattamento di dati di loro competenza.

Pertanto, tenuto conto dell'Organigramma funzionale dell'Azienda Speciale "S.I. Impresa",

PROPONE

- Di confermare la nomina della dr.sa Maria Rosaria Furgiuele quale responsabile del trattamento dei dati personali nonché della protezione degli stessi;

- Di approvare il "Manuale sulle misure di sicurezza e organizzative in ambito Privacy (GDPR)" e le relative procedure, in allegato al presente provvedimento che ne costituiscono parte integrante;

- Di nominare quali incaricati per il trattamento degli archivi cartacei e informatizzati, i responsabili dei seguenti uffici ciascuno per quanto di competenza:

    1. Ufficio Affari generali, Segreteria e protocollo;
    2. Ufficio Contabilità e tesoreria
    3. Ufficio Programmazione, controllo di gestione e Personale
    4. Ufficio Formazione
    5. Ufficio Comunicazione, Sito internet e politiche Privacy
    6. Ufficio Servizi camerali
    7. Ufficio progetti e attività di supporto alle Aziende
    8. Ufficio amministrazione LCM

- Di demandare al Responsabile del trattamento dei dati personali la nomina dell'Amministratore dei sistemi informatici, responsabile della manutenzione di tutti i sistemi informatici aziendali;

Il Dirigente Responsabile
(Area Amministrativa e del Personale)

L'Amministratore Unico

vista l'istruttoria e la proposta di determinazione avanzata dal Dirigente Responsabile dell'Area Amministrativa e del Personale, Dott.ssa Maria Antonietta Polito, la quale svolge anche le funzioni di verbalizzante, e che attesta la regolarità del procedimento;

in qualità di legale rappresentante dell'Azienda e titolare del trattamento dei dati personali;

valutate positivamente le competenze professionali degli incaricati per il trattamento degli archivi cartacei e informatizzati;

DELIBERA

- Di confermare la nomina della dr.sa Maria Rosaria Furgiuele quale responsabile del trattamento dei dati personali nonché della protezione degli stessi;

- Di approvare il "Manuale sulle misure di sicurezza e organizzative in ambito Privacy (GDPR)" e le relative procedure, in allegato al presente provvedimento che ne costituiscono parte integrante;

- Di nominare quali incaricati per il trattamento degli archivi cartacei e informatizzati, i responsabili dei seguenti uffici ciascuno per quanto di competenza:

    9. Ufficio Affari generali, Segreteria e protocollo;
    10. Ufficio Contabilità e tesoreria
    11. Ufficio Programmazione, controllo di gestione e Personale
    12. Ufficio Formazione
    13. Ufficio Comunicazione, Sito internet e politiche Privacy
    14. Ufficio Servizi camerali
    15. Ufficio progetti e attività di supporto alle Aziende
    16. Ufficio amministrazione LCM

- Di demandare al Responsabile del trattamento dei dati personali la nomina dell'Amministratore dei sistemi informatici, responsabile della manutenzione di tutti i sistemi informatici aziendali;
- di pubblicare la presente deliberazione nella Sezione "Amministrazione trasparente" del sito dell'Azienda Speciale.

L'Amministratore Unico
(Girolamo Pettrone)

Simpresa

Azienda Speciale della CCIAA di Napoli

MANUALE GDPR

SIImpresa – Manuale GDPR

redatto ai sensi del D.Lgs. n. 101 del 4 settembre 2018 e del Regolamento Europeo n. 679 del 27 aprile 2016

Indice generale

1 Scopo e Campo di applicazione

Scopo del presente Manuale è quello di descrivere i compiti, le responsabilità e le modalità operative relative a tutte le procedure di trattamento dei dati personali operate da SIImpresa, Azienda Speciale Unica della Camera di Commercio di Napoli.

1.1 Obblighi derivanti dalla Legge

Nel caso di SIImpresa, benché in base al Regolamento l'emissione del presente Documento non sia obbligatoria, purtuttavia il Titolare ha avvertito la necessità di riunire tutte le norme organizzative ed i regolamenti interni in un unico testo allo scopo di facilitarne l'applicazione da parte di tutto il personale. L'emissione del presente documento è comunque conforme alle prescrizioni di cui alle Misure minime di Sicurezza previste nell'Allegato B del Codice.

1.2 Campo di Applicazione

Il presente Documento Programmatico sulla Sicurezza si applica a tutte le attività svolte dall'Azienda Speciale unica SIImpresa.

Le prescrizioni contenute in questo documento vanno applicate in generale a qualunque trattamento di Dati Personali effettuato nell'Azienda, e quindi ai Trattamenti di Dati:

- dei quali l'Ente è direttamente Titolare;
- dei quali l'Ente è co-titolare, insieme ad altro ente od organizzazione;
- dei quali l'Ente ha affidato alcune operazioni del trattamento ad apposito Responsabile;
- dei quali l'Ente opera in qualità di Responsabile.

1.3 Obbligo dell'osservanza delle disposizioni del GDPR in SIImpresa

Le prescrizioni contenute nel presente documento vanno rispettate e fatte rispettare all'interno di SIImpresa, in base alle competenze di ciascuno. Tutti i dipendenti di SIImpresa, devono essere edotti sulla sua esistenza e informati sui suoi contenuti.

Eventuali situazioni di deviazione accertate rispetto a quanto prescritto nel presente documento dovranno essere documentate e rimosse nel più breve tempo possibile.

Il presente documento dovrà essere aggiornato periodicamente con le modalità e la cadenza che il Titolare del trattamento vorrà applicare.

2 Riferimenti normativi generali

- D.Lgs. 101 del 4 settembre 2018;
- Direttiva Europea n. 680 del 27 aprile 2016;
- Regolamento Europeo n. 679 del 27 aprile 2016;
- D.Lgs. 196 del 30 giugno 2003 e ss.mm.ii.;
- Provvedimenti del Garante per la Protezione dei dati personali.

2.1 Riferimenti normativi specifici

Stante la natura e le finalità di SIImpresa, nell'attesa nella pubblicazione del futuro Regolamento per la certificazione della protezione dei dati personali, si ritiene opportuna, oltre all'applicazione di quanto previsto nel D. Lgs. 101/2018, nel Regolamento Europeo n. 679/2016, l'applicazione delle precedenti norme specifiche di cui al Titolo III, capo II, del D.Lgs. 196/2003 intitolato "Regole ulteriori per i soggetti pubblici", che si riportano di seguito:

REGOLE ULTERIORI PER I SOGGETTI PUBBLICI

Art. 18 (Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici)

1. Le disposizioni del presente capo riguardano tutti i soggetti pubblici, esclusi gli enti pubblici economici.

2. Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.

3. Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal presente codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.

4. Salvo quanto previsto nella Parte II per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato.

5. Si osservano le disposizioni di cui all'articolo 25 in tema di comunicazione e diffusione.

Art. 19 (Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari)

1. Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'articolo 18, comma 2, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente.

2. La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'articolo 39, comma 2, e non è stata adottata la diversa determinazione ivi indicata.

3. La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

Art. 20 (Principi applicabili al trattamento di dati sensibili)

1. Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

2. Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo.

3. Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2.

4. L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente.

Art. 21 (Principi applicabili al trattamento di dati giudiziari)

1. Il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

2. Le disposizioni di cui all'articolo 20, commi 2 e 4, si applicano anche al trattamento dei dati giudiziari.

Art. 22 (Principi applicabili al trattamento di dati sensibili e giudiziari)

1. I soggetti pubblici conformano il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.

2. Nel fornire l'informativa di cui all'articolo 13 i soggetti pubblici fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.

3. I soggetti pubblici possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

4. I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato.

5. In applicazione dell'articolo 11, comma 1, lettere c), d) ed e), i soggetti pubblici verificano periodicamente l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. Al fine di assicurare che i dati sensibili e giudiziari siano indispensabili rispetto agli obblighi e ai compiti loro attribuiti, i soggetti pubblici valutano specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'indispensabilità dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.

6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.

8. I dati idonei a rivelare lo stato di salute non possono essere diffusi.

9. Rispetto ai dati sensibili e giudiziari indispensabili ai sensi del comma 3, i soggetti pubblici sono autorizzati ad effettuare unicamente le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.

10. I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psicoattitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto tra dati sensibili e giudiziari, nonché i trattamenti di dati sensibili e giudiziari ai sensi dell'articolo 14, sono effettuati solo previa annotazione scritta dei motivi.

11. In ogni caso, le operazioni e i trattamenti di cui al comma 10, se effettuati utilizzando banche di dati di diversi titolari, nonché la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge.

12. Le disposizioni di cui al presente articolo recano principi applicabili, in conformità ai rispettivi ordinamenti, ai trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale.

3 Termini, Definizioni ed Abbreviazioni

Regolamento: Regolamento Europeo n. 679 del 27 aprile 2016

Codice: D.Lgs. 196/03-"Codice di Protezione in materia di dati personali", così come modificato dal D. Lgs. 101/18

SI Impresa: Azienda Speciale Unica della Camera di Commercio di Napoli, nata nel 2016 dalla fusione per incorporazione delle Aziende Agripromos, Cesvitec, Com-Tur, Laboratorio Chimico Merceologico e Proteus nell'Azienda Speciale Eurosportello secondo il disposto della Legge 580/93 sul 'Riordinamento delle Camere di Commercio, Industria, Artigianato e Agricoltura', art. 2 comma 5, come modificato dal D.Lgs. 219/2016.

CdC: Camera di Commercio, Industria, Artigianato e Agricoltura

U.O.: Unità Organizzativa (in SIImpresa)

Titolare del trattamento: "la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza"[1]

Responsabile del trattamento: "la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali"[2]

Responsabile della protezione dei dati: "la persona esperta nella protezione dei dati, il cui compito è valutare e organizzare la gestione del trattamento di dati personali, e dunque la loro protezione, all'interno di un'azienda, di un ente o di una associazione, affinché questi siano trattati in modo lecito e pertinente"[3]

4 Elenco dei trattamenti di dati personali effettuati

Nel presente capitolo sono individuati i trattamenti effettuati in SIImpresa, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura interna od esterna operativamente preposta, nonché degli strumenti impiegati. L'elenco di tali trattamenti è riportato nella Tabella, allegata:

Tabella 1.1. L'ELENCO DEI TRATTAMENTI DI DATI PERSONALI

In essa ogni trattamento è suddiviso in base alla U.O. interessata ed individuato tramite un identificativo.

---

1 Art. 4 comma 1 lettera f – D.Lgs. 196/2003
2 Art. 4 comma 1 lettera g – D.Lgs. 196/2003
3 Art. 39 – Regolamento Europeo n. 679/2016

Ai fini della corretta interpretazione della tabella occorre anche considerare che:

Alcuni trattamenti (puntualmente individuati nella Tabella) operati dalla U.O. Progetti e attività di supporto alle Aziende nell'ambito delle funzioni ad essa demandata, sono operati trattando comunque dati personali secondo incarico ed in base alle procedure definite nell'ambito di altre strutture (la struttura opera come Responsabile del trattamento, incaricata da strutture esterne).

La Tabella 1.1 riportata in Allegato è aggiornata alla data di emissione del presente Documento.

4.1 Competenze e responsabilità delle strutture preposte ai trattamenti

L'articolazione delle competenze e delle responsabilità delle singole strutture preposte ai trattamenti discende primariamente dalla struttura organizzativa dell'Azienda.

In tale ambito è possibile distinguere i trattamenti effettuati dall'Azienda Speciale in due grandi categorie:

1. trattamenti effettuati nello svolgimento delle funzioni istituzionali;
2. trattamenti, previsti dalla legge, effettuati per esigenze organizzative aziendali.

Tipicamente i trattamenti rientranti nel secondo tipo hanno ad oggetto:

a) Dati contabili

   Inerenti ai dati necessari per la gestione della contabilità aziendale. Detti dati vengono utilizzati esclusivamente per rapporti di carattere commerciale e non vengono trattati da personale non autorizzato né ceduti o comunque comunicati e/o diffusi a terzi.

b) Dati retributivi e del personale

   Inerenti ai dati necessari per l'amministrazione del personale dell'Azienda Speciale. Detti archivi vengono utilizzati esclusivamente per rapporti di carattere amministrativo e non vengono trattati da personale non autorizzato né ceduti o comunque comunicati e/o diffusi a terzi, fatti salvi gli obblighi di legge.

Con riferimento ai diversi uffici individuati nell'apposita tabella, si specifica inoltre quanto segue:

Assistenza alle imprese

Le attività della U.O. sono soggette a sistema di gestione per la qualità certificato e seguono le apposite procedure descritte nel Manuale della Qualità.

Le attività svolte per l'assistenza alle imprese si concretizzano in:

a) attività di Sportello (Euro Infocentre): risoluzione a quesiti su tematiche varie e rendicontazione semestrale alla Commissione UE. I dati anagrafici dei richiedenti sono conservati attraverso un software proprietario con procedure di sicurezza apposite.
b) Banca dati per la ricerca di partner commerciali;
c) Informazione proattiva: servizi di informazione alle imprese su eventi (convegni, workshop, etc.) ed iniziative. L'informazione viene resa tramite posta elettronica e bollettini di informazione (cartaceo e telematico);
d) Consultazioni periodiche (sondaggi, etc.).

Amministrazione

La contabilità viene gestita attraverso software interno con la consulenza di un soggetto esterno appositamente incaricato.

Con specifico riferimento alla compilazione e stampa dei cedolini dei dipendenti, tale compito è stato affidato tramite apposito incarico a società esterna.

4.2 Analisi dei rischi che incombono sui dati

Ai fini della redazione del presente Documento Programmatico sulla sicurezza SIImpresa ha provveduto ad effettuare un'analisi dei rischi che incombono sui dati e sulle loro elaborazioni e fruibilità.

Giova a tal proposito richiamare quanto disposto dall'art. 32 del Regolamento, che al comma 2 detta i principi generali in materia di valutazione del livello di sicurezza:

"Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati"

Pertanto l'Azienda Speciale ha provveduto a rilevare i principali eventi potenzialmente dannosi per la sicurezza dei dati, con le relative possibili conseguenze e la gravità di ciascuna di esse.

L'analisi dei rischi è stata estesa sia al trattamento di dati attraverso strumenti elettronici, sia ai trattamenti cartacei ed in considerazione del contesto fisico – ambientale in cui i trattamenti vengono effettuati.

Tale analisi dei rischi andrà riveduta almeno annualmente e comunque tenuta aggiornata rispetto all'evoluzione delle tecnologie e/o a mutamenti organizzativi dell'ente.
In merito alla sicurezza dei locali si rinvia agli adempimenti attuati da SIImpresa in osservanza delle previsioni del D.Lgs. n. 81/2008.

Sistema di misurazione: l'analisi dei rischi è stata effettuata adottando un sistema di misurazione di tipo qualitativo (rischio alto/medio/basso). La valutazione è eseguita considerando il contesto operativo in cui il rischio viene collocato, il livello del rischio del fattore umano commisurato al grado di consapevolezza da parte del singolo operatore, e il livello di protezione assicurato dagli strumenti adottati.
Metodo di valutazione: il metodo di valutazione tiene conto ed esprime un valore di rischio per ciascuna minaccia tenuto conto della natura del dato trattato, della finalità del trattamento, della destinazione o meno del dato ad essere reso pubblico nell'ambito delle funzioni istituzionali esercitate dall'Ente.

Tutte tali valutazioni sono riportate nella allegata:

Tabella 1.2. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

5 Misure in essere e da adottare

Nell'ambito di SIImpresa i trattamenti che coinvolgono e/o possono coinvolgere dati sensibili o giudiziari sono effettuati sia con strumenti informatici sia senza l'ausilio di strumenti informatici.
Per quanto riguarda i trattamenti effettuati con strumenti elettronici posti in essere direttamente da SIImpresa, ossia senza avvalersi delle procedure informatiche messe a disposizione da altro soggetto esterno, l'ente provvede direttamente ad adeguarsi alle prescrizioni in materia di misure minime di sicurezza.

5.1 Sicurezza Fisica

.5.1.1 *Sicurezza fisica dei dati elaborati senza l'ausilio di strumenti elettronici*

Per quanto riguarda i locali e gli archivi che contengono dati personali di questa tipologia, l'Azienda si è dotata di aree ad accesso controllato. Tali aree devono essere all'interno di aree sotto la responsabilità diretta di SI Impresa.

Per tali aree:

- Il locale deve essere chiuso, salvo eventuali accessi autorizzati da parte di singoli incaricati e/o imprese di pulizia o sorveglianza.
- L'accesso deve essere consentito solo alle persone autorizzate.
- L'accesso deve essere possibile solo dall'interno dell'area sotto la responsabilità dell'Azienda Speciale.
- Il responsabile incaricato mantiene un effettivo controllo sull'area di sua responsabilità.

L'accesso a tali aree e la gestione di tali archivi è regolata da apposita procedura:

POS 01 – ACCESSO AGLI ARCHIVI CARTACEI

Allegata al presente manuale.

Le U.O. interessate ed i trattamenti specifici sono indicati nella Tabella 1.1, già ricordata.

5.2 Sicurezza informatica

Tutte le procedure organizzative e le regole di sicurezza adottate da SI Impresa per la protezione dei trattamenti effettuati tramite supporto informatico sono compendiate nelle:

POS 02 – SICUREZZA DEI SISTEMI INFORMATICI (SI);

POS 03 – ACCESSI LOGICI;

POS 04 – GESTIONE ANTIVIRUS.

Allegate al presente Manuale

5.3 Valutazione d'impatto sulla protezione dei dati

Secondo quanto previsto all'art. 35 del Regolamento:

"Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di

procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali."

L'art. 35, paragrafo 7, del Regolamento individua il contenuto minimo obbligatorio di una tale valutazione, ossia:

a) una descrizione sistematica dei trattamenti previsti, delle finalità dei trattamenti e, se presente, dell'interesse legittimo del titolare;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;
d) le misure, anche di sicurezza, previste per affrontare i rischi e garantire la protezione dei dati personali e dimostrare la conformità al Regolamento.

La Valutazione d'impatto dovrebbe contenere anche informazioni relative:

- all'adesione da parte del titolare e/o del responsabile ai codici di condotta di cui all'art. 40;
- alle opinioni degli interessati (o dei loro rappresentanti) sul trattamento previsto;
- al riesame effettuato sulla conformità del trattamento alla Valutazione in caso di variazioni del rischio (cfr. art. 35, paragrafi 8, 9 e 11).

Qualora il Titolare decida di procedere alla raccolta delle opinioni degli interessati o dei loro rappresentanti, potrà farlo secondo le seguenti modalità:

- questionario inviato ai futuri clienti del titolare;
- quesito rivolto ai rappresentanti del personale;
- studio generico sulle finalità e mezzi del trattamento.

Qualora la decisione adottata dal Titolare si discosti dall'opinione degli interessati, bisognerà documentare le motivazioni che hanno condotto alla prosecuzione o meno del progetto. Dovranno in tal caso essere documentate anche le motivazioni della mancata consultazione degli interessati.

La Valutazione d'impatto deve essere svolta comunque ***prima*** di mettere in atto le procedure di raccolta e gestione dei dati, caratteristiche del trattamento.

L'art. 36 Regolamento prevede poi che il titolare ha l'obbligo di consultare il Garante qualora la Valutazione d'impatto effettuata indichi che il trattamento "presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio". Anche tale attività va effettuata prima della effettiva messa in atto delle procedure di raccolta e gestione dei dati.

6 Descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati

Per tutti i trattamenti di dati personali effettuati con strumenti elettronici in cui partecipa il Responsabile sono previste da parte di quest'ultimo apposite procedure di salvataggio periodico dei dati, nonché procedure di ripristino della loro disponibilità.

I compiti, le responsabilità e le modalità operative di tali attività sono riportate nella:

POS 05 – BACKUP RESTORE

Allegata al presente Manuale.

7 Previsione di interventi formativi degli incaricati del trattamento

Sono previsti interventi formativi generalizzati a tutti i dipendenti dell'Azienda Speciale da attuare con periodicità almeno annuale. Detti interventi sono tesi a rendere edotti gli incaricati sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano, sulle modalità per aggiornarsi sulle misure minime adottate dal Titolare.

Sono altresì previsti interventi formativi nei confronti di nuovi assunti ovvero in caso delle modalità di trattamento o di trasferimento di mansioni. Detti interventi sono svolti dal capo ufficio dell'incaricato entro 30 gg. dal verificarsi dell'evento che richiede la formazione stabilita.

In Appendice viene allegata la scheda

TABELLA 1.3. - PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI OBBLIGATORI

aggiornata alla data di emissione del presente Documento.

8 Trattamenti di dati personali affidati all'esterno della struttura del titolare

I trattamenti informatici affidati all'esterno sono quelli effettuati da Responsabili esterni in base ad appositi vincoli contrattuali.

I Responsabili esterni sono vincolati, nell'ambito dei trattamenti a loro affidati, al rispetto delle previsioni del presente Manuale tramite un espresso conferimento di incarico secondo le modalità riportate nell'Allegato:

TESTO 1 – INCARICO TRATTAMENTO-CONSULENTI ESTERNI.

Allegato al contratto con cui viene conferito l'incarico di consulenza.

9 Allegati

POS 01 – ACCESSO AGLI ARCHIVI CARTACEI

INDICE

SCOPO

Scopo di questa Procedura è quello di definire gli Standard Generali di Sicurezza a cui ottemperare in ambito aziendale, in modo da:

- poter assicurare l'accesso alle informazioni aziendali registrate su supporto cartaceo, indipendentemente da dove siano allocate, alle sole persone autorizzate;
- assicurare qualità ed integrità di tali informazioni;
- proteggere le informazioni, riducendo al minimo i possibili danni causati a *S*/Impresa in caso di danneggiamento, perdita o accesso non autorizzato a tali informazioni;
- assicurare la disponibilità delle informazioni al personale autorizzato e per le operazioni consentite.

CAMPO DI APPLICAZIONE

La presente pocedura è applicabile a tutti gli archivi cartacei (esistenti e nuovi) da cui può dipendere la conformità dei servizi erogati ed il trattamento delle informazioni ad essi relativi, alle norme per il trattamento dei dati personali.

RIFERIMENTI NORMATIVI

- Direttiva Europea n. 680 del 27 aprile 2016;
- Regolamento Europeo n. 679 del 27 aprile 2016;
- D.Lgs. 196 del 30 giugno 2003 e ss.mm.ii.;
- Provvedimenti del Garante per la Protezione dei dati personali.

RESPONSABILITA'

Responsabile dell'archivio

È responsabile della conservazione e della manutenzione dell'archivio.

Ha il compito di sovrintendere alla corretta operatività delle procedure e di garantire la sicurezza delle informazioni conservate negli archivi aziendali, ove previsti.

In allegato alla presente procedura si riporta una tabella contenente le informazioni relative agli archivi cartacei aziendali ed ai relativi Responsabili.

Responsabile dei Trattamenti dei Dati

Ha il compito di assicurare la coerenza e la qualità dei risultati prodotti dal sistema (contenuto).

E' responsabile del mantenimento nel tempo dello stato di consistenza e significatività delle informazioni.

Utente

Individuo che utilizza e gestisce un archivio cartaceo.

TERMINI E DEFINIZIONI

Sistema di archiviazione

Un sistema progettato per eseguire una funzione di archiviazione specifica o un gruppo di funzioni.

STRUTTURA DEL DOCUMENTO

La sicurezza degli archivi cartacei può essere divisa in:

- Sicurezza logica: gestione dell'accesso ai principali Sistemi di archiviazione ed ai dati aziendali ivi archiviati;
- Sicurezza fisica: controllo dell'accesso alle aree riservate, controllo dei sistemi di sicurezza installati a protezione di tali aree e degli edifici che le ospitano.

ISTRUZIONI OPERATIVE

Sicurezza logica

La maggior parte delle informazioni aziendali, quando archiviate su supporto cartaceo, sono allocate in aree ed armadi a ciò dedicati. E' importante definire appropriati livelli di accesso alle informazioni per gli utenti, sulla base delle loro esigenze di lavoro, tenendo sempre fermo il

presupposto che le informazioni siano sempre reperibili, inalterabili, attendibili e protette da accessi non autorizzati.

Politica di sicurezza adottata

L'accesso alle informazioni aziendali allocate in archivi cartacei avviene a mezzo di rilascio di autorizzazione da parte del Responsabile del Trattamento dati o del Responsabile dell'Archivio.
Al fine di poter aver accesso ai servizi aziendali forniti, un utente deve soddisfare i seguenti requisiti:

- essere un utente autorizzato;
- essere a conoscenza delle procedure adottate per la protezione dei dati raccolti per l'espletamento del servizio;
- essere a conoscenza delle procedure e politiche di sicurezza.

Per accedere agli archivi cartacei, ogni utente deve essere identificato tramite una autorizzazione scritta, registrata sull'apposito registro. Questa autorizzazione è essenziale per la identificazione e l'evidenza dell'assenso ad accedere agli archivi di ogni utente di *SI*Impresa.

I dati fondamentali per gestire la sicurezza degli accessi sono:

Identificativo: questo è l'identificativo dell'utente. Esso:

- deve essere facilmente associabile all'utente;
- è in chiaro e quindi visibile anche a utenti diversi;
- deve essere unico, nel caso la regola di composizione porti alla creazione di due identificativi identici si deve prevedere una regola per risolvere questi casi.

Dati caratteristici dell'accesso: essi:

- devono contenere la data di inizio e fine dell'accesso;
- devono essere associati ad un unico utente;
- devono prevedere una scadenza;
- devono prevedere una motivazione all'accesso;

- devono comprendere anche se i dati da accedere devono essere resi disponibili in sola lettura o per la modifica.

Le regole per definire i dati fondamentali per un sistema che gestisce la sicurezza degli accessi, ossia Identificativo e Dati caratteristici, devono essere definite in un'apposita procedura operativa, che ne descriva la struttura e le modalità di trattamento assieme alle responsabilità delle figure aziendali interessate.

Oltre alla definizione di come un utente possa accedere agli archivi cartacei dell'azienda, bisogna anche definire quali regole tali accessi devono seguire:

- ad ogni coppia di Identificativo e Dati caratteristici deve essere associato:
  - un livello di accesso per il quale siano definiti tutti i permessi e le restrizioni;
  - un profilo che può essere definito per il singolo utente o con una logica a gruppi.

Ogni sistema di controllo degli accessi ad archivi cartacei deve avere un Responsabile degli archivi con il compito di:

- gestire la registrazione degli utenti nelle varie aree riservate;
- gestire la registrazione dei Dati caratteristici;
- gestire gli accessi ai locali;
- gestire le eventuali richieste di accessi da parte di personale estraneo all'Azienda.

Altre forme di protezione

Devono essere utilizzate tutte le tecnologie e le procedure che permettono di aumentare il grado di sicurezza dei dati aziendali come il blocco delle aree e degli armadi in cui sono allocati gli archivi in caso di assenza di richieste di accesso da parte degli utenti, la messa in atto di procedure per la protezione dei dati in caso di pericolo di corruzione o distruzione degli stessi, la protezione degli archivi da accessi da parte di personale non autorizzato.

Sicurezza fisica

Ogni area ove vengono processate / gestite informazioni deve essere sottoposta a controlli di "protezione fisica" appropriata alla dimensione ,alla complessità delle attività ed alla criticità delle operazioni e dei dati trattati in quell' area.

Parlando di Sicurezza Fisica si intende:

- sicurezza legata ai luoghi (accesso ad edifici, stanze, ecc...)
- sicurezza legata ai dati (accesso, registrazione, trasporto, ecc...)
- sicurezza legata alle macchine (copia su supporto cartaceo o scannerizzazione e archiviazione su supporto informatico)

Accesso alle aree in cui sono conservate le informazioni

Tali sono i luoghi dove vengono posti i supporti che archiviano e gestiscono i dati aziendali, l'accesso a tali luoghi è gestito dal Responsabile del Trattamento dei Dati *S*Impresa che ne regolamenta gli accessi. Per limitare l'accesso alle sole attività necessarie alle attività aziendali, il Responsabile del Trattamento o il Responsabile dell'archivio concedono temporaneamente l'autorizzazione, che viene registrata sull'apposito "Registro Accessi" riportando l'Identificativo ed i Dati caratteristici della persona che accede.

POS 02 – SICUREZZA DEI SISTEMI INFORMATICI (SI)

INDICE

SCOPO

Scopo di questa Procedura è quello di definire gli Standard Generali di Sicurezza IT a cui ottemperare in ambito aziendale, in modo da:

- poter assicurare l'accesso alle informazioni aziendali, indipendentemente da dove siano allocate, alle sole persone autorizzate;
- assicurare qualità ed integrità di tali informazioni;
- proteggere le informazioni, riducendo al minimo i possibili danni causati a *S*Impresa in caso di danneggiamento, perdita o accesso non autorizzato a tali informazioni;
- assicurare la disponibilità delle informazioni in linea.

CAMPO DI APPLICAZIONE

La presente procedura è applicabile a tutti i sistemi computerizzati (esistenti e nuovi) da cui può dipendere la conformità dei servizi erogati ed il trattamento delle informazioni ad essi relativi, alle norme per il trattamento dei dati personali.

RIFERIMENTI NORMATIVI

- D.Lgs. 101 del 4 settembre 2018;
- Direttiva Europea n. 680 del 27 aprile 2016;
- Regolamento Europeo n. 679 del 27 aprile 2016;
- D.Lgs. 196 del 30 giugno 2003 e ss.mm.ii.;
- Provvedimenti del Garante per la Protezione dei dati personali.

RESPONSABILITA'

Amministratore di Sistema

È responsabile degli aspetti tecnici e della manutenzione del sistema.
Ha il compito di sovrintendere alla corretta operatività delle procedure e di garantire la sicurezza delle informazioni conservate nei sistemi di backup aziendali, ove previsti.

Responsabile dei Trattamenti dei Dati

Ha il compito di assicurare la coerenza e la qualità dei risultati prodotti dal sistema (contenuto).

E' responsabile del mantenimento nel tempo dello stato di consistenza e significatività delle informazioni.

Esegue le attività di back-up, se così previsto, così come pianificato dall'Amministratore di Sistema.

Utente

Individuo che utilizza e gestisce un sistema computerizzato

TERMINI E DEFINIZIONI

Sistema Computerizzato

Un sistema composto da hardware e software progettato per eseguire una funzione specifica o un gruppo di funzioni.

L'hardware comprende i mainframe, i mini-computer, i personal computer collegati in rete o stand-alone.

Il software comprende quello sviluppato internamente e quello fornito da terzi.

STRUTTURA DEL DOCUMENTO

La sicurezza dei sistemi computerizzati può essere divisa in:

- Sicurezza logica: gestione dell'accesso ai principali Sistemi (ERP, Posta Elettronica, Intranet/Internet), ai server ed ai PC aziendali, ai Data Base ed ai dati storici aziendali archiviati;
- Sicurezza fisica: controllo dell'accesso alle aree riservate, controllo dei sistemi di sicurezza installati a protezione di tali aree e degli edifici che le ospitano.

ISTRUZIONI OPERATIVE

Sicurezza logica

La maggior parte delle informazioni aziendali sono archiviate elettronicamente su Server aziendali. E' importante definire appropriati livelli di accesso alle informazioni per gli utenti, sulla base delle loro esigenze di lavoro, tenendo sempre fermo il presupposto che le informazioni siano sempre reperibili, inalterabili, attendibili e protette da accessi non autorizzati.

La Sicurezza degli accessi non deve essere limitata ai principali Sistemi aziendali ma anche ai sistemi come Posta Elettronica e Intranet/Internet.

Politica di sicurezza adottata

L'accesso alle informazioni aziendali avviene sia per mezzo di sistemi multi utente, cioè sistemi che permettono l'accesso contemporaneo alle informazioni a più persone autorizzate, sia con l'utilizzo di sistemi mono utente.
Al fine di poter connettersi alla rete e poter aver accesso ai servizi aziendali forniti, un utente deve soddisfare i seguenti requisiti:

- essere un utente autorizzato;
- essere a conoscenza delle procedure adottate per la protezione dei dati raccolti per l'espletamento del servizio;
- essere a conoscenza delle procedure e politiche di sicurezza.

Per accedere ai servizi di rete aziendali ed a tutti i sistemi computerizzati, ogni utente deve essere identificato da una User ID e da una Password. Questi sono due elementi essenziali per la identificazione e l'autorizzazione ad accedere ai servizi di rete (applicazioni specifiche, stampanti, aree condivise, aree di salvataggio dati, ecc.) di ogni utente di SI Impresa.

Le caratteristiche fondamentali di questi dati per gestire la sicurezza degli accessi sono:

User ID: questo è l'identificativo dell'utente. Esso:

- deve essere facilmente associabile all'utente, per esempio costruito attraverso una combinazione di nome e di ufficio o area;

- è in chiaro e quindi visibile anche a un utente diverso;
- non ha una scadenza;
- deve avere una regola di composizione per cui per ogni utente è univocamente determinabile;
- non deve essere modificabile dall'utente ma solo dall'Amministratore di Sistema;
- deve essere unico, nel caso la regola di composizione porti alla creazione di due user id identiche si deve prevedere una regola per risolvere questi casi.

- **Password**: questa è la chiave di accesso al sistema. Essa:

- deve essere criptata e quando viene digitata non deve essere leggibile;
- deve essere associata ad un'unico user id (almeno all'atto della creazione della stessa User ID);
- deve avere una scadenza;
- deve essere modificabile a discrezione dall'utente;
- deve avere delle regole, almeno di minima, per essere composta: per esempio una lunghezza minima e il tipo di caratteri permessi.

Le regole per definire i dati fondamentali per un sistema che gestisce la sicurezza degli accessi, ossia User ID e Password, devono essere definite in un'apposita procedura operativa, che ne descriva la struttura e le modalità di assegnazione assieme alle responsabilità delle figure aziendali interessate.

Oltre alla definizione di come un utente possa accedere ai sistemi multi utente dell'azienda, bisogna anche definire quali regole tali accessi devono seguire:

- deve esserci un numero massimo di tentativi di accesso al sistema oltre il quale la User ID viene bloccata;

- ad ogni coppia di User ID e Password deve essere associato:
  - un livello di accesso per il quale siano definiti tutti i permessi e le restrizioni
  - un profilo che può essere definito per il singolo utente o con una logica a gruppi.

Per i sistemi mono utente si possono contemplare due differenti casi:

- sistemi esistenti, per i quali, pur essendo preferibile una gestione della sicurezza tramite l'utilizzo di User ID e Password per i differenti livelli di accesso, si ritiene sufficiente l'esistenza di livelli di accesso differenti controllati unicamente tramite password;
- sistemi da introdurre in azienda per i quali deve essere possibile una gestione dei livelli di accesso al sistema basata sull'utilizzo di una User ID e una Password non per ogni livello di accesso ma per ogni utente con le caratteristiche precedentemente descritte.

Ogni sistema di controllo deve avere un Amministratore di sistema con il compito di:

- gestire l'amministrazione degli account e degli User ID;
- gestire l'autenticazione degli utenti alle varie aree riservate;
- gestire l'amministrazione delle Password;
- gestire gli accessi locali;
- gestire gli accessi da remoto;
- gestire gli accessi alle Applicazioni;

Antivirus

L'integrità dei dati deve essere protetta anche da intrusioni di agenti esterni (programmi) che possono essere introdotti all'interno della rete aziendale, in modo involontario e senza averne un controllo, dagli stessi utenti tramite file provenienti dall'esterno. Tali agenti sono chiamati virus e hanno la capacità, soprattutto se non si interviene tempestivamente, di corrompere i dati che sono presenti sulla macchina su cui si trovano o peggio sulle macchine collegate in rete aziendale.

L'integrità dei dati viene protetta dall'attacco di virus informatici tramite un software anti-virus, in grado di operare in tutti gli ambienti informatici dei vari Sistemi. Il software anti-virus deve essere

periodicamente sottoposto a processi di aggiornamento al fine di garantirne l'efficacia contro virus di più recente generazione.

L'installazione, l'aggiornamento e la gestione del software anti-virus sono competenza della Funzione ICT.

Per quanto riguarda le modalità di installazione sui Server, distribuzione sui Client, aggiornamento alle versioni superiori ed alle modalità operative in caso di attacco deve essere emessa una procedura che ne spieghi le strategie a le modalità di esecuzione.

Altre forme di protezione

Devono essere utilizzate tutte le tecnologie e le procedure che permettono di aumentare il grado di sicurezza dei dati aziendali come il blocco delle work station in caso di assenza prolungata dell'utente, l'esecuzione di backup per garantire la possibilità di ripristino dei dati in caso di corruzione degli stessi, la protezione degli archivi da accessi da parte di personale non autorizzato.

Inoltre, essendo presente nella rete aziendale una connessione con la rete esterna (internet), si deve proteggere la rete aziendale da intromissioni da parte di persone esterne; tale protezione deve essere effettuata utilizzando le tecniche che vengono messe via via a disposizione dall'evoluzione tecnologica come ad es. i firewall, sia hardware che software.

Sicurezza fisica

Ogni area ove vengono processate / gestite informazioni deve essere sottoposta a controlli di "protezione fisica" appropriata alla dimensione ,alla complessità delle attività ed alla criticità delle operazioni e dei dati trattati in quell' area.

Parlando di Sicurezza Fisica si intende:

- sicurezza legata ai luoghi (accesso ad edifici, stanze, ecc...)
- sicurezza legata ai dati (accesso, registrazione, trasporto, ecc...)
- sicurezza legata alle macchine (PC, Server, Applicazioni)

Accesso al CED

È il luogo dove vengono posti i principali supporti informatici che archiviano e gestiscono i dati aziendali, l'accesso a tale luogo è regolamentato dal Responsabile del Trattamento dei Dati *SI*Impresa che ne regolamenta gli accessi. Per limitare l'accesso alle sole attività necessarie al buon funzionamento dei sistemi, il Responsabile concede temporaneamente l'autorizzazione ad accedere al CED che viene registrata sull'apposito "Registro Accessi CED" riportando il nome della persona che accede, giorno e ora di entrata e di uscita.

INDICE

1SCOPO

Scopo della presente procedura è quello di definire le regole relative all'accesso logico a Sistemi ed Applicativi dell'Azienda (database, software, PC, server) in modo da fornire elevati standard di sicurezza e garantire alle informazioni aziendali un'adeguata protezione da alterazioni, cancellazioni, accessi non autorizzati ed una loro continua disponibilità.

Tale politica di gestione della sicurezza dei dati elettronici, se correttamente applicata, dovrebbe:

- poter assicurare l'accesso alle informazioni aziendali, indipendentemente da dove siano allocate, solo alle persone autorizzate
- assicurare qualità ed integrità di tali informazioni
- poter proteggere le informazioni , riducendo al minimo i possibili danni causati all'Azienda in caso di danneggiamento, perdita o diffusione a persone non autorizzate di tali informazioni
- assicurare la disponibilità delle informazioni in linea con le esigenze del Business
- essere in linea con le esigenze di Legge e dei Regolamenti Europei e con gli accordi presi con i Partner di Business.

2.CAMPO DI APPLICAZIONE

La presente procedura è applicabile a tutti i sistemi computerizzati (esistenti e nuovi) da cui può dipendere la conformità dei servizi erogati e del trattamento delle informazioni ad essi relativi, alle norme di Legge nazionali ed ai Regolamenti Europei. Questi sistemi computerizzati comprendono, a titolo di esempio:

- Sistemi di rilevazione e gestione dei dati degli utenti;
- Sistemi di rilevazione e gestione dei dati dei collaboratori diretti;
- Sistemi di gestione della documentazione;
- Sistemi di laboratorio;
- Sistemi di controllo e gestione delle attività di servizio.

Questa procedura si applica sia a sistemi sviluppati internamente a *SI*Impresa, sia a sistemi forniti da altre organizzazioni. Si applica indipendentemente dalle dimensioni del sistema.

3.RIFERIMENTI NORMATIVI

- D.Lgs. 101 del 4 settembre 2018;
- Direttiva Europea n. 680 del 27 aprile 2016;
- Regolamento Europeo n. 679 del 27 aprile 2016;
- D.Lgs. 196 del 30 giugno 2003 e ss.mm.ii.;
- Provvedimenti del Garante per la Protezione dei dati personali.

4.RESPONSABILITA'

Responsabile della Protezione dei Dati

Ha il compito di informare e consigliare il Titolare o il Responsabile dei trattamenti, nonché i dipendenti, sugli obblighi previsti dalle norme in materia e quindi verificarne l'attuazione e l'applicazione

Se richiesto, potrà fornire pareri ed assistere il Titolare in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti.

Egli ha il compito di realizzare l'inventario dei trattamenti e tenere il registro degli stessi.

Responsabile dei Trattamenti dei Dati

E' la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento dei dati personali.

Egli deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.

Amministratore di Sistema

E' la persona fisica o giuridica preposta da *S*Impresa a predisporre la piattaforma del sistema informatico secondo le specifiche del fornitore del sistema. Sovraintende all'installazione dell'eventuale software fornendo supporto ai tecnici del fornitore.

Provvede a configurare il sistema al fine di garantire il corretto funzionamento del sistema. Ha il compito di sovrintendere alla corretta operatività delle procedure e di garantire la sicurezza delle informazioni conservate nei sistemi di backup aziendali, ove previsti.

Configura le policies di gestione degli accessi creando i differenti profili utente. Può resettare le credenziali di accesso qualora vengano dimenticate dall'utente, può bloccare un utente. Non può essere utente del sistema.

5.TERMINI E DEFINIZIONI

Sistema Computerizzato

Un sistema composto da hardware e software progettato per eseguire una funzione specifica o una serie di funzioni. L'hardware comprende i mainframe, i mini-computer, i personal computer collegati in rete o stand-alone. Il software comprende quello sviluppato internamente e quello fornito da terzi.

Incaricato del trattamento

Persona autorizzata al trattamento dei dati personali sotto l´autorità diretta del Titolare o del Responsabile

6.TIPI DI ACCESSO

La sicurezza degli accessi logici ai sistemi computerizzati può essere divisa in:

- Accesso di sistema: gestione dell'accesso ai PC o al dominio (se previsto);
- Accesso applicativo: gestione dell'accesso ai principali Sistemi (ERP, Posta Elettronica, Intranet/Internet, ecc...), ai server ed ai PC aziendali, ai dati storici archiviati;
- Accesso alle risorse: gestione dell'accesso alle periferiche di rete e locali collegate ai computer;
- Accesso remoto: gestione degli accessi da parte del personale esterno;
- Accesso agli strumenti di laboratorio controllati da computer.

7.ISTRUZIONI OPERATIVE

La maggior parte delle informazioni raccolte dall'Azienda sono archiviate elettronicamente su PC o Server aziendali. E' importante definire appropriati livelli di accesso alle informazioni per gli utenti,

sulla base delle loro esigenze di lavoro, tenendo sempre fermo il presupposto che le informazioni siano sempre reperibili, inalterabili ed attendibili.

La Sicurezza degli accessi non deve essere limitata ai principali Sistemi aziendali ma anche ai sistemi come Posta Elettronica e Intranet/Internet.

L'accesso alle informazioni aziendali avviene sia per mezzo di sistemi multi utente, cioè sistemi che permettono l'accesso contemporaneo alle informazioni a più persone autorizzate, sia con l'utilizzo di sistemi mono-utente (stand-alone).

7.1 Accesso di sistema

Per accedere ai servizi di rete aziendali e a tutti i sistemi computerizzati, ogni utente deve appartenere ad un dominio o un gruppo di lavoro, pertanto deve essere identificato da una User ID e da una Password. Questi sono due elementi essenziali per la identificazione e l'autorizzazione ad accedere ai servizi di rete di ogni utente di *S*/Impresa.

E' compito dell'Amministratore di Sistema definire la User ID ed assegnare una Password di primo accesso per ogni nuovo utente.

Le regole standard stabilite in *S*/Impresa sono:

Al fine di poter connettersi alla rete e poter aver accesso ai servizi aziendali forniti, un utente deve soddisfare i seguenti requisiti:

- essere un utente autorizzato;
- essere a conoscenza delle procedure e politiche di sicurezza;
- essere in accordo con le condizioni riportate nelle procedure aziendali.

Di seguito sono indicate le regole che governano la fruizione dei sistemi aziendali:

User ID è composta da almeno sei (6) caratteri definiti in base alla contrazione del ruolo o dell'area di appartenenza.

Nel caso di esigenze particolari si procede all'utilizzo di otto (8) caratteri.

Tale gestione è univoca sia per l'autenticazione presso il server di dominio o gruppo di lavoro che per l'accesso ai sistemi gestionali.

Password è composta da almeno otto (8) caratteri obbligatoriamente alfanumerici di tipo complesso.

Per ogni nuovo utente viene assegnata dall'Amministratore di Sistema una nuova password in seguito modificabile da parte dell'utente stesso.

La gestione delle password varia a seconda del sistema:

Accesso alla rete di dominio (autenticazione presso il server di dominio):

Ogni utente dovrà provvedere trimestralmente al cambiamento della stessa rispettando i requisiti precedentemente descritti. Il periodo di validità delle Password ed i requisiti della password inserita sono controllati automaticamente dal Sistema, che avviserà l'utente e richiederà l'immissione o la modifica della nuova password.

Alla digitazione della password, il Sistema mostra un carattere " * " in corrispondenza di ogni lettera della Password digitata, in modo tale che quest'ultima non possa essere letta da eventuali persone presenti al momento dell'inserimento. La password di accesso al Sistema, una volta definita dall'utente, deve essere consegnata in busta chiusa al Responsabile della Protezione dei Dati il quale provvederà a conservarla in luogo sicuro e protetto.

Nel caso in cui l'utente dimentichi la propria password, dovrà comunicarlo all'Amministratore di Sistema, che provvederà a ripristinare una password provvisoria nel più breve tempo possibile.

In caso di errata digitazione per 3 (tre) volte consecutivamente il sistema automaticamente blocca l'accesso e l'utente dovrà comunicarlo all'Amministratore di Sistema, che provvederà a ripristinare la password provvisoria nel più breve tempo possibile.

Nelle postazioni più sensibili viene impostata la partenza automatica dello screensaver in modo tale che in caso di mancato utilizzo della postazione per un periodo di tempo configurabile venga richiesto nuovamente l'inserimento della password per poter fruire della postazione.

Posta Elettronica

Ogni utente del dominio fruisce della posta elettronica pertanto ha automaticamente a disposizione, al momento dell'accesso in rete, un account di posta aziendale. L'accesso è regolato automaticamente dall'accesso al sistema senza la necessità di inserire nuovamente la password.

Il servizio di gestione della posta elettronica è disponibile attraverso Outlook dove le credenziali per la consultazione della posta non sono disponibili in chiaro per l'utente che è abilitato alla ricezione della posta senza conoscerne le password.

7.2 Accesso agli applicativi

Per ogni applicativo è previsto un accesso come Amministratore al quale è attribuito il livello gerarchico più alto possibile; questo utente pur possedendo tutti i diritti disponibili non deve essere utilizzato per la gestione corrente ma solo per inserire o modificare gli utenti o per modificare ad aggiornare le impostazioni degli applicativi.

Nel caso di normale utilizzo e gestione del sistema, anche l'Amministratore del Sistema entrerà come normale utente con diritti di accesso al sistema a livello organizzativo e non amministrativo.

Gli utenti definiti per un applicativo sono utilizzabili solo in ambito del singolo applicativo e non hanno alcun accesso ad altri programmi.

Gli applicativi presenti in azienda hanno un sistema di password indipendente gestito dall'Amministratore del Sistema che , su richiesta degli utenti permette il cambio password da parte dell'utente.

Alla digitazione della password, il Sistema mostra un carattere " * " in corrispondenza di ogni lettera della Password digitata, in modo tale che quest'ultima non possa essere letta da eventuali persone presenti al momento dell'inserimento. La password di accesso al Sistema, una volta definita dall'utente, deve essere consegnata in busta chiusa al Responsabile della Protezione dei Dati il quale provvederà a conservarla in luogo sicuro e protetto.

Nel caso in cui l'utente dimentichi la propria password, dovrà comunicarlo al Responsabile della Protezione dei Dati, che provvederà a ripristinare la password standard nel più breve tempo possibile.

In caso di errata digitazione per 3 (tre) volte consecutivamente il sistema automaticamente blocca l'accesso e l'utente dovrà comunicarlo all'Amminstratore di Sistema, che provvederà a ripristinare la password provvisoria nel più breve tempo possibile.

<u>Sistema Gestionale</u>

Ad ogni utente che deve usare il sistema viene assegnata una coppia di User ID e Password.

La formulazione della User ID e della password, oltre che la loro gestione, è identica a quella già illustrata per la User ID e la password di accesso alla rete locale.

In caso di mancato utilizzo dell'applicativo per un periodo di tempo configurabile l'applicativo richiede il nuovo inserimento della password per poter eseguire le funzioni disponibili.

Sistemi di Laboratorio

Il sistema è fruibile da postazioni PC dotate del software "Eusoft.lab", così come descritto nella procedura IO-01-01 del Sistema di Gestione del Laboratorio. Quindi sfrutta la sicurezza del sistema applicativo di cui tali postazioni sono dotate. A tal scopo ad ogni utente viene assegnata una coppia di User ID e Password creata secondo le stesse modalità relative all'accesso al sistema Windows. Un identificativo diverso viene associato ad ogni utente, e quindi risulta personale.

L'accesso è controllato anche per l'avvio del software delle postazioni di misura che ha dei criteri di gestione simili al Sistema Operativo della macchina su cui è installato ma non dipendenti dallo stesso.

La formulazione della User ID e della password, oltre che la loro gestione, è identica a quella già illustrata per la User ID e la password di accesso alla rete locale.

7.3 Accesso alle risorse

Le risorse disponibili in azienda e condivise in rete sono essenzialmente stampanti, scanner e file condivisi accentrati in file server aziendali. L'accesso alle risorse suddette è così regolato:

Risorse hardware: Stampanti, Scanner

L'accesso a queste risorse è vincolato all'appartenenza al dominio NT dell'utente.

File

I file condivisi sono su spazio disco di alcuni server aziendali.

L'accesso a tali risorse è regolato dal fatto che l'utente appartenga al dominio NT.

Esistono tre tipologie di accesso:

- accesso libero (per gli utenti del dominio) non regolato da appartenenza a gruppi o reparti;

- accesso regolamentato da appartenenza a reparto;
- accesso nominale a file personali.

La gestione degli accessi ai file aventi accessi regolamentati avviene in base alle responsabilità o agli incarichi di trattamento dati conferiti alla singola persona.

L'accesso alle risorse aziendali è così regolato:

Risorse hardware	Accesso consentito tamite autenticazione sia attaverso i PC con accesso al dominio o alla macchina stand alone, o con user e password per gli strumenti di controllo in laboratorio.
File	Accesso consentito agli utenti appartenenti al dominio o con autorizzazioni a livello di cartelle / archivi in base alle responsabilità e/o incarichi.
Applicazioni	ERP con autenticazione, Microsoft Office con accesso al PC, Acrobat Reader con accesso al PC
Internet	L'accesso ad internet è consentito agli utenti autorizzati. Gli eventuali limiti dell'autorizzazione, per ciascuna Area o ufficio, sono formulati dal Direttore tramite una apposita Comunicazione Interna.

7.4 Accesso remoto

Le risorse disponibili in azienda non sono disponibili dall'esterno tramite collegamenti dedicati via modem. In azienda è presente un apparato di comunicazione che funge da router con un sistema firewall che impedisce l'accesso da remoto.

POS 04 – GESTIONE ANTIVIRUS

INDICE

SCOPO

Lo scopo della presente procedura consiste nell'identificare i compiti, le responsabilità e le modalità operative per la corretta gestione degli strumenti aziendali posti a difesa delle postazioni client e server contro gli attacchi e la diffusione dei virus informatici.

Nell'ambito della gestione del sistema informativo aziendale è necessario predisporre tutte le procedure operative che garantiscano nel tempo la protezione del sistema e che permettano di difendere le postazioni in caso di tentativo di infezione virale da parte di un virus informatico.

In tale contesto, risulta necessario disporre che in tutte le macchine, potenzialmente esposte a pericolo di contagio, sia client che server, siano installati software antivirus commerciali.

CAMPO DI APPLICAZIONE

La presente procedura si applica alla gestione dei software antivirus sia per i Server aziendali sia per tutte le postazioni client, senza distinzione fra fisse e mobili. Si applica inoltre agli strumenti per la protezione da virus informatici veicolati per mezzo della posta elettronica.

RIFERIMENTI NORMATIVI

- D.Lgs. 101 del 4 settembre 2018;
- Direttiva Europea n. 680 del 27 aprile 2016;
- Regolamento Europeo n. 679 del 27 aprile 2016;
- D.Lgs. 196 del 30 giugno 2003 e ss. mm. ii.;
- Provvedimenti del Garante per la Protezione dei dati personali.

RESPONSABILITA'

- <u>Amministratore di Sistema</u>
  - Verifica la corretta applicazione della presente procedura.
  - Compila le istruzioni di lavoro riportanti le attività di dettaglio per l'aggiornamento delle firme virali e dei motori di scansione.
  - Identifica il personale adeguato per lo svolgimento delle attività tecniche.
  - Provvede a che sia correttamente installato e configurato il software e l'hardware sulla base delle esigenze degli utenti finali.

- Predispone le opportune azioni correttive da svolgere per la realizzazione di ulteriori attività in caso di aggiornamenti non effettuati.
- Applica le istruzioni operative contenute nella documentazione tecnica dei prodotti di cui tratta la presente procedura.
- Gestisce eventuali ulteriori attività necessarie per debellare un'infezione virale non completamente contrastata dai software antivirus aziendali (applicazione patch, service pack, ecc...)

TERMINI E DEFINIZIONI

- Virus Informatico

  Una parte di codice o un programma in grado di compromettere o alterare in qualsiasi modo il corretto funzionamento della macchina su cui viene eseguito.

- Software Antivirus

  Un programma, costantemente attivo il cui fine è: monitorare i computer in cui è installato ed intercettare i virus provenienti dall'interno e/o dall'esterno della rete aziendale.

- Amministratore di Sistema

  Ha il compito di sovrintendere alla corretta operatività delle procedure tecniche e di garantire la sicurezza delle informazioni degli elaboratori aziendali.

  È responsabile degli aspetti tecnici e della manutenzione del sistema.

  E' responsabile della corretta configurazione e dell'applicazione delle istruzioni operative descritte nella documentazione allegata ai prodotti antivirus.

- Utente

  Individuo che utilizza, mantiene o gestisce un sistema computerizzato.

- Registro del Sistema (Log Book)

  Registro su cui vengono riportati tutti gli interventi effettuati sul sistema e le anomalie riscontrate citando la data di intervento.

ISTRUZIONI OPERATIVE

Le attività previste nella gestione della sicurezza contro i virus informatici possono essere descritte facendo riferimento alla documentazione resa disponibile dal produttore del software antivirus adottato dalla *S*IImpresa con accesso tramite credenziali in possesso dell'Amministratore di Sistema. Sulla stessa piattaforma, una volta acceduti al sistema, è presente il manuale del prodotto completo.

Suggerimenti e corrette pratiche di utilizzo sono disponibili in forma di FAQ per gli utenti senza credenziali di accesso.

AVG Internet Security

La procedura per la protezione dai virus informatici prevede la pianificazioni delle seguenti operazioni dettagliate nei paragrafi successivi:

- l'installazione del software, definito Agent, su ogni client e workstation;
- l'attivazione degli strumenti per l'aggiornamento delle firme virali;
- il controllo centralizzato da dashboard in remoto dello stato di protezione dei PC.

Si rimanda al manuale operativo del prodotto per la definizione della corretta procedura per l'installazione, configurazione e manutenzione dei componenti.

Tramite la corretta configurazione del software di aggiornamento è possibile mantenere sempre aggiornato sia il file delle definizioni sia il motore delle scansioni, fondamentale per intercettare qualsiasi parte di codice virale.

In caso di virus

Qualora si verifichi la presenza di un virus, malware o altro programma identificato come non sicuro, l'antivirus è configurato per procedere autonomamente alla rimozione del file infettante e alla bonifica del file infetto. Il report delle attività sospette è a disposizione dell'Amministratore di Sistema che può eventualmente interventire sulla macchina infetta qualora il software non sia riuscito ad eliminare il problema.

Come prima azione viene isolato il PC staccandolo dalla rete, si procede con l'accesso al PC in modalità Administrator per verificare le attività presenti sul PC. Successivamente si procede alla scansione approfondita del disco alla ricerca dei file infetti, una volta identificati i file infetti non

rimossi si procede alla cancellazione dei file terminado eventuali programmi attivi che impediscono la cancellazione del file. Terminata la bonifica manuale si procede al riavvio del PC e ad un ulteriore scansione approfondita del disco. Una volta risolto il problema il PC viene ricollegato alla rete facendo accedere l'utente.

Successivamente si procede alla scansione delle cartelle accessibili all'utente sul server o sugli archivi.

Tutte le attività svolte dall'antivirus sono tracciate dallo stesso, eventuali interventi manuali vengono registrati sull'apposito modello "Registro attività antivirus".

POS 05 – BACKUP RESTORE

INDICE

SCOPO

Scopo della presente procedura è quello di definire le modalità di esecuzione per il Back-up ed il Restore di dati e/o applicazioni residenti sui Server aziendali di *S*/Impresa e, ove previsto, su altri sistemi critici "stand alone", in modo da garantire nel tempo il buon funzionamento dei Sistemi e la protezione dei dati raccolti, oltre a permettere rapidamente il ripristino delle attività di servizio in caso di malfunzionamenti.

CAMPO DI APPLICAZIONE

Questa Procedura è applicabile a tutti i sistemi informatici con dati archiviabili.

RIFERIMENTI NORMATIVI

- D.Lgs. 101 del 4 settembre 2018;
- Direttiva Europea n. 680 del 27 aprile 2016;
- Regolamento Europeo n. 679 del 27 aprile 2016;
- D.Lgs. 196 del 30 giugno 2003 e ss.mm.ii.;
- Provvedimenti del Garante per la Protezione dei dati personali.

RESPONSABILITA'

I ruoli e le responsabilità relativamente alla procedura di Backup / Restore sono i seguenti:

Amministratore di Sistema

- Provvede all'adeguata configurazione del software e dell'hardware di back-up sulla base di quanto richiesto dal Responsabile dei Trattamenti dei Dati e, sulla base delle esigenze degli utenti finali, definisce le attività operative di dettaglio (comandi, attivazione di procedure automatizzate, ecc.) da effettuare per l'esecuzione del back-up;
- Predispone le opportune azioni correttive da eseguire per l'esecuzione di ulteriori attività in caso di backup con esito negativo.
- Stabilisce le modalità di archiviazione dei supporti di back-up.

- Verifica la fattibilità e gestisce le richieste di restore per provvedere ad esaudirle nei tempi tecnici più brevi possibili.
- Provvede all'immediata comunicazione dell'avvenuto restore all'utente richiedente.

Responsabile della Protezione dei Dati

- Definisce la lista degli archivi da sottoporre a back-up e relative modalità operative di dettaglio.
- Riporta su un apposito modulo cronologicamente tutte le attività di backup e restore.

TERMINI E DEFINIZIONI

Sistema Computerizzato

Un sistema composto da hardware e software progettato per eseguire una funzione specifica o una serie di funzioni. L'hardware comprende i mainframe, i mini-computer, i personal computer collegati in rete o stand-alone. Il software comprende quello sviluppato internamente e quello fornito da terzi.

Descrizione della procedura di back-up

La procedura di back-up prevede la definizione dei seguenti elementi, che saranno dettagliati nei paragrafi successivi:

- Tipologie di back-up
- Tipologie di dati
- Strategie di back-up
- Periodo di conservazione dei dati di back-up
- Supporti di archiviazione e modalità di conservazione
- Documentazione

Con particolare riferimento ai server, le attività di back-up vengono eseguite direttamente dall'Amministratore di sistema o da persone da lui delegate, sempre comunque sotto la

supervisione dell'Amministratore che deve verificare periodicamente la corretta esecuzione del back-up.

Tipologie di backup

Si possono distinguere le seguenti tipologie di backup:

- **Full backup**: sono salvati tutti i dati, indipendentemente dal fatto che vi siano state modifiche o meno dall'ultimo backup effettuato. E' la modalità più semplice e comoda da gestire in caso di ripristino dei dati ma anche la più dispendiosa in termini di spazio e tempo.

- **Backup differenziale**: sono salvate tutte le informazioni salvate dall'ultimo full backup. In questo modo si riducono le dimensioni del backup ma per il ripristino bisogna avere a disposizione l'ultimo backup completo.

- **Backup incrementale**: è la copia delle sole informazioni modificate dall'ultimo backup eseguito. In questo viene salvato il numero minimo di informazioni ma per il ripristino occorre avere l'ultimo full backup e tutti i backup incrementali precedenti;

- **Clonazione**: viene creata un'immagine completa della partizione o del disco. Questo tipo di back-up permette di sostituire il disco con uno identico senza lacuna modifica ai file o alle configurazioni, non è inoltre necessaria alcuna operazione di estrazione dati da archivi compressi o modificati.

Tipologie di dati

E' possibile distinguere le seguenti tipologie di dati:

Dati statici: sono i dati con basso grado di variabilità.

Dati dinamici: sono i dati con elevato grado di variabilità (dati utenti o derivati da applicazioni).

Database: sono dati strutturati gestiti da specifiche applicazioni. E' importante distinguerli dai dati dinamici in quanto l'applicazione che li gestisce generalmente consente il salvataggio e il recupero dei dati con modalità peculiari.

Strategie di backup

Le attività di backup in *SI*Impresa comprendono il salvataggio dei dati statici, dinamici e dei dati legati a Database. In particolare i Database vengono gestiti come i dati dinamici e salvati come file dati.

Periodo di conservazione dei dati di backup

I backup sono conservati per un periodo variabile a seconda del sistema oggetto di backup, in generale la ritenzione dei dati salvati dal server è di almeno 2 settimane (full back-up) dal momento della loro creazione.

Speciali richieste in merito a dati critici verranno valutate caso per caso e potranno essere gestite da specifiche procedure od istruzioni.

Supporti di archiviazione

Per le macchine virtuali potrà essere adottato un dispositivo di archiviazione di rete avente almeno le seguenti caratteristiche:

Unità di back-up: 1 NAS da 8 dischi da 2Tb in RAID 1

Software di back-up: Backup VMware

Unità oggetto di back-up:

- Intera macchina virtuale procedura manuale/frequenza settimanale

Software di back-up: Cobian Backup 11

Unità oggetto di back-up:

- Data Base ERP/HPLC procedura automatica/frequenza giornaliera
- Documenti su server procedura automatica/frequenza giornaliera
- Documenti su client procedura automatica/frequenza giornaliera

Software di back-up: CloneHD

Unità oggetto di back-up:

- Client/HPLC procedura automatica/frequenza mensile

Per i sistemi "stand alone", ove richiesto, i dati possono essere estratti e masterizzati su un NAS da 2Tb dedicato.

- **Archiviazione fisica:** i supporti per il backup devono essere archiviati a cura del Responsabile della Protezione dei Dati.

  Il disco viene prelevato al termine della giornata lavorativa e custodito in un archivio accessibile solo al personale autorizzato.

  I supporti magnetici sono archiviati in apposito armadio in zona controllata.

- **Archiviazione logica**: l'archiviazione logica delle copie di back-up avviene automaticamente o manualmente con software adeguati, differenti a seconda del sistema/dati da salvare; il back-up è protetto da password complessa, in accordo alla procedura "Accessi logici".

Documentazione

Ogni sistema informatico aziendale dispone di apposita scheda identificativa con numerazione progressiva univoca riportata nel registro dei sistemi aziendali; in essa, qualora sia previsto un criterio di back-up, devono essere riportate le seguenti informazioni:

- identificativo del sistema che effettua il back-up
- hardware utilizzato (marca, modello, caratteristiche principali)
- date, orari e frequenze di back-up (quando)
- dati inclusi nel back-up (che cosa)
- periodo di conservazione (per quanto)
- tipologia di salvataggio (come)
- luogo di conservazione dei supporti di back-up (dove).

L'aggiornamento e la conservazione di questa documentazione sono a carico del Responsabile della Protezione dei Dati e supervisionati dal Responsabile del Trattamento dei Dati.

Descrizione della procedura di restore

Il recupero dei dati dai set di back-up avviene in caso di danneggiamento, perdita o cancellazione (intenzionale o accidentale) di file sulla cartella origine.

Richiesta di restore

La richiesta di una attività di Restore può essere dovuta a:

- Esigenze di servizio e/o problematiche applicative o di sistema (restore di applicazioni, sistema operativo, disaster recovery, ecc.)
- Esigenze dell'utente (cancellazione accidentale o volontaria di file, recupero di dati storici, ecc.)

Nel primo caso la richiesta è gestita direttamente dall'Amministratore di Sistema competente che provvede ad esaudirla nei tempi più opportuni.

Nel secondo caso invece, la richiesta deve essere avanzata dall'utente all'Amministratore di Sistema.

Le informazioni necessarie all'Amministratore di Sistema per procedere sono:

- Autorizzazione preventiva da parte del Responsabile del Trattamento Dati;
- Identità del richiedente, in particolare per dati sensibili, riservati o confidenziali;
- L'esatto percorso dei file da ripristinare;
- La data a cui si desidera ripristinare i file;
- Dove si intendono ripristinare i file (per default si assume che il percorso sia quello di origine);
- Se con il ripristino si debbano sovrascrivere o meno i file preesistenti;
- Data entro cui deve completarsi l'attività.

E' compito dell'Amministratore di Sistema verificare la fattibilità dell'attività di Restore e disporre nei tempi concordati l'esecuzione del Restore.

E' altresì compito dell'Amministratore di Sistema provvedere a dare immediata comunicazione dell'avvenuto Restore all'utente che ne ha fatto richiesta.

Crash Test

Vengono periodicamente effettuati dei crash test che prevedono:

- ripristino funzionalità dei server su nuova macchina;
- ripristino archivi documentali;
- ripristino workstation strumenti analitici.

L'effettuazione dei crash test deve essere programmata almeno 1 volta all'anno.

Registrazione

Tutte le attività di back-up sono registrate dai software che gestiscono il back-up in modalità automatica, i restore devono essere riportati dall'Amministratore di Sistema, nell'apposito modulo, che dovrà contenere i report relativi alle attività. Nel modello verranno riportati i seguenti dati estratti dal file log dell'applicazione di back-up/restore:

- Data di esecuzione del back-up;
- Esito dell'operazione;
- Data di esecuzione del Restore;
- Data del back-up da cui vengono recuperati i file;
- File richiesti, relativo percorso di origine, e di destinazione (se diverso da quello di origine);
- Esito dell'operazione per le attività di restore.

Tabella 1.1 - ELENCO DEI TRATTAMENTI DI DATI PERSONALI

	DESCRIZIONE SINTETICA DEL TRATTAMENTO		NATURA DEI DATI TRATTATI				
Identificativo del trattamento	Finalità del trattamento o attività svolta	Categorie di interessati	SE Dati sensibili	SE Dati giudiziari	STRUTTURA DI RIFERIMENTO - INCARICATO DEL TRATTAMENTO	ALTRE STRUTTURE (ANCHE ESTERNE) CHE CONCORRONO AL TRATTAMENTO	DESCRIZIONE DEGLI STRUMENTI UTILIZZATI
UO FORMAZIONE							
Curriculum allievi dei corsi	Selezione per partecipazione a corsi	Utenti singoli	SI	NO	Ufficio formazione Sanità Maria		Supporto cartaceo
Curriculum docenti dei corsi	Selezione per albo docenti per corsi	Utenti singoli	SI	NO	Ufficio formazione Sanità Maria		Supporto cartaceo+ informatico
Dati anagrafici e numero di personale aziende di tirocinio	Realizzazione tirocini	Imprese	SI	NO	Ufficio formazione Sanità Maria		Supporto cartaceo+ informatico
Foto degli eventi	Realizzazione eventi	Utenti singoli	SI	NO	Ufficio formazione Sanità Maria		Supporto cartaceo+ informatico

Tabella 1.1 - ELENCO DEI TRATTAMENTI DI DATI PERSONALI

	DESCRIZIONE SINTETICA DEL TRATTAMENTO		NATURA DEI DATI TRATTATI				
Identificativo del trattamento	Finalità del trattamento o attività svolta	Categorie di interessati	SE Dati sensibili	SE Dati giudiziari	STRUTTURA DI RIFERIMENTO - INCARICATO DEL TRATTAMENTO	ALTRE STRUTTURE (ANCHE ESTERNE) CHE CONCORRONO AL TRATTAMENTO	DESCRIZIONE DEGLI STRUMENTI UTILIZZATI
UO LABORATORIO							
Segreteria	Dati clienti e fornitori	Fornitori e clienti	SI	NO	Uff. Segreteria LCM: Isacchini Vittorio	Consulente fiscale	Software gestionale, software contabilità mail PEC, archivio cartaceo
Laboratorio	Analisi	Clienti	SI	NO	Amministrazione LCM: Isacchini Vittorio	Tre Laboratori del sistema intercamerale per attività analitiche non eseguibili in Laboratorio	Apparecchiature e software applicativi, archivio cartaceo
Amministrazione Laboratorio	Gestione clienti e fornitori	Gestione contabile e fiscale clienti e fornitori	SI	NO	Amministrazione LCM: Isacchini Vittorio	Consulente fiscale Equitalia Inps, CCIAA Napoli	Software gestione contabilità, mail, PEC, accesso online a INPS ed Equitalia, archivio cartaceo, pacchetto Office
UO CONTABILITA							
Dati anagrafici imprese	Contabilità	Imprese/Clienti/Benificiari	SI	NO	Amministrazione e contabilità: Carraturo Alessandro	Amministrazione / Affari Generali / Formazione / Internazionalizzazione / Comunicazione / Personale / LCM Consulente Fiscale-Lavoro	Cartaceo e digitale Software contabilità Server / NAS
Dati personali	Contabilità	Imprese/Clienti/Benificiari	SI	NO	Amministrazione e contabilità: Carraturo Alessandro	Amministrazione / Affari Generali / Formazione / Internazionalizzazione / Comunicazione /	Cartaceo e digitale Software contabilità Server / NAS

Tabella 1.1 - ELENCO DEI TRATTAMENTI DI DATI PERSONALI

	DESCRIZIONE SINTETICA DEL TRATTAMENTO		NATURA DEI DATI TRATTATI				
Identificativo del trattamento	Finalità del trattamento o attività svolta	Categorie di interessati	SE Dati sensibili	SE Dati giudiziari	STRUTTURA DI RIFERIMENTO - INCARICATO DEL TRATTAMENTO	ALTRE STRUTTURE (ANCHE ESTERNE) CHE CONCORRONO AL TRATTAMENTO	DESCRIZIONE DEGLI STRUMENTI UTILIZZATI
						Personale / LCM Consulente Fiscale-Lavoro	
Dati finanziari	Contabilità	Imprese/Clienti/Benificiari	SI	NO	Amministrazione e contabilità: Carraturo Alessandro	Amministrazione / Affari Generali / Formazione / Internazionalizzazione / Comunicazione / Personale / LCM Consulente Fiscale-Lavoro	Cartaceo e digitale Software contabilità Server / NAS
UO PROGETTI E ATTIVITA' DI SUPPORTO ALLE AZIENDE							
Scheda Registrazione utenza (*Intake assessment*)	Registrazione utenti richiedenti servizi informativi EEN: rilevazioni: dati anagrafici, economici, richiesta del servizio, elaborazione e risposta	Persone fisiche e giuriche	SI	NO	Ufficio progetti e attività di supporto alle Aziende: Raffone M.C.		Scheda Registrazione cartacea Armadi archivio utenza Posta elettronica Personal computer
Richiesta Informazioni	Registrazione utenti richiedenti servizi informativi EEN: rilevazioni dati anagrafici, economici	Persone fisiche e giuriche	SI	NO	Ufficio progetti e attività di supporto alle Aziende: Raffone M.C.		Scheda registrazione in formato World o cartacea Posta elettronica (e-mail generale SI IMPRESA , funzionar competenti) Portale web SI IMPRESA
Scheda registrazione servizio EEN POD	Registrazione nella banca dati on line della Commissione europea del profilo richiesta partner commerciali	Persone giuriche	SI	NO	Ufficio progetti e attività di supporto alle Aziende: Raffone M.C..	EASME /CE (Belgio)	Scheda Registrazione in formato World o cartacea Portale web SI IMPRESA area intranet Portale EASME web intranet: https://een.ec.europa.eu/

Tabella 1.1 - ELENCO DEI TRATTAMENTI DI DATI PERSONALI

	DESCRIZIONE SINTETICA DEL TRATTAMENTO		NATURA DEI DATI TRATTATI				
Identificativo del trattamento	Finalità del trattamento o attività svolta	Categorie di interessati	SE Dati sensibili	SE Dati giudiziari	STRUTTURA DI RIFERIMENTO - INCARICATO DEL TRATTAMENTO	ALTRE STRUTTURE (ANCHE ESTERNE) CHE CONCORRONO AL TRATTAMENTO	DESCRIZIONE DEGLI STRUMENTI UTILIZZATI
Scheda registrazione Business review	Registrazione utenti aderenti servizio Business Review e richiedenti servizi informativi EEN: rilevazioni dati anagrafici, economici	Persone giuriche	SI	NO	Ufficio progetti e attività di supporto alle Aziende: Raffone M.C.		Scheda Registrazione in formato World o cartacea Portale IMT web intranet: http://res.ivf.se/bridgeconomies/
Scheda registrazione eventi del tipo Brokerage Event/ company mission in ambito EEN	Registrazione utenti aderenti servizio: rilevazioni dati anagrafici, economici, professionali, etc. Gestione degli incontri b2b (domande e richieste di) Follow up distanziati nel tempo via email	Persone fisiche e giuriche	SI	NO	Ufficio progetti e attività di supporto alle Aziende: Raffone M.C.	Portale web "B2Match"il cui uso è consentito da EASME /CE	Scheda registrazione in formato World o cartacea oppure on line fornito da B2Match (su incarico a pagam.)
Scheda registrazione eventi vari: seminari, corsi di formazione, workshop, incontri b2b	Registrazione utenti aderenti servizio: rilevazioni dati anagrafici, economici, professionali, etc.	Persone fisiche e giuriche	SI	NO	Ufficio progetti e attività di supporto alle Aziende: Raffone M.C..		Scheda Registrazione in formato World o cartacea Posta elettronica

Tabella 1.2. ***ANALISI DEI RISCHI CHE INCOMBONO SUI DATI***

RISCHI	SÌ/NO	DESCRIZIONE DELL'IMPATTO SULLA SICUREZZA (GRAVITÀ: ALTA/MEDIA/BASSA)
RISCHI CONSEGUENTI A COMPORTAMENTI DEGLI OPERATORI		
SOTTRAZIONE DI CREDENZIALI DI AUTENTICAZIONE	SÌ	BASSO
CARENZA DI CONSAPEVOLEZZA, DISATTENZIONE O INCURIA	SI	MEDIO – SI STANNO SENSIBILIZZANDO GLI OPERATORI SULLA DELICATEZZA DELLA GESTIONE USER/PW PER L'ACCESSO AI SISTEMI
COMPORTAMENTI SLEALI O FRAUDOLENTI	NO	NON ESISTONO PRECEDENTI NOTI DI COMPORTAMENTI DEL GENERE
ERRORE MATERIALE	SÌ	BASSO - GLI OPERATORI SONO SENSIBILIZZATI SULLE PROCEDURE OPERATIVE
RISCHI CONSEGUENTI AD EVENTI RELATIVI AGLI STRUMENTI		
AZIONE DI VIRUS INFORMATICI O DI PROGRAMMI SUSCETTIBILI DI RECARE DANNO	SI (NO CODICE MALIZIOSO - NO DIALERS)	BASSO - ACCESSO RETE INTRANETE/INTERNET; ACCESSO MEDIANTE E-MAIL; ACCESSO MEDIANTE SUPPORTI DI MEM. (FLOPPY, IN PARTICOLARE). INCIDENZA BASSA PERCHÉ ACCESSO E' LIMITATO E BEN CONTROLLATO IL SISTEMA
SPAMMING O TECNICHE DI SABOTAGGIO	COME SOPRA	BASSO - COME SOPRA
MALFUNZIONAMENTO, INDISPONIBILITÀ O DEGRADO DEGLI STRUMENTI	SI	BASSO – GLI STRUMENTI OBSOLETI SONO SOSTITUITI PERIODICAMENTE
ACCESSI ESTERNI NON AUTORIZZATI	SI	MOLTO BASSO – LA RETE INTRANET E' CONTROLLATA DA ACCESSI AUTORIZZATI TRAMITE FIREWALL
INTERCETTAZIONE DI INFORMAZIONI IN RETE	NO	LE CONNESSIONI SULLE BANCHE DATI SONO EFFETTUATE SU PROTOCOLLI SICURI DI COMUNICAZIONE
RISCHI CONSEGUENTI AD EVENTI RELATIVI AL CONTESTO		
ACCESSI NON AUTORIZZATI A LOCALI/REPARTI AD ACCESSO RISTRETTO	NO	I LOCALI AD ACCESSO RISTRETTO SONO CHIUSI A CHIAVE. Il MATERIALE E' CONTENUTO IN ARMADI CHIUSI A CHIAVE. DURANTE L'ORARIO DI LAVORO I LOCALI SONO PRESIDIATI DAI DIPENDENTI DELL'UFFICIO. FUORI L'ORARIO DI LAVORO I LOCALI SONO CHIUSI A CHIAVE.
SOTTRAZIONE DI STRUMENTI CONTENENTI DATI	SI	BASSO – LIMITATO L'ACCESSO AI LOCALI CON STRUMENTI CONTENENTI DATI
EVENTI DISTRUTTIVI, NATURALI O ARTIFICIALI	SI	BASSO – LA PREVENZIONE PER POSSIBILI EVENTI AMBIENTALI

Tabella 1.2. ***ANALISI DEI RISCHI CHE INCOMBONO SUI DATI***

(MOVIMENTI TELLURICI, SCARICHE ATMOSFERICHE, INCENDI, ALLAGAMENTI, CONDIZIONI AMBIENTALI, ETC…), NONCHÉ DOLOSI, ACCIDENTALI O DOVUTI AD INCURIA		E' ATTUATA IN BASE AL D.LG.VO N. 81/2008.
GUASTO AI SISTEMI COMPLEMENTARI (IMPIANTO ELETTRICO, CLIMATIZZAZIONE, ETC…)	SI	MEDIO – GLI APPARATI E MACCHINARI DI RETE (SERVER, HUB, ROUTER) DEVONO ESSERE DOTATI DI APPOSITI GRUPPI DI CONTINUITA'
ERRORI UMANI NELLA GESTIONE DELLA SICUREZZA FISICA	SI	MEDIO – VENGONO SENSIBILIZZATI I DIPENDENTI SULLE PRECAUZIONI DA ADOTTARE

Tabella 1.3 ***PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI***

DESCRIZIONE SINTETICA DEGLI INTERVENTI FORMATIVI	CLASSI DI INCARICO O TIPOLOGIE DI INCARICATI	TEMPI PREVISTI
Specifici interventi formativi degli incaricati del trattamento, finalizzati alla trasmissione della conoscenza: 1. dei rischi che incombono sui dati 2. delle misure disponibili per prevenire eventi dannosi 3. dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività 4. delle responsabilità che ne derivano 5. delle modalità per aggiornarsi sulle misure minime adottate dal titolare	**TUTTO IL PERSONALE**	**ENTRO IL 31.10.2018**
La formazione viene programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali	**TUTTO IL PERSONALE**	**ENTRO 30 GIORNI** dall'assunzione in servizio dal cambiamento delle mansioni dall'introduzione di nuovi strumenti