Consulenza per la Certificazione ISO 27001 Sicurezza delle Informazioni

Realizzazione di un Sistema di Gestione per la Sicurezza delle Informazioni, in conformità alla norma UNI CEI ISO/IEC 27001 Tecnologie informatiche – Tecniche per la Sicurezza – Sistemi di Gestione per la Sicurezza delle informazioni – Requisiti.

PREMESSA

Il sistema di gestione per la sicurezza delle informazioni preserva la riservatezza, l'integrità e la disponibilità dalle informazioni mediante l'applicazione di un processo di gestione del rischio e dà fiducia alle parti interessate sull'adeguatezza della gestione dei rischi.

È importante che il sistema di gestione per la sicurezza delle informazioni sia parte integrante dei processi e della struttura gestionale complessiva dell'organizzazione e che la sicurezza delle informazioni sia considerata nella progettazione dei processi, dei sistemi informativi e dei controlli.

Un sistema di gestione per la sicurezza delle informazioni deve essere commisurato alle necessità dell'organizzazione.

DESCRIZIONE DELLA CONSULENZA OFFERTA.

1) Progettazione e Realizzazione del Sistema di Gestione per la Sicurezza delle Informazioni in conformità alla norma UNI CEI ISO/IEC 27001.

- Verifica delle attività dell'Organizzazione, dei processi, dei ruoli e delle funzioni;
- Verifica del Contesto e della Gestione dei Rischi;
- Definizioni interfacce operative;
- Individuazione del responsabile per la sicurezza informatica e di un Amministratore di Sistema;
- Analisi del Sistema e pianificazione delle attività.

La Consulenza verrà realizzata redigendo:

- La definizione dello scopo e del campo di applicazione per la certificazione ISO/IEC 27001
- La Valutazione dei rischi
- La Dichiarazione di Applicabilità (S.O.A.) come da appendice A della norma che prevede 114 controlli
- La Politica di Sicurezza Informatica
- Le lettere di nomina
- L'elenco apparecchiature HW e SW
- Elenco Applicativi e relative licenze
- Integrazione delle Informazioni documentate ISO 9001 con gli aspetti della ISO/IEC 27001
- Procedure di back up, ripristino dati, disaster recovery
- Procedure di business continuity, gestione degli incidenti informatici con il supporto, per quanto di competenza, dell'Amministratore del Sistema.

I punti della norma UNI CEI ISO/IEC 27001:

1. Scopo e campo di applicazione/presentazione della Società
2. Riferimenti normativi
3. Termini e Definizioni
4. Contesto dell'Organizzazione

4.1 Comprendere l'organizzazione e il suo contesto con Risk Management in accordo con Gestione del rischio UNI ISO 31000 Principi e linee guida

4.2 Comprendere le esigenze e le aspettative delle parti interessate

4.3 Determinare il campo di applicazione del sistema di gestione

CONSULENZA INTEGRATA S.R.L.
Sede legale ed amministrativa: Via Dardanelli, 15
00195 - ROMA - Tel. 06.83652695
E-mail: areacommerciale@consulenzaintegrata.eu
Partita IVA e Codice Fiscale 11663201009 - Capitale Sociale € 10.000,00 i.v.

4.4 Sistema di gestione per la sicurezza delle informazioni
5. Leadership
5.1 Leadership e impegno
5.2 Politica
5.3 Ruoli, responsabilità e autorità nell'organizzazione
6. Pianificazione
6.1 Azioni per affrontare rischi e opportunità, Risk Management
6.2 Obiettivi per la sicurezza delle informazioni e pianificazione per conseguirli
7. Supporto
7.1 Risorse
7.2 Competenza
7.3 Consapevolezza
7.4 Comunicazione
7.5 Informazioni documentate
8. Attività Operative
8.1 Pianificazione e controllo operativi
8.2 Valutazione del rischio relativo alla sicurezza delle informazioni
8.3 Trattamento del rischio relativo alla sicurezza delle informazioni
9. Valutazione delle Prestazioni
9.1 Monitoraggio, misurazione, analisi e valutazione
9.2 Audit interno
9.3 Riesame di direzione
10. Miglioramento
10.1 Non conformità e azioni correttive
10.2 Miglioramento continuo

2) Corso di formazione base sulla norma UNI CEI ISO/IEC 27001 per il responsabile qualità e per i responsabili di processo. (max. 10 persone).
3) Audit Interno e Penetration Test
   In questa fase è necessario effettuare un “test di penetrazione” dei sistemi informatici e delle difese predisposte dalla Società, test che deve essere effettuato a cura di Società da fornitore esterno competente.
   A completamento del “test di penetrazione” è previsto un Audit interno sul sistema di sicurezza informatica per verificare la conformità alla norma UNI CEI ISO/IEC 27001.
4) Supporto al Riesame della Direzione
   Il riesame di direzione deve includere considerazioni su:
   a) lo stato delle azioni derivanti dai precedenti riesami di direzione;
   b) i cambiamenti dei fattori esterni e interni che hanno attinenza con il sistema di gestione per la sicurezza delle informazioni;
   c) le informazioni di ritorno sulle prestazioni relative alla sicurezza delle informazioni, compresi gli andamenti:
   1) delle non conformità e azioni correttive;
   2) dei risultati del monitoraggio e della misurazione;
   3) dei risultati di audit;
   4) del raggiungimento degli obiettivi per la sicurezza delle informazioni;

CONSULENZA INTEGRATA S.R.L.
Sede legale ed amministrativa: Via Dardanelli, 15
00195 - ROMA - Tel. 06.83652695
E-mail: areacommerciale@consulenzaintegrata.eu
Partita IVA e Codice Fiscale 11663201009 - Capitale Sociale € 10.000,00 i.v.

d) le informazioni di ritorno dalle parti interessate;
e) i risultati della valutazione del rischio e lo stato del piano di trattamento del rischio;
f) le opportunità per il miglioramento continuo.

Gli elementi in uscita dal riesame di direzione devono comprendere decisioni relative alle opportunità per il miglioramento continuo e ogni necessità di modifiche al sistema di gestione per la sicurezza delle informazioni.

5) Assistenza durante l'effettuazione della visita di certificazione da parte dell'Organismo Prescelto.

Assistenza durante l'effettuazione della visita di Certificazione da parte dell'ente scelto durante stage 1 e stage 2. Il tempo necessario per l'Audit sarà stabilito dall'Ente di Certificazione.

Risultato previsto; Certificazione secondo la norma UNI CEI ISO 27001.

MANTENIMENTO IMPLEMENTAZIONE DEL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Ad avvenuta Certificazione:

- Eventuale Revisione Documentale
- Audit per verificare lo stato di conformità aziendale al Sistema di Gestione
- Riesame del Sistema
- Assistenza in qualità di osservatore durante l'effettuazione della visita di sorveglianza da parte dell'Organismo di Certificazione

Dasa-Rägister

IQ-1012-05

Certificato NO.
Certificate NO.

2012-10-09

Data di prima emissione
First issue date

2017-11-06

Data di ultima emissione
Last issue date

2018-10-09

Data di scadenza
Expiry date

President & C.E.

Auditing Director

Dasa-Rägister S.p.A.
Italy - 00071 Pomezia - Roma
Via dei Castelli Romani, 22
Tel.+ 39 0691622002
Fax +39 069107126
www.dasa-raegister.com
Offices: Milano, Roma, Bari

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

SGQ N° 052A PRD N° 245B
SGA N° 030D
SSI N° 011G

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC

Signatory of EA, IAF and ILAC Mutual Recognition Agreements

CERTIFICATE

Dasa-Rägister S.p.A.

ENTE CERTIFICATORE CERTIFICA CHE IL SISTEMA DI GESTIONE PER LA QUALITÀ DI
CERTIFICATION BODY CERTIFIES THAT THE QUALITY MANAGEMENT SYSTEM OF

Consulenza Integrata S.r.l.

Italia - 00195 Roma - Via Dardanelli, 15

È STATO VERIFICATO E TROVATO CONFORME AI REQUISITI DELLO STANDARD
HAS BEEN ASSESSED AND FOUND IN COMPLIANCE WITH THE STANDARD REQUIREMENTS

EN ISO 9001:2015

Per le seguenti attività aventi come oggetto
Consulenza di direzione nei settori: Qualità, Ambiente, Salute e Sicurezza sui luoghi di lavoro, Medicina del Lavoro, Sistemi di Gestione Integrata, Sistemi di gestione secondo Dlgs 231/01, Sicurezza Alimentare, Privacy. Progettazione ed erogazione di corsi di formazione continua nei settori: Qualità, Ambiente, Salute e Sicurezza sui luoghi di lavoro, Medicina del Lavoro, Sistemi di Gestione Integrata, Sistemi di gestione secondo Dlgs 231/01, Sicurezza Alimentare, Privacy. Progettazione ed erogazione di piani formativi aziendali finanziati da fondi interprofessionali

For the following activities having as object
Managerial Consultancy in the following area: Quality, Environment, Health and Safety at Workplaces, Occupational Medicine, Integrated Management Systems, Management systems according to Dlgs 231/01, Food Safety, Privacy. Design and provision of continual training courses in the following area: Quality, Environment, Health and Safety at Workplaces, Occupational Medicine, Integrated Management Systems, Management systems according to Dlgs 231/01, Food Safety, Privacy. Design and provision of Business training courses financed by interprofessional funds

Settori - Sectors **35 - 37**

Informazioni puntuali e aggiornate circa lo stato della presente Certificazione sono disponibili all'indirizzo www.dasa-raegister.com.
Punctual and updated information regarding this Certification is available at www.dasa-raegister.com.

Riferirsi alla Documentazione del Sistema di Gestione Qualità dell'Organizzazione per i dettagli delle singole esclusioni ai requisiti della Norma ISO 9001:2015. La validità del presente Certificato è subordinata al rispetto delle prescrizioni del Regolamento di Certificazione Dasa-Rägister, dei requisiti della Norma ISO 9001:2015, ad un programma di sorveglianza annuale e ad un riesame ogni tre anni.

Refer to the Documents of the Quality Management System of the Organisation for details regarding the exclusions to ISO 9001:2015 Standard requirements. The validity of this Certificate is subordinated by a full respect of that prescribed in Dasa-Rägister's Certification Regulation, of ISO 9001:2015 Standard requirements, to an annual surveillance programme and to a three yearly re-assessment.

CONSULENZA INTEGRATA S.R.L.
Sede legale ed amministrativa: Via Dardanelli, 15
00195 - ROMA - Tel. 06.83652695
E-mail: areacommerciale@consulenzaintegrata.eu
Partita IVA e Codice Fiscale 11663201009 - Capitale Sociale € 10.000,00 i.v.