ISMS

Information Security Management System

Ai sensi della ISO/IEC 27001:2017

Manuale Sistema di Gestione della Sicurezza delle Informazioni (MGSI)

NETCOM ENGINEERINGS.p.a.

Sede Legale e Operativa : Via Nuova Poggioreale, C.tro Polif. T7 - Napoli
P.IVA IT07277340639

Nota:
Nessuna parte di questo documento può essere riprodotta o trasmessa in qualsiasi forma e con qualsiasi mezzo, elettronico o altro, compresa la fotocopia, la ristampa, o di registrazione, per qualsiasi scopo senza il consenso scritto della NETCOM ENGINEERINGS.p.a..

Storia delle modifiche

Edizione	Revisione	Data di emissione	Sintesi delle variazioni	Redatto	VERIFICATO	APPROVATO
1	**00**	04.02.2019	Prima emissione	RISMS	DG	DG
1	**01**	13.03.2020	Aggiornamento Sede Legale	RISMS	DG	DG

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

INDICE

0. INTRODUZIONE
   a. Generalità
   b. Approccio per processi
   c. Compatibilità con altri sistemi di gestione
1. SCOPO E CAMPO DI APPLICAZIONE
   a. Generalità
   b. Applicazione
2. RIFERIMENTI NORMATIVI
3. TERMINI E DEFINIZIONI
4. SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI
   4.1 REQUISITI GENERALI
   4.2 STABILIRE E GESTIRE IL ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM)
      4.2.1.a: SCOPO
      4.2.1.b: DEFINIZIONE DELLA POLITICA
      4.2.1.c: DEFINIZIONE APPROCCIO SISTEMATICO ALLA VALUTAZIONE DEL RISCHIO
      4.2.1.d: IDENTIFICAZIONE DEL RISCHIO
      4.2.1.e: VALUTAZIONE DEL RISCHIO
      4.2.1.f: VALUTAZIONI DELLE OPZIONI PER IL TRATTAMENTO DEL RISCHIO
      4.2.1.g: SELEZIONE DEI CONTROLLI PER IL TRATTAMENTO DEI RISCHI
      4.2.1.h: PREPARAZIONE DI UNA DICHIARAZIONE DI APPLICABILITA'
         4.2.2 ISTITUZIONE E ATTUAZIONE DELL'ISMS
         4.2.3 SORVEGLIANZA E RIESAME DELL'ISMS
         4.2.4: MANTENIMENTO E MIGLIORAMENTO DELL'ISMS
   4.3 REQUISITI RELATIVI ALLA DOCUMENTAZIONE
      4.3.1: GENERALITA'
      4.3.2: CONTROLLO DELLA DOCUMENTAZIONE
      4.3.3: CONTROLLO DELLE REGISTRAZIONI
5. RESPONSABILITA' DELLA DIREZIONE
      5.1: IMPEGNO DELLA DIREZIONE
      5.2: GESTIONE DELLE RISORSE
         5.2.1: MESSA A DISPOSIZIONE DELLE RISORSE
         5.2.2: ADDESTRAMENTO, CONSAPEVOLEZZA E COMPETENZA
6. VERIFICHE ISPETTIVE INTERNE (AUDIT INTERNI)
7. RIESAME DA PARTE DELLA DIREZIONE
      7.1: GENERALITA'
      7.2: ELEMENTI IN INGRESSO PER IL RIESAME
      7.3: ELEMENTI IN USCITA PER IL RIESAME
8. MIGLIORAMENTO DELL'ISMS
      8.1: MIGLIORAMENTO CONTINUO
      8.2: AZIONI CORRETTIVE
      8.3: AZIONI PREVENTIVE

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

Introduzione
a: Generalità

A causa della fenomenale crescita nell'utilizzo delle IT ed applicazioni IT è cresciuta la necessità di gestire i controlli di sicurezza di tutti i sistemi di informazione. La sicurezza dei sistemi informativi assume una grande importanza per il successo di un'organizzazione, come la sopravvivenza dell'organizzazione dipende dalla precisione, la velocità e l'affidabilità del flusso di informazioni da essa gestito. Ogni abuso non autorizzato così come accidentale di informazioni o del sistema informativo può provocare la perdita finanziaria, discontinuità di business, la reputazione danneggiata, divulgazione impropria, cause legali e non conformità con le disposizioni normative, ecc. Pertanto, una costante vigilanza insieme ad una informazione ampia e corretta applicazione programma di gestione della sicurezza è il requisito minimo per la consegna efficace del servizio dell'organizzazione e il costante apporto alla crescita economica.

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

b: Approccio per processi

Il presente manuale si basa sull'approccio per processi noto come "Plan-Do-Check-Act" (PDCA), che viene applicato per strutturare tutti i processi del SGSI. La figura 1 illustra come un SGSI assuma come elementi in ingresso i requisiti per la sicurezza delle informazioni e le aspettative delle parti interessate e come, attraverso le necessarie azioni e processi, fornisca i risultati per la sicurezza delle informazioni che soddisfino tali requisiti e aspettative.

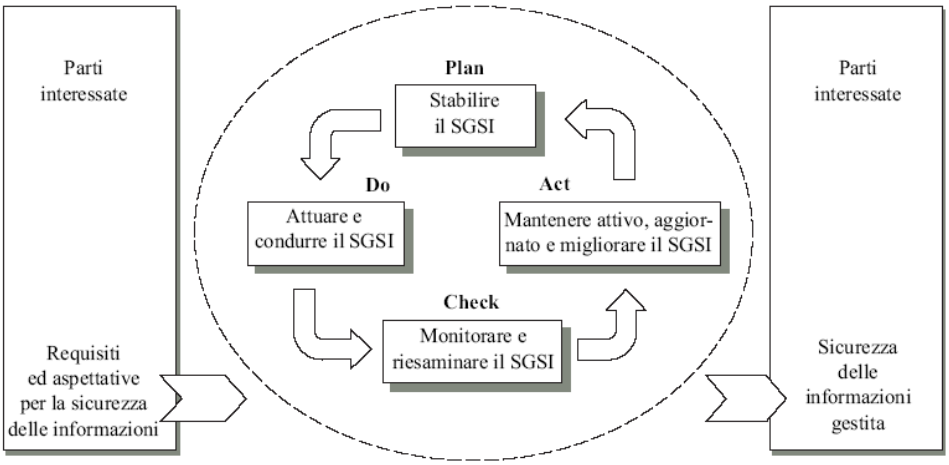


Figura 1

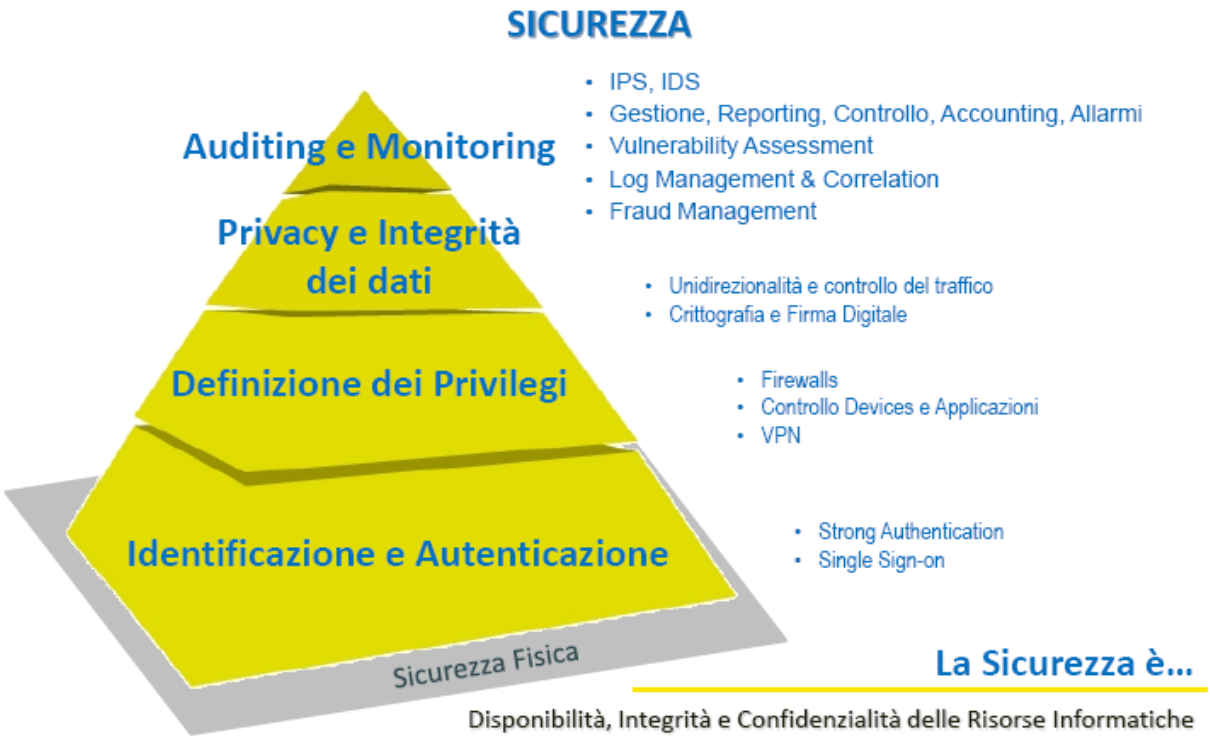
Processi - Attività ed Output delle fasi del ciclo di vita del S.G.S.I.

FASI	PROCESSI	ATTIVITA'
Pianificare (Plan) Descritta nella norma nel paragrafo 4.2.1	**Stabilire il contesto dell'SGSI & Valutazione del Rischio**	· Definire lo scopo dell'SGSI e le regole · Definire un approccio sistematico alla valutazione del rischio · Identificare i rischi · Aplicare l'approccio sistematico per valutare i rischi · Identificare e valutare le scelte per il trattamento dei rischi · Scegliere controlli oggettivi e controlli per il trattamento dei rischi
Fare (Do) Descritta nella norma nel paragrafo 4.2.2	***Progettare e Implementare l'SGSI***	· Misurare le performance dell'SGSI · Identificare i miglioramenti nell'SGSI e implementarle effettivamente · Prendere azioni correttive e preventive appropriate · Comunicare i risultati e le azioni e consultarsi con tutte le parti coinvolte · Revisionare l'SGSI dove necessario · Assicurarsi che le revisioni raggiungano gli scopi loro designati

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

Controllare (Check) Descritta nella norma nel paragrafo 4.2.3	***Controllare ed esaminare l'SGSI***	· Eseguire le procedure e altri controlli (p.e. per scoprire errori, identificare invasioni riuscite e non riuscite) · Intraprendere regolari revisioni dell'efficacia dell'SGSI · Esaminare il livello di rischio residuo e del rischio accettabile · Eseguire procedure · Implementare un programma specifico di controllo · Implementare controlli che sono stati scelti · Gestire le operazioni · Gestire le risorse · Implementare le procedure e altri controlli dei procedimenti · Esaminare una revisione formale del proprio SGSI su base regolare · Registrare e scrivere il report di tutte le azioni ed eventi
Agire (Act) Descritta nella norma nel paragrafo 4.2.1	**Migliorare l'SGSI**	· Implementare un programma specifico di controllo · Implementare controlli che sono stati scelti · Gestire le operazioni · Gestire le risorse · Implementare le procedure e altri controlli dei procedimenti

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.



<u>La struttura organizzativa dell'azienda NETCOM ENGINEERINGS.p.a.</u>

NetCom Engineeringè l'espressione integrata di imprese presenti sul mercato da diversi anni: Core Informatica, Media Motive, Netcom Industry, Netcom Sistemi. Il Gruppo nasce come naturale evoluzione dell'incontro di queste esperienze imprenditoriali.

L'azienda ha un trend di crescita in decisa ascesa e punta a consolidare il posizionamento nei mercati tradizionali, oltre che ad esplorare e a penetrare le nuove opportunità di sviluppo nel mercato globale.

MISSION

Co-responsabilità nella crescita dei clienti, fornendo soluzioni e supporto realizzativo ai progetti di sviluppo;

Contributo, in approccio sistemico, alla crescita dei mercati di riferimento;

Attenzione, alla crescita di tutti i collaboratori, promuovendone il benessere professionale e motivandoli a raggiungere performance sempre migliori.

Obiettivo primario del Gruppo è sostenere le aziende nelle loro quotidiane attività di ideazione creazione e sviluppo di nuovi prodotti e servizi con lo scopo di "Produrre valore in ogni azione".

VISION

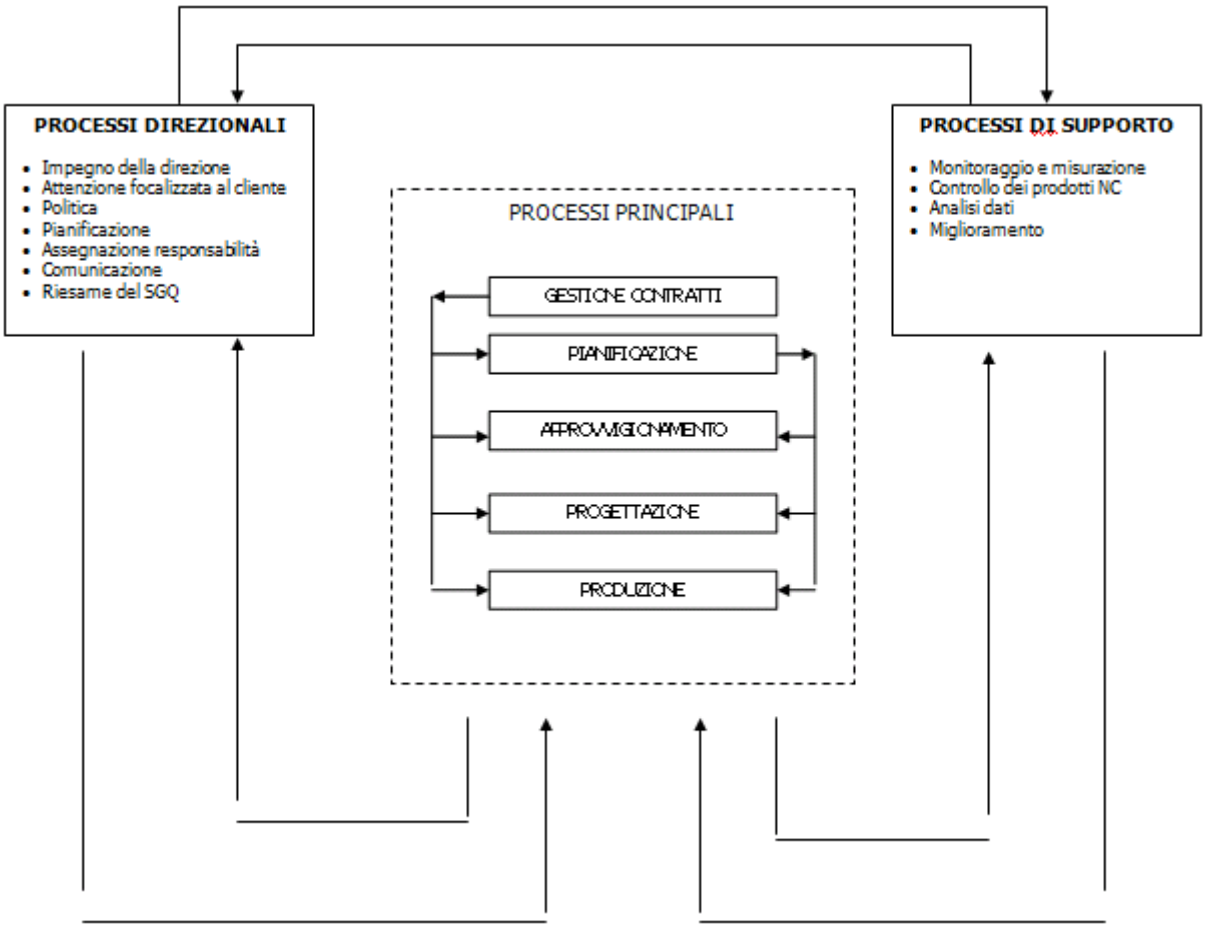
Alle origini di ogni grande gruppo, c'è sempre un grande sogno che per divenire realtà deve alimentarsi con il talento.

Competitività, solidità e credibilità: idee orientate alla crescita.

Lo scopo è essere innovativi e proattivi in un confronto e un dialogo totale con tutti gli stakeholders interessati a costruire e a perseguire risultati eccellenti. "Gente che lavora felice e un lavoro che rende felici"La struttura organizzativa complessiva della società NETCOM ENGINEERINGS.p.a. è come mostrato nell'allegato organigramma.

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

Breve descrizione dei processi della NETCOM ENGINEERINGS.p.a.:



Flusso delle informazioni e dei dati/interazione tra i processi

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

Il catalogo dei servizi comprende:

- *Progettazione, sviluppo, manutenzione e gestione software.*
- *Consulenza informatica*

c: Compatibilità con altri sistemi di gestione

Il SGSI è compatibile con il Sistema di Gestione per la Qualità secondo lo standard ISO 9001:2015 con cui condivide alcune procedure ed istruzioni.

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

0. SCOPO E CAMPO DI APPLICAZIONE

a: Generalità

Il presente manuale è stato elaborato allo scopo di fornire un modello per stabilire, attuare, condurre, monitorare, riesaminare, mantenere attivo, aggiornare e migliorare un sistema di gestione per la sicurezza delle informazioni (SGSI). L'adozione di un SGSI è da parte della NETCOM ENGINEERINGS.p.a. una scelta strategica. La progettazione e l'attuazione di un SGSI sono influenzate dalle esigenze e dagli obiettivi, dai requisiti di sicurezza, dai processi utilizzati e dalla dimensione e struttura dell'organizzazione.

Il presente Manuale specifica i requisiti di un sistema di gestione per la sicurezza delle informazioni adottato dalla società per:

- Stabilire
- Attuare
- Condurre
- Monitorare
- Riesaminare
- Aggiornare
- Migliorare

b: Applicazione

Il presente Manuale di gestione per la sicurezza delle informazioni (MGSI) si applica al seguente scopo:

- **Progettazione, sviluppo, manutenzione e gestione software.**
- **Consulenza informatica**

Il SGSI si applica al momento alle sole sedi di Napoli ove risiede fisicamente il CED aziendale.

Via Nuova Poggioreale, C.tro Polif. T7 piano 5 – Napoli
Via Nuova Poggioreale, C.tro Polif. T7 piano 6 – Napoli

Non è applicabile il controllo A.06.02.02 Telelavoro in quanto l'azienda non ha contratti di telelavoro.

Il programma di gestione delle informazioni di sicurezza è costituito dalle politiche di sicurezza ben definite e documentate, da standard e linee guida per la gestione del rischio. La conformità e la affidabilità del sistema di gestione delle informazioni è garantito, inoltre, dall'uso di adeguate e corrette pratiche commerciali nonché di meccanismi di sicurezza adeguati.

Questo manuale descrive la politica di sicurezza delle informazioni della NETCOM ENGINEERINGS.p.a.. Il sistema di gestione delle informazioni è stato progettato per garantire che tutte le prescrizioni relative al Sistema di Gestione Sicurezza delle Informazioni siano riconosciute e che l'attuazione sia coerente ed uniforme con i requisiti della norma ISO 27001.
La politica di sicurezza si focalizza sui seguenti ambiti:

• **Sistema di sicurezza del computer**: In riferimento a CPU, periferiche e sistemi operativi. Ciò include la sicurezza dei dati.
• **Sicurezza fisica**: Relativamente ai locali occupati dagli addetti e dalle attrezzature.

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

• **Sicurezza di funzionamento**: Impianti di alimentazione, attività di funzionamento.
• **Sicurezza procedurali:** Relativamente alla gestione del personale e degli utenti.
• **Sicurezza delle comunicazioni**: Comunicazioni relative alle attrezzature, al personale, alle vie di trasmissione, ed alle aree fisiche adiacenti.

I requisiti di sicurezza derivano da tre fonti principali:

1. La valutazione dei rischi. Attraverso una attenta valutazione dei rischi, le minacce ai beni sono identificate, la vulnerabilità definita, le probabilità di accadimento valutate e l'impatto potenziale è stimato.
2. Un'altra fonte sono i requisiti di legge, regolamentari e contrattuali che l'organizzazione, i partner commerciali, appaltatori e fornitori di servizi devono soddisfare e rispettare
3. Un'ulteriore fonte è il particolare insieme di principi, obiettivi e requisiti aziendali per l'elaborazione delle informazioni che l'organizzazione ha messo a punto per sostenere le sue attività.

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

2. RIFERIMENTI NORMATIVI

- ✓ ISO/IEC 27000 Principi e vocabolario;
- ✓ ISO/IEC 27001 Requisiti per un Sistema di Gestione per La Sicurezza delle Informazioni (Ed 2017) ;
- ✓ ISO/IEC 27002 Linea guida – Raccomandazioni per un Sistema di Gestione per La Sicurezza delle Informazioni (Ed.2017);
- ✓ D.lgs. 196/2003 cosi come aggiornato dal Reg.UE 2016/679 e D.lgs 101/2018
- ✓ ISO 19011:2018 Linee guida per audit di sistemi di gestione
- ✓ D.lgs 235/2010, modifiche al Codice dell'Amministrazione Digitale 82/2005 con introduzione della valenza 2702 de c.c. per la firma elettronica avanzata relativi aggiornamenti
- ✓ DPCM 22 Febbraio 2013 sulla firma elettronica avanzata e relativi aggiornamenti
- ✓ [doc. web n. 3132642] Schema di provvedimento in tema di riconoscimento biometrico e firma grafometrica relativi aggiornamenti

Computer Crime

- ✓ Legge 547 del 1993, sul computer crime.
- ✓ Legge 48 del 2008, di ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica, firmata a Budapest il 23 novembre 2001. La Convenzione costituisce il primo accordo internazionale riguardante i crimini commessi attraverso internet o altre reti informatiche. La Convenzione estende la portata del reato informatico includendo tutti i reati in qualunque modo commessi mediante un sistema informatico, anche nel caso in cui la prova del reato sia sotto forma elettronica.
- ✓ Dlgs 373 del 2000, sulla tutela dei servizi ad accesso controllato.
- ✓ Sentenza 4 del 21 aprile 2000 (file 2000_sentenza_RAI.pdf), che assolve l'imputato per accesso non autorizzato al sistema informatico del GR1 della RAI perché il sistema non è stato valutato "sufficientemente protetto".
- ✓ Legge 281 del 2006, di conversione del Decreto Legge 259/2006, sulle intercettazioni telefoniche illegali.
- ✓ Sentenza 175 del 2006 del Tribunale di Chieti (file 2006_Sentenza_175_Tribunale_Chieti.pdf), che fa chiarezza sulla controversa questione dell'acquisizione delle "prove informatiche": si devono rispettare le norme del codice di procedura penale che disciplinano la formazione della prova.
- ✓ Legge 269 del 1998, modificata dalla Legge 38 del 2006, sulla pornografia. I requisiti tecnici che dovranno essere adottati dagli ISP sono descritti dal Decreto Interministeriale del 8 gennaio 2007 (file 2007-01-29-Req-tecnici-pedopornografia.pdf).

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

✓

✓ **Responsabilità amministrativa delle imprese**

✓

✓ Decreto Legislativo 231 del 2001, più volte modificato. Introduce la responsabilità in sede penale degli enti, che si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto illecito. Precedentemente gli amministratori e le società non pativano conseguenze per reati commessi dal personale. Con questo Decreto Legislativo gli organi dirigenti non incorrono nelle sanzioni se applicano modelli organizzativi atti a prevenire taluni reati.

✓ Decreto 201 del 2003 del Ministero della Giustizia. Reca il regolamento previsto dall'articolo 85 del Decreto Legislativo 231 del 2001. Specifica le modalità di formazione e tenuta dei fascicoli degli uffici giudiziari; i compiti ed il funzionamento dell'Anagrafe nazionale e soprattutto le modalità di presentazione, di esame, di valutazione dell'efficacia dei codici di comportamento previsti per mitigare le sanzioni a carico degli enti.

✓

✓ Normativa Privacy

✓

✓ Per consultare la normativa in materia di protezione dei dati personali (o "privacy"), si segnala il sito del Garante italiano (http://www.garanteprivacy.it).

✓

✓ Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (detto anche "GDPR" o "General data protection regulation" o "Regolamento europeo sulla privacy"), il testo base in materia di Privacy;

✓ Decreto Legislativo 196 del 2003 ("Codice in materia di protezione dei dati personali"), che, con le modifiche apportate dal D. Lgs. 101 del 2018, rappresenta l'integrazione del GDPR nell'ordinamento italiano;

✓ Il GDPR è accompagnato da una Direttiva per il trattamento dei dati da parte delle "autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali"; la Direttiva è stata recepita nell'ordinamento italiano con il D. Lgs. 51 del 2018;

✓ La normativa italiana è integrata ulteriormente da normativa secondaria, la cui applicabilità dovrà essere rivalutata entro fine 2018:

✓ Provvedimenti generali (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3755203);

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

✓ Codici di deontologia (Allegati da A.1 a A.7 del Codice privacy; https://www.garanteprivacy.it/web/guest/codice);

✓ Autorizzazioni generali al trattamento delle categorie particolari di dati personali (https://www.garanteprivacy.it/web/guest/home/provvedimenti-normativa/provvedimenti/autorizzazioni);

✓ Linee guida (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1772725);

✓ Importanti sono le "Opinion" dell'European Data Protection Board (o EDPB); si trovano sul sito del Garante (https://www.garanteprivacy.it/web/guest/regolamentoue) e, in più lingue, dell'EDPB (https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_it);

✓ Legge 300 del 1970, Statuto dei Lavoratori: limita le possibilità di controllo a distanza dei lavoratori da parte del datore di lavoro;

✓ Sentenza del 20 giugno 2006 del Tribunale Ordinario di Torino, Sezione distaccata di Chivasso relativa alla possibilità, da parte del datore di lavoro, di accedere alla casella personalizzata del dipendente (file 2006_06_20-sentenza-mailbox-aziendale.pdf>;

✓ Provvedimento sulla localizzazione di veicoli aziendali, con ulteriori link ad altri provvedimenti su questa materia (https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9023246).

✓

✓ **Diritto d'Autore**

✓

✓ Legge 633 del 1941, governa il Diritto d'autore in Italia ed è stata modificata parecchie volte nel corso degli anni. Qui di seguito sono proposte le disposizioni più significative dal punto di vista dell'informatica:

✓ Dlgs 518/1992 di attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore.

✓ Dlgs 169/1999, di attuazione della direttiva 96/9/CE relativa alla tutela giuridica delle banche di dati.

✓ Dlgs 68/2003, di attuazione della direttiva 2001/29/CE.

✓ DL "Urbani" 72/2004 convertito in legge dalla L. 128/2004.

✓ Legge 43/2005, che converte il Decreto Legge 7 del 2005.

✓ Decreto Legislativo 118/2006 di attuazione della direttiva 2001/84/CE.

✓ Decreto Legislativo Dlgs 140/2006 attuazione della direttiva 2004/48/CE.

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

✓ Legge 2 del 2008, che prevede la possibilità di pubblicare senza oneri su Internet materiale a uso didattico o scientifico.

✓ Dlgs 373 del 2000, sulla tutela dei servizi ad accesso controllato.

✓ Dlgs 30 del 2005, Codice della proprietà industriale.

✓ Regolamento di attuazione del Codice della proprietà industriale, emesso con il Decreto 33 del 13 gennaio 2010 del Ministero dello Sviluppo Economico.

✓ DPCM 31 del 2009, tratta del "bollino" SIAE da apporre sui supporti come cd dvd ecc.

✓

✓ **Normativa sulla Firma digitale e Gestione documentale**

✓

✓ D.Lgs. 82 del 2005 o "Codice dell'Amministrazione Digitale" (più volte modificato, più recentemente dal Dlgs 235 del 2010), norma di riferimento per quanto riguarda la firma digitale. Attua quanto previsto dall'articolo 15, comma 2 della legge del 15 marzo 1997, n. 59 e rappresenta l'adeguamento italiano alla Direttiva Europea 1999/93/CE. Questo Decreto Legislativo, inoltre, regolamenta il Sistema Pubblico di Connettività (SPC).

✓ DPR 445/2000, il precedente riferimento per la firma digitale, ora ridotto alle sole parti concernenti la gestione di atti e documenti nell'ambito della Pubblica Amministrazione;

✓ Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno: questo abroga la direttiva 1999/93/CE e quindi parte del D.Lgs. 82, secondo modalità non ancora stabilite.

✓

✓ Da un punto di vista tecnico, sono in vigore i seguenti provvedimenti, eventualmente richiesti da norme abrogate ma tuttora validi:

✓

✓ Norme sulla dematerializzazione della documentazione:

✓ DPCM del 22 febbraio 2013: Regole tecniche in materia di generazione, apposizione e verifi ca delle fi rme elettroniche avanzate, qualificate e digitali (di cui all'articolo 71 del D.Lgs.82); sostituisce i precedenti DPCM del 13 gennaio 2004 e del 30 marzo 2009.

✓ Deliberazione CNIPA n. 45 del 2009 (scaricabile nella versione consolidata con le modifiche del 2010 da www.digitpa.gov.it): regole per il riconoscimento e la verifica del documento informatico a

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

cui attenersi a norma del DPCM del 30 marzo 2009; sostituisce la precedente deliberazione CNIPA 4/2005.

✓ DPCM del 30 ottobre 2003 (file 2003_DPCM_30_ottobre_schema_cert_sic.pdf): schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione.

✓ Deliberazione CNIPA 11/2004 e note esplicative (scaricabile da www.digitpa.gov.it): regole tecniche per la riproduzione e conservazione di documenti su supporto ottico.

✓ Norme applicabili alla Pubblica Amministrazione:

✓ D.P.C.M. 31 ottobre 2000: regole tecniche per il protocollo informatico della Pubblica Amministrazione.

✓ Delibera AIPA n. 51 del 2000 (file 2000_delibera_AIPA_51_PA.pdf): regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni (apparentemente, questa delibera non è più in uso e quindi, forse, implicitamente abrogata).

✓ DPCM del 1 aprile 2009 sulle regole di sicurezza della SPC

✓

✓ **Norme sulla posta elettronica certificata (PEC):**

✓ DPR 68 del 2005: regolamento per l'utilizzo della posta elettronica certificata (PEC).

✓ Decreto del novembre 2005 della Presidenza del Consiglio dei Ministri e relativo Allegato: regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata.

✓ Legge "anti-crisi" 2/2009 (di conversione del DL 185/2008): modifica il DPR 68 del 2005 e rende obbligatorio l'uso della PEC ad alcuni soggetti dal novembre 2011.

✓ ulteriori regolamenti sul sito www.digitpa.gov.it

✓ Norme relative alle firme elettroniche (un elenco più esaustivo e aggiornato è mantenuto da AgID sul proprio sito, alla voce Home - Agenda Digitale - Infrastrutture e architetture - Firme elettroniche):

✓ Deliberazione CNIPA n. 45 del 2009 (scaricabile nella versione aggiornata da www.digitpa.gov.it): specifiche tecniche per garantire l'interoperabilità tra i diversi certificatori.

✓ Circolare CNIPA 48 del 2005 (scaricabile da www.digitpa.gov.it): modalità per presentare la domanda di iscrizione nell'elenco pubblico dei certificatori.

✓ **Norme applicabili alla fatturazione elettronica**:

✓ Decreto Legislativo 52 del 2004: modalità di fatturazione elettronica (richiama la circolare AIPA 42 sostituita dalla Deliberazione CNIPA 11/2004).

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

✓ Decreto del Ministero dell'Economica e delle Finanze del 23 gennaio 2004 (file 2004_decr_min_eco_23_gennaio_fiscali_doc_informatici.pdf.

✓ Norme sulla Carta Nazionale dei Servizi:

✓ D.P.R. 117 del 2004: regolamento sulla carta nazionale dei servizi.

✓ Decreto interministeriale del 9 dicembre 2004 (file 2004_decreto_9_dicembre.pdf: regole tecniche relative alla carta nazionale dei servizi.

✓

✓ Sentenza della Corte di Cassazione del 19 febbraio 2008: conferma la validità di una comunicazione via e-mail. Anche se con riferimenti a dispositivi ormai abrogati, risulta essere un precedente interessante (il file).

✓

✓ **Normativa sugli Internet Service Provider**

✓

✓ Decreto Legislativo 259 del 2003 (noto come Legge Gasparri o Codice delle comunicazioni elettroniche), di regolamento, tra gli altri, delle reti e dei servizi di comunicazione elettronica ad uso pubblico.

✓ Decreto "Urbani" 72/2004, impone agli Internet Service Provider alcune pesanti responsabilità per ciò che concerne il diritto d'autore.

✓ Legge 269 del 1998, sulla pornografia, che richiede agli ISP attività di controllo e segnalazione con requisiti tecnici stabiliti dal Decreto Interministeriale del 8 gennaio 2007 (file 2007-01-29-Req-tecnici-pedopornografia.pdf).

✓ Per quanto riguarda la "data retention", ossia la conservazione dei dati di traffico telefonico e telematico, sono applicabili:

✓ Decreto-legge 27 luglio 2005, n. 144, convertito in legge con modificazioni dalla Legge 155 del 2005, detto "Decreto Pisanu" e successivamente modificato dal DL 225/2010 convertito in Legge 10 del 2011.

✓ Decreto Legislativo 109 di recepimento della Direttiva 2006/24/CE.

✓ Legge 48 del 2008, di ratifica della Convenzione di Budapest sulla criminalità informatica.

✓ Sul sito della Cassazione http://www.cortedicassazione.it è stato pubblicato un interessante Studio recante una disamina dei più recenti contributi giurisprudenziali e dottrinali in tema di intercettazioni, che pone in evidenza i contrasti ancora aperti.

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

✓ Regolamenti tecnici determinati da delibere dell'AGCOM (www.agicom.it) che richiedono, in particolare, la redazione e pubblicazione di documenti sulla qualità dei servizi e la Carta dei Servizi per: telefonia vocale fissa (Delibere n. 254/04/CSP e n. 79/09/CSP), comunicazioni mobili e personali (Delibere n. 104/05/CSP e n. 79/09/CSP), televisione a pagamento (Delibera n. 278/04/CSP), accesso a Internet da postazione fissa (Delibere n. 131/06/CSP e n. 244/08/CSP).

✓

✓ **Normativa sulla sicurezza delle reti (Direttiva NIS e infrastrutture critiche**)

✓

✓ Decreto legislativo 61/2011, "Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione"; questo D. Lgs. non è mai stato realmente applicato anche in vista del recepimento della Direttiva NIS.

✓ Decreto legislativo 65/2018, "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione."; questo D. Lgs. è il recepimento della cosiddetta Direttiva NIS (network and information security).

✓

✓ **Normativa sull'e-commerce**

✓

✓ La normativa di base sull'e-commerce è composta dai seguenti:

✓

✓ Decreto legislativo 70/2003, regolamentazione del commercio elettronico e, più in generale, dei servizi della società dell'informazione.

✓ Codice del Consumo (Dlgs 206/2005), affronta il tema della pubblicità ingannevole e comparativa e dei contratti a distanza.

✓

✓ Sono stati pubblicati nel tempo ulteriori dispositivi normativi specialistici, tra cui:

✓

✓ Dlgs 190/2005, sulla commercializzazione a distanza di servizi finanziari.

✓ i regolamenti sui giochi on-line decreti dell’AAMS, reperibili presso www.aams.gov.it

✓

✓ Normativa sulle infrastrutture critiche

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

✓

✓ Dlgs 61 del 2011, per il quale ogni azienda “critica” dovrà avere un responsabile della sicurezza unico e un “Piano della Sicurezza dell’Operatore”. Attualmente, le infrastrutture ICT non sono comprese nella normativa vigente, ma potrebbero esserlo in future revisioni.

✓

✓ **Normativa sul Segreto di Stato**

✓

✓ Il tema è di interesse anche per chi si occupa di sicurezza delle informazioni solo nell'ambito delle imprese private:

✓

✓ Legge 124 del 2007 sulla disciplina del Segreto di Stato

✓ DPCM 7 del 12 giugno 2009 "Determinazione dell'ambito dei singoli livelli di segretezza, dei soggetti con potere di classifica, dei criteri d'individuazione delle materie oggetto di classifica nonché dei modi di accesso nei luoghi militari o definiti di interesse per la sicurezza della Repubblica" (comprende a classificazione delle informazioni)

✓ DPCM 4 del 22 luglio 2011 "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate" (riporta le misure di sicurezza)

✓ Legge 241 del 1990 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi"

✓ DPR 184 del 2006 "Regolamento recante disciplina in materia di accesso ai documenti amministrativi." (riporta ulteriori specifiche rispetto a quelle già indicate dalla Legge 241/1990)

✓ DPCM 11 aprile 2002 sulla certificazione dei prodotti e sistemi IT coinvolti nel Segreto di Stato

✓

✓ **Normativa sull'accessibilità (Legge Stanca**)

✓

✓ Legge 4/2004 (nota come Legge Stanca) per l'accessibilità dei soggetti disabili agli strumenti informatici; ad essa dovranno seguire dei decreti attuativi.

✓ DPR 75 del 2005, regolamento di attuazione di cui all'articolo 10 della Legge Stanca.

✓ Decreto 8 luglio 2005 del Ministero per l’Innovazione e le Tecnologie: Requisiti tecnici e i diversi livelli per l'accessibilità agli strumenti informatici.

Per dettagli vedasi “Elenco documenti di origine esterna”

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

3. TERMINI E DEFINIZIONI

ACCETTAZIONE DEI RISCHI: Decisione di accettare i rischi

ANALISI DEL RISCHIO: Attività volta ad identificare minacce e vulnerabilità di un sistema allo scopo di definire gli obiettivi di sicurezza e di permettere la gestione del rischio.

ASSET: Qualsiasi cosa di valore per l 'Organizzazione

ATTACCO: Azione od evento che può pregiudicare la sicurezza di un sistema

AUDIT: Processo sistematico indipendente e documentato per ottenere evidenze della verifica ispettiva e valutarle con obiettività, al fine di stabilire in quale misura i criteri di verifica ispettiva sono stati soddisfatti

BEST PRACTICE: Migliore approccio possibile per affrontare una determinata situazione; è basato sull'osservazione su quanto fatto dalle Organizzazioni leader in circostanze analoghe

COMUNICAZIONE DEL RISCHIO: Scambio o condivisione di informazioni riguardo il rischio tra la Direzione e le parti interessate.

CONSEGUENZE: Risultato di un evento

CONTINUITA' OPERATIVA: Insieme di attività volte a minimizzare gli effetti distruttivi di un evento che ha colpito una Organizzazione o parte di essa con l'obiettivo di garantire la continuità delle attività in generale. Include il Disaster Recovery.

CONTROLLO ACCESSI: Funzione di sicurezza volta a controllare che un utente possa espletare le sole operazioni di loro competenza.

CONTROMISURE: Strumento di natura tecnologica, organizzativa o fisica, atto a contrastare un attacco nei confronti di un sistema.

CONTROLLO DEI RISCHI: Azioni implementate dalle decisioni della gestione dei rischi

DANNO: Effetto che può essere prodotto da una minaccia.

DICHIARAZIONE DI APPLICABILITA': Dichiarazione documentata che descrive gli obiettivi di controllo e i controlli rilevanti ed applicabili al SGSI della Organizzazione.

DISPONIBILITA': Assicurazione che gli utenti autorizzati abbiano accesso alle informazioni e agli assets quando ne fanno richiesta.

DISASTER RECOVERY: Insieme di attività volte a ripristinare lo stato del sistema informatico o parte di esso, compresi gli aspetti fisici e organizzativi e le persone necessarie per il suo funzionamento, con l'obiettivo di riportarlo alle condizioni antecedenti ad un evento disastroso.

EVENTO DI SICUREZZA DELLE INFORMAZIONI: Identificata occorrenza dello stato di un sistema, servizio o rete indicante una possibile vulnerabilità della politica di sicurezza delle informazioni, un'avaria delle contromisure o una situazione non osservata in precedenza ma rilevante per la sicurezza.

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

EVITARE I RISCHI: Decisione di non coinvolgimento, o azione di ritiro da una situazione di rischio

GARANZIA: Fiducia nella capacità di un sistema di protezione di soddisfare i requisiti di sicurezza.

GESTIONE DEGLI INCIDENTI: Insieme delle attività, dei processi e procedure, dell'Organizzazione e delle misure di sicurezza volti al rilevamento, alla risposta e alla risoluzione degli incidenti di sicurezza.

GESTIONE DEI RISCHI: Attività coordinate per dirigere e controllare una Organizzazione per quanto riguarda i rischi.

IDENTIFICAZIONE: Atto per cui un soggetto dichiara di essere se stesso; è il primo passo per l'autenticazione.

IDENTIFICAZIONE DEI RISCHI: Processo per trovare, elencare e caratterizzare elementi di rischio

IDENTIFICAZIONE DELLE SORGENTI: Processo per trovare, elencare e caratterizzare sorgenti di rischio

INCIDENTE DI SICUREZZA DELLE INFORMAZIONI: Evento o serie di eventi di sicurezza delle informazioni non voluti o inattesi che hanno una probabilità significativa di compromettere operazioni di business e di minacciare la sicurezza delle informazioni.

INTEGRITA': Assicurazione circa l'accuratezza e la completezza delle informazioni e i metodi di processo.

LIVELLO DI SERVIZIO: Indicatore che traduce le attese qualitative in obiettivi quantitativi misurabili sulla base dei quali è possibile verificare il rispetto delle clausole contrattuali ed in particolare dei livelli di qualità pattuiti.

LOG: File o altro documento elettronico che registra informazioni dettagliate sugli eventi di un sistema, di solito nella stessa sequenza in cui si verificano.

MECCANISMI DI SICUREZZA: Strumenti, apparati, software, algoritmi, procedure organizzative e operative che realizzano le funzioni di sicurezza.

MINACCIA: Una potenziale causa o un incidente che può causare danni ad un sistema o alla Organizzazione.

MISURAZIONE DEI RISCHI: Processo di comparazione tra il rischio stimato su i criteri definiti dei rischi per determinare l'importanza del rischio

MITIGAZIONE: Limitazione di alcune conseguenze negative di un particolare evento

OBIETTVI DI SICUREZZA: Esigenza di protezione da determinati attacchi contro i dati e le risorse del sistema informativo.

OTTIMIZZAZIONE DEI RISCHI: Processo, relativo al rischio per minimizzare le conseguenze negative e massimizzare le conseguenze positive e le loro rispettive probabilità

PAROLA CHIAVE: Password.

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

PASSWORD: Stringa di caratteri, generalmente cifrata dall' elaboratore, che autentica un utente ad un sistema.

PDCA (Plan-Do-Check-Act) : Modello dei sistemi di gestione articolato attraverso le fasi della definizione, realizzazione, esercizio, monitoraggio, revisione, manutenzione e miglioramento continuo dei processi.

PIANO DELLA SICUREZZA: Documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell' ambito, in genere di una Organizzazione.

POLITICA: Intenzione totale e strategie formalmente espresse dalla Direzione.

POLITICHE DELLA SICUREZZA: Costituiscono l'insieme dei principi, norme, regole, consuetudini che regolano la gestione delle informazioni di una Organizzazione in termini di protezione e distribuzione. Si possono classificare in politiche di alto livello e funzionali.

PRIVACY: Tratta la riservatezza in merito alle informazioni riguardanti la persona. In Italia il concetto di Privacy è correlato al Decreto Legislativo 30 giugno 2003. n. 196 "Codice in materia di protezione di dati personali".

PROBABILITA': dimensione che un evento possa accadere.

REQUISITI DI SICUREZZA: Esprimono ciò che si intende per sicurezza: riservatezza, integrità e disponibilità.

RIDUZIONE DEI RISCHI: Azioni prese per diminuire le probabilità negative e le conseguenze o entrambe associate al rischio

RIPRISTINO: Attività che consiste nel riportare un sistema al suo stato precedente a un errore. Nel caso di perdita di dati, permette di rigenerarli come erano prima dell'evento, in genere partendo da un back up.

RISCHIO: Combinazione della probabilità di un evento e le sue conseguenze.

RISCHI RESIDUI: Rischio rimanente dopo il trattamento

RISERVATEZZA (CONFIDENZIALITA'): Assicurazione che le informazioni siano accessibili solo da utenti autorizzati.

RUOLI E RESPONSABILITA': Definisce la categoria delle funzioni organizzative all'interno di un'organizzazione per la sicurezza che hanno lo scopo di specificare le figure operative che pianificano e gestiscono il sistema di protezione evidenziando le responsabilità e le attività di loro competenza.

SGSI (SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI): La parte del sistema di gestione, basata su un approccio dei rischi, per stabilire, implementare, monitorare, riesaminare, mantenere e migliorare il sistema di sicurezza delle informazioni.

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

STATEMENT OF APPLICABILITY: Dichiarazione documentata che descrive gli obiettivi di controllo e i controlli rilevanti ed applicabili al SGSI della Organizzazione.

STIMA DEI RISCHI: Processo usato per assegnare valori alle probabilità e conseguenze

TRASFERIMENTO DEI RISCHI: Condividere con altre parti il valore della perdita o benefici di guadagni, per un rischio

TRATTAMENTO DEI RISCHI: Processo di selezione ed implementazione di misure per modificare il rischio

VALUTAZIONE DEI RISCHI: Processo di analisi dei rischi e misurazione dei rischi

VULNERABILITA': Una debolezza di un asset o gruppo di asset che può determinare una o più minacce.

4. SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

4.1 Requisiti generali

4.2 Stabilire e gestire il ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM)

4.2.1.a: SCOPO

Per uniformità ai punti della norma ISO 27001, vedasi sezione §1 del presente manuale.

Il presente Manuale di gestione per la sicurezza delle informazioni (MGSI) si applica al seguente campo di applicazione:

Progettazione, sviluppo, manutenzione e gestione software. Consulenza informatica.

E' escluso il punto A.6.2.2 Telelavoro della norma perché non vengono utilizzate procedure contabili e/o gestionali con assegnazione di risorse/asset aziendali

Le caratteristiche del business sono quindi quelle coperte dalle attività indicate. Il business di NETCOM ENGINEERINGS.p.a. si caratterizza per la forte necessità di soddisfare i requisiti dei clienti.

La struttura organizzativa è riportata dall'organigramma.

Da un punto di vista fisico, NETCOM ENGINEERINGS.p.a. ha sede in Via Via Nuova Poggioreale, C.tro Polif. T7 – Napoli Piano 5 e Piano 6 (CED).

La sede operativa della società è in un ufficio dislocato in un edificio di più piani di cui la NETCOM ENGINEERINGS.p.a. occupa il 5° ed il 6° per un totale di circa 400 m2. Il piano 5° è dedicato principalmente alle attività di amministrazione e funzioni di staff, mentre il piano 6° alle attività di Software Factory e consulenza.
L'edificio fa parte di un centro Polifunzionale composto da più edifici protetti da una recinzione e con un servizio di vigilanza h24. Inoltre ogni edificio è dotato dalla 8 alle 19 di servizi di vigilanza singoli.
Gli uffici sono protetti da porte blindate, da un servizio di allarme di ultima generazione con combinatore telefonico e da un sistema di videosorveglianza attivo 24 h.

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

L'ingresso agli uffici è subordinato all'identificazione ed autorizzazione della Reception.

4.2.1.b: DEFINIZIONE DELLA POLITICA

Vedasi Allegato n. 2

4.2.1.c: DEFINIZIONE APPROCCIO SISTEMATICO ALLA VALUTAZIONE DEL RISCHIO

La NETCOM ENGINEERINGS.p.a. ha definito un metodo sistematico per la valutazione del rischio. Tale metodo è illustrato nel Documento di Valutazione dei rischi predisposto: Allegato n. 6

4.2.1.d: IDENTIFICAZIONE DEL RISCHIO

LA METODOLOGIA

La metodologia utilizzata ha richiesto come prima fase l'individuazione dei servizi su cui svolgere l'analisi. Ciascun servizio è stato descritto indicandone sommariamente le specificità, l'organizzazione coinvolta nella sua gestione e utilizzo, incluse le terze parti, i confini fisici e la tecnologia coinvolta.

Valutazione degli impatti

Per ciascun servizio sono stati valutati i danni per l'azienda in caso di perdita di Riservatezza, Integrità e Disponibilità delle informazioni gestite dal servizio.

Identificazione e valutazione delle minacce

Per singolo servizio, sono state identificate e valutate le minacce che possono avere impatti su di esso.

La valutazione è dinamica, in quanto potranno essere aggiunte ulteriori minacce, oltre a quelle già previste. Per ogni minaccia, sono state documentate le motivazioni che hanno portato alla decisione del valore attribuito.

Analisi dei controlli di sicurezza

Sono stati analizzati i controlli di sicurezza che operano sul servizio.

4.2.1.e: VALUTAZIONE DEL RISCHIO

Il metodo applicato confronta il valore del rischio inerente per ciascuna minaccia con quello attribuito a ciascun controllo che la contrasta.

4.2.1.f: VALUTAZIONI DELLE OPZIONI PER IL TRATTAMENTO DEL RISCHIO

Le Contromisure hanno lo scopo di ridurre il Rischio dovuto alla presenza di Vulnerabilità. Possono avere vari obiettivi:

1. Ridurre la probabilità di occorrenza delle minacce
2. Ridurre le vulnerabilità
3. Ridurre gli impatti

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

e possono essere di vari tipi:

- Fisico (ad es. un cancello, un badge, un estintore ecc.)
- Procedurale (ad es. il fatto di mostrare un documento all'ingresso, un giro di sorveglianza fatto a orari diversi e non regolari, polizie ecc.)
- Tecnico (ad es. l'installazione di un RAID, un backup ecc.)
- Personale (ad es. corsi di formazione sulla sicurezza, training specializzato ecc.)

Le contromisure attuate sono di tipo:

- Preventive (cioè atte a prevenire l'occorrenza del problema)
- Dissuasive (cioè hanno lo scopo di dissuadere un eventuale attaccante, come una guardia armata, una legge, un cartello, ecc.)
- Palliative (cercano di diminuire l'impatto di un problema)
- Rivelatrici (cercano di rivelare l'insorgere del problema prima possibile per limitarne l'impatto)
- Protettrici (cercano di ridurre la vulnerabilità, ad es. dei sacchi di sabbia messi a protezione di una finestra al verificarsi di un uragano)

4.2.1.g: SELEZIONE DEI CONTROLLI PER IL TRATTAMENTO DEI RISCHI

Sulla base della valutazione del rischio, la NETCOM ENGINEERINGS.p.a. ha definito un programma per ridurre il rischio di qualsiasi attività in cui il livello è oltre i limiti accettabili. Per ciascuno dei fattori individuati a seguito della valutazione dei rischi è stato definito un trattamento.

Possibili opzioni di trattamento del rischio includono:

a) l'applicazione di controlli appropriati per ridurre i rischi;
b) di accettare consapevolmente e oggettivamente i rischi, a patto che tale approccio soddisfi la politica ed i criteri per l'accettazione del rischio;
c) evitare i rischi, non consentendo azioni che comportano i rischi che si verificheranno;
d) il trasferimento dei rischi associati ad altri soggetti, ad esempio, assicuratori o fornitori.

I controlli devono assicurare che i rischi siano ridotti ad un livello accettabile tenendo conto:

a) i requisiti e vincoli della normativa nazionale e internazionale e regolamenti;
b) gli obiettivi organizzativi;
c) i requisiti operativi e dei vincoli;
d) costi di attuazione e di funzionamento in relazione ai rischi di ridursi, e rimanendo proporzionale alle esigenze dell'organizzazione e dei vincoli;
e) la necessità di bilanciare gli investimenti in attuazione e il funzionamento dei controlli contro i danni che potrebbero derivare da errori di protezione.

Deve essere comunque affermato che nessun insieme di controlli può garantire la sicurezza totale delle informazioni gestite.
E' sempre ravvisabile un'azione di gestione che potrebbe essere necessaria per attuare, monitorare, valutare e migliorare l'efficienza e l'efficacia dei controlli di sicurezza che supportano gli obiettivi aziendali.

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

Rif. Allegato n. 6 Documento di valutazione del rischio

4.2.1.h: PREPARAZIONE DI UNA DICHIARAZIONE DI APPLICABILITA'

Lo Statement of applicability (SOA – Dichiarazione di applicabilità) riporta i controlli proposti dalla seconda parte dello standard (descritti in modo molto più sintetico e generico rispetto alla prima parte) e i dettagli relativi alla loro realizzazione o le motivazioni della loro esclusione. Il SOA riporta i riferimenti alle eventuali procedure correlate. Il SOA riporta le modifiche apportate tra le diverse versioni.

Per dettagli vedasi l'Allegato 3 "Dichiarazione di Applicabilità"

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

4.2.2 ISTITUZIONE E ATTUAZIONE DELL'ISMS

La Direzione è responsabile per la sicurezza delle informazioni. Si avvale di risorse per il controllo, monitoraggio e salvaguardia dei dati.
Le mansioni delle risorse sono riportate nel Mansionario (vedi allegato 4)

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

4.2.3 SORVEGLIANZA E RIESAME DELL'ISMS

La NETCOM ENGINEERINGS.p.a. svolge le seguenti attività relative alla sicurezza delle informazioni.

- Pianificazione e implementazione delle misure di trattamento del rischio determinato come descritto. (Il piano identifica l'appropriata azione di gestione, le responsabilità e le priorità per la gestione di rischio per la sicurezza delle informazioni.
- Attuazione di programmi di formazione e sensibilizzazione per gli utenti generici.
- Gestione delle risorse e delle operazioni per la sicurezza informatica efficace.
- Aiutare ad individuare e attuare le procedure e gli altri controlli in grado di consentire una rapida individuazione e la risposta agli incidenti di sicurezza.

4.2.4: MANTENIMENTO E MIGLIORAMENTO DELL'ISMS

NETCOM ENGINEERINGS.p.a. utilizza i dati di sicurezza per adottare azioni di miglioramento nei seguenti ambiti.

- Implementare i miglioramenti individuati nel ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM), comprese le azioni preventive e correttive, in un modo così come individuate dalla gestione.
- Applicare gli insegnamenti tratti dalle esperienze di sicurezza di altre organizzazioni, come ad esempio clienti, fornitori e altri, a seconda dei casi.
- Comunicare i risultati della revisione ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) e prevedere che tutte le parti interessate arrivino ad un piano comune.
- Controllare che i miglioramenti raggiungano l'obiettivo previsto.

Il ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) è monitorato e rivisto periodicamente per migliorarne il funzionamento nelle seguenti aree:

- Rilevazione dei rischi per la sicurezza che possono influenzare il buon funzionamento dei servizi erogati
- Identificazione di violazioni della sicurezza fallite.
- Determinare se le attività di sicurezza delegate a persone o attuate dalle tecnologie dell'informazione siano stati eseguite come previsto;
- Azioni rapide ed efficaci adottate per risolvere una violazione della sicurezza che riflette le priorità di business.

  Revisione dell'efficacia del ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) (compresa la politica di sicurezza e di incontro degli obiettivi, e revisione dei controlli di sicurezza), condotte dal Comitato sulla sicurezza, tenendo conto di audit di sicurezza, incidenti, suggerimenti e feedback da tutte le parti interessate.

Miglioramento e rivalutazione tenendo conto di:

- Organizzazione
- Tecnologia
- Gli obiettivi di business e dei processi
- Le minacce identificate

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

- I cambiamenti nel contesto operativo esterno che possono influire sul funzionamento

4.3 REQUISITI RELATIVI ALLA DOCUMENTAZIONE

La documentazione mantenuta per il ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) include quanto segue:

- Dichiarazione documentata della politica di sicurezza, che viene fornita in sintesi e pubblicizzata.
- I dettagli del campo di applicazione del ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM), e le procedure e il controllo a supporto del ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM).
- Una metodologia di valutazione del rischio così come il rapporto dello stesso per tutte le informazioni e le risorse di elaborazione delle informazioni.
- Piano di trattamento del rischio per ogni entità.
- Le procedure documentate nell'ambito di applicazione del ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) necessarie a garantire il funzionamento efficace di pianificazione e controllo dei processi informativi sua sicurezza.
- Una dichiarazione di applicabilità dello standard ISO 27001, debitamente approvato dalla Direzione.

Tutta la documentazione è a disposizione degli utenti come descritto dalla politica ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) .

I documenti e le registrazioni possono essere in formato elettronico o su carta.

4.3.1: GENERALITA'

4.3.2: CONTROLLO DELLA DOCUMENTAZIONE

Tutti i documenti ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) sono protetti e controllati come descritto in politica e comprendono quanto segue:

- L'approvazione prima dell'emissione dei documenti
- Revisione del documento e metodi di aggiornamento, tra stato della versione di emissione di documenti appropriati e la disponibilità nel punto di utilizzo

Tutta la documentazione del Sistema, prima di essere approvata dalla funzione incaricata. La distribuzione all'interno controllata.

La documentazione prevista del SGSI prevede:

- Politica ed obiettivi per la sicurezza;
- Descrizione dei confini del SGSI (ambito o perimetro);
- Metodologia e Rapporto di valutazione dei rischi;
- Piano di trattamento dei rischi;
- Procedure documentate per : Gestione della Documentazione, Audit Interni
- Interne (Audit), Azioni Correttive,
- Registrazioni del SGSI;

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

- Valutazioni sull' efficacia del SGSI;
- Dichiarazione di Applicabilità : l'elenco di tutte le contromisure adottate con inclusi i motivi di scelta ed eventuale esclusione sono riportati in allegato;
- Altra documentazione dell'Organizzazione per la definizione di ruoli e responsabilità, pianificazione e gestione del SGSI.

Rif. procedura PG 01 GESTIONE DELLE INFORMAZIONI DOCUMENTATE

4.3.3.: CONTROLLO DELLE REGISTRAZIONI

Attraverso l'applicazione sistematica delle regole che la NETCOM ENGINEERINGS.p.a. si è costruita, si ha a possibilità di:

- disporre di registrazioni sempre aggiornate e leggibili
- poter dimostrare la conformità e l'efficace funzionamento del Sistema
- mantenerle il più possibile integre nel tempo, in collocazioni adeguate sia per le versioni cartacee che elettroniche
- identificarle e reperirle rapidamente in tutti i casi necessari
- eliminarle quando non più necessarie.

Le modalità di gestione dei documenti del Sistema di Gestione e di quelli di origine esterna utilizzati come riferimento per lo svolgimento delle attività sono definite in apposita Procedura Operativa.

L'elenco delle Procedure Operative, delle Istruzioni Tecniche e della Modulistica di registrazione, sono riportati in allegato al presente Manuale e vengono gestiti da RISMS.

5. RESPONSABILITA' DELLA DIREZIONE

5.1.: IMPEGNO DELLA DIREZIONE

La direzione della NETCOM ENGINEERINGS.p.a. si impegna a stabilire, implementare, gestire, monitorare, revisionare, mantenere e il migliorare il ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) . La direzione dirige il compito sulla valutazione del rischio e del trattamento e controlla l'ISMS per mezzo di verifiche periodiche. E questo ha fatto sì, grazie all'istituzione di una politica di sicurezza dell'informazione, di stabilire gli obiettivi della sicurezza delle informazioni così come i ruoli e le responsabilità per la sicurezza informatica.
La direzione fornisce inoltre le risorse sufficienti per sviluppare, implementare, gestire e mantenere il ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) .

Sono garantite comunicazioni a tutti gli interessati all'interno dell'organizzazione, sottolineando l'importanza di raggiungere gli obiettivi di sicurezza delle informazioni conformemente alla politica di sicurezza delle informazioni, le responsabilità secondo la legge e la necessità di un miglioramento continuo.

5.2.: GESTIONE DELLE RISORSE

5.2.1.: MESSA A DISPOSIZIONE DELLE RISORSE

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

NETCOM ENGINEERINGS.p.a. ha stabilito i requisiti e ha fornito le necessarie risorse necessarie per stabilire, implementare, gestire e mantenere il ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) . Ciò al fine di assicurare che le procedure di sicurezza delle informazioni di supporto alle esigenze di business siano implementate, identificate e e che soddisfino i requisiti legali e normativi e gli obblighi contrattuali della sicurezza, mantenendo la sicurezza adeguata per la corretta applicazione di tutti i controlli implementati, svolgere la revisione quando necessario, e di reagire adeguatamente ai risultati compresi i miglioramenti del ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM). .

5.2.2.: ADDESTRAMENTO, CONSAPEVOLEZZA E COMPETENZA

NETCOM ENGINEERING S.p.a. assicura che tutto il personale con responsabilità assegnate definite nel ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) è competente per eseguire i compiti richiesti. Questo è assicurato grazie all'istituzione di numerosi processi tra cui:

- Fornire formazione e certificazione competenze per il personale coinvolto.
- Mantenere record di istruzione, formazione, competenze, esperienza e le qualifiche di tutto il personale.

NETCOM ENGINEERINGS.p.a. assicura inoltre che tutto il personale interessato è consapevole della rilevanza ed importanza delle attività di informazione, la loro sicurezza e su come essi contribuiscono al raggiungimento degli obiettivi ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) , per mezzo di varie attività formative.

6. AUDIT INTERNI

NETCOM ENGINEERING S.p.a. effettua controlli di conformità a quanto pianificato a intervalli regolari per determinare se il controllo degli obiettivi, controlli, processi e procedure del proprio ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) è conforme ai requisiti di sicurezza e informazioni identificate e se sono effettivamente attuate e mantenute.

Le valutazioni di rischio per la sicurezza sarà eseguita con frequenza di 12 mesi. Un'ulteriore analisi del rischio può essere realizzata se lo richiede il contesto imprenditoriale e di funzionamento e quanto ritenuto necessario da avvenuti cambiamenti.

Il fabbisogno supplementare della revisione è quello di verificare se il ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) è conforme ai requisiti della ISO 27001.

La gestione responsabile dell'area oggetto di audit deve assicurare che le azioni sono prese senza indebito ritardo per eliminare le non conformità eliminando le loro cause.

Le Modalità di audit sono definite nella procedura PG09 VALUTAZIONE DELLE PRESTAZIONI E MIGLIORAMENTO CONTINUO.
Il programma di audit è pianificato, prendendo in considerazione lo stato e l'importanza dei processi e delle aree in oggetto, come anche i risultati degli audit precedenti. I criteri per l'audit, l'ambito, la frequenza e i metodi sono ben definiti rispettando le definizioni, principi e gestione di un programma di audit previsti dalla ISO 19011. La selezione degli auditors e la condotta dell'audit garantisce

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

obiettività ed imparzialità dei processi. Gli auditors non possono effettuare audit sul loro proprio lavoro. Le responsabilità e i requisiti per pianificare e condurre gli audit, nonché per presentare i risultati e mantenere le annotazioni sono definiti in una procedura documentata. Il management responsabile dell'area soggetta all'audit garantisce che si agirà senza ritardo per eliminare le non conformità individuate e le loro cause. Le attività di miglioramento includono la verifica delle azioni intraprese e la presentazione dei risultati di verifica.

7. RIESAME DA PARTE DELLA DIREZIONE

La direzione NETCOM ENGINEERINGS.p.a. riesamina il sistema ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) ad intervalli pianificati (una volta l'anno) per assicurare la sua idoneità, adeguatezza ed efficacia. Questo include la valutazione delle opportunità di miglioramento e richiede modifiche da essere chiaramente documentate e registrazioni conservate secondo definite procedure .

7.1.: GENERALITA'

7.2.: ELEMENTI IN INGRESSO PER IL RIESAME

La direzione riesamina le prestazioni del ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) tramite informazioni su:

- o Risultato dei controlli/visite ispettive
- o Informazioni di ritorno da tutte le parti interessate
- o Tecnologie/procedure che sono proposte dai vari responsabili dell'ISMS in ottica di miglioramento
- o Stato delle azioni preventive/correttive
- o Minacce e vulnerabilità non soddisfacentemente trattate nei precedenti risk assessments
- o Follow up sulle iniziative decise nei precedenti riesami
- o Qualsiasi evento interno/esterno all'azienda ce debba essere riflesso nell'ISMS
- o Raccomandazioni per il miglioramento

7.3.: ELEMENTI IN USCITA PER IL RIESAME

Elementi di output del riesame della direzione comprende tutte le decisioni e le azioni relative a quanto segue.

- o programmi di miglioramento
- o aggiornamento del piano di trattamento del rischio
- o requisiti di aggiornamento delle procedure sulla base di: bus requirement /security requirements, business processes (nuovi,variati), normativa,obblighi contrattuali, variazioni dei livelli di rischio accettabili
- o dimensionamento risorse
- o miglioramenti nei sistemi di monitoraggio delle prestazioni del sistema

8. MIGLIORAMENTO DELL'ISMS

8.1.: MIGLIORAMENTO CONTINUO

NETCOM ENGINEERINGS.p.a. si impegna a migliorare continuamente l'efficacia del ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) attraverso l'utilizzo della politica di

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.

sicurezza delle informazioni, i risultati degli audit, l'analisi degli eventi monitorati e analisi della gestione, reclami.

8.2: AZIONI CORRETTIVE

NETCOM ENGINEERINGS.p.a. interviene per eliminare la causa delle non conformità nella realizzazione e il funzionamento del ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) al fine di prevenire il ripetersi di incidenti di sicurezza. Tutti i dipendenti devono seguire le procedure atte a garantire lo stesso. Diverse misure sono generalmente raccomandate per questo scopo a tutti gli interessati. La procedura per l'azione preventiva comprende:

- Essere consapevoli della politica della sicurezza e delle responsabilità, permettendo all'individuo di identificare le non conformità di attuazione e / o il funzionamento del ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM) .
- Assistere nel determinare le cause di non conformità
- Registrazione delle azioni intraprese e la revisione delle azioni correttive intraprese.

ALLEGATI

1. Organigramma
2. Politica
3. SOA
4. Mansionario
5. Nomina RISMS
6. Documento valutazione rischi sicurezza
7. Verbale riesame direzione
8. Obiettivi e programma di miglioramento

Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma senza il preventivo consenso della NETCOM GROUP S.p.a.