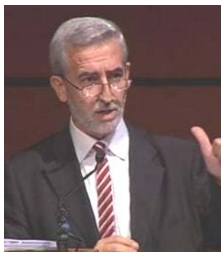
2019 NOTIZIE
n. 003 - GENNAIO 2019
LA CONOSCENZA GENERA LE IDEE PER L'INNOVAZIONE DELLE IMPRESE
Aggiornamenti legislativi, normativi, tecnologici e organizzativi per migliorare il sistema di gestione aziendale

SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

UNI CEI EN ISO/IEC 27001:2017



Dott. Ing. G. GAETANI
- Ingegnere della Conoscenza
- Esperto di Organizzazioni Aziendali Complesse
- Progettista di "Modelli 231"
- Componente/Presidente di Organismi di Vigilanza per "Modelli 231"
- Esperto di Compliance di Sistema e Prodotto

Dott. Ing. P. TRENTINI
- Responsabile divisione "Compliance per Medie e Grandi Imprese" del Gruppo 2G
- Esperto di "Internal Auditing" per Sicurezza, Ambiente e Energia
- Esperto di Sistemi di Gestione Qualità, Sicurezza, Ambiente, Energia e Sicurezza delle Informazioni

Dott. Ing. A. SALISBURGO
- PROJECT MANAGER del Gruppo 2G Management Consulting
- Esperto di Sistemi di Gestione per la Qualità, Ambiente e Sicurezza delle Informazioni
- Consulente di Modelli di Organizzazione, Gestione e Controllo (D.Lgs. 231/01 s.m.i.)
- Consulente per la redazione della Dichiarazione Non Finanziaria

1. INTRODUZIONE

Prima di illustrare gli aspetti operativi per la progettazione e la documentazione di un Sistema di Gestione è importante condividere le definizioni dei termini "dati", "informazioni" e "sicurezza delle informazioni".

Con il termine *"dati"* si intende *"rappresentazioni originarie (cioè non interpretate) di un fenomeno, evento o fatto, effettuate con simboli o loro combinazioni, o di qualsiasi altra forma espressa legate ad un qualsiasi supporto".*

Con il termine "informazioni" si intende una *"aggregazione ed elaborazione di dati elementari di interesse per i destinatari ed importanti per il processo decisionale presente e futuro".*

L'informazione è indispensabile per il successo e la crescita di ogni organizzazione e quindi si configura sempre più come un asset di inestimabile valore che impone una adeguata tutela: è la moneta del 21° secolo.

Per questo motivo la "sicurezza delle informazioni" assume una primaria importanza poiché investe diversi aspetti e cioè i beni, il software proprietario, il business, l'immagine, la reputazione, tutto ciò che viene richiesto dalle norme giuridiche (es. D.Lgs. 196/03, D.Lgs. 63/2018).

Con il termine "sicurezza delle informazioni" si intende la salvaguardia di:
- RISERVATEZZA (assicurare che l'informazione sia accessibile solo a chi è autorizzato);
- INTEGRITÀ (salvaguardare l'accuratezza e la completezza delle informazioni e dei beni collegati quando necessario);
- DISPONIBILITÀ (assicurare che gli utenti autorizzati abbiano accesso all'informazione e ai beni collegati quando necessario.

Questa definizione non riguarda solamente la sicurezza in funzione degli attacchi dal mondo esterno ma comprende l'intero ciclo di vita delle informazioni che si presentano in formato scritto, elettronico, parlato, trasmesse via e-mail e relative agli aspetti interni e/o esterni dell'azienda.

Il "sistema di gestione della sicurezza delle informazioni" comprende aspetti organizzativi e gestionali (non è sufficiente implementare un insieme di controlli e procedure per la sicurezza, occorre gestirli e mantenerli nel tempo) oltre ad aspetti tecnici (quindi non solo l'applicazione di strumenti più appropriati al singolo obiettivo di protezione come introduzione di firewall, antivirus, backup, ecc…).

UNA IMPRESA DELLA CONOSCENZA E DI SERVIZI INNOVATIVI
GRUPPO 2G MANAGEMENT CONSULTING
Gruppo 2G Management Consulting s.r.l.
Largo Re Umberto, 106 • 10128 - Torino Tel. 011. 50.50.62 (r.a.) • Fax 011. 50.46.60
www.gruppo2g.com e-mail: gruppo2g@gruppo2g.com

2019 NOTIZIE
n. 003 - GENNAIO 2019
LA CONOSCENZA GENERA LE IDEE PER L'INNOVAZIONE DELLE IMPRESE
Aggiornamenti legislativi, normativi, tecnologici e organizzativi per migliorare il sistema di gestione aziendale

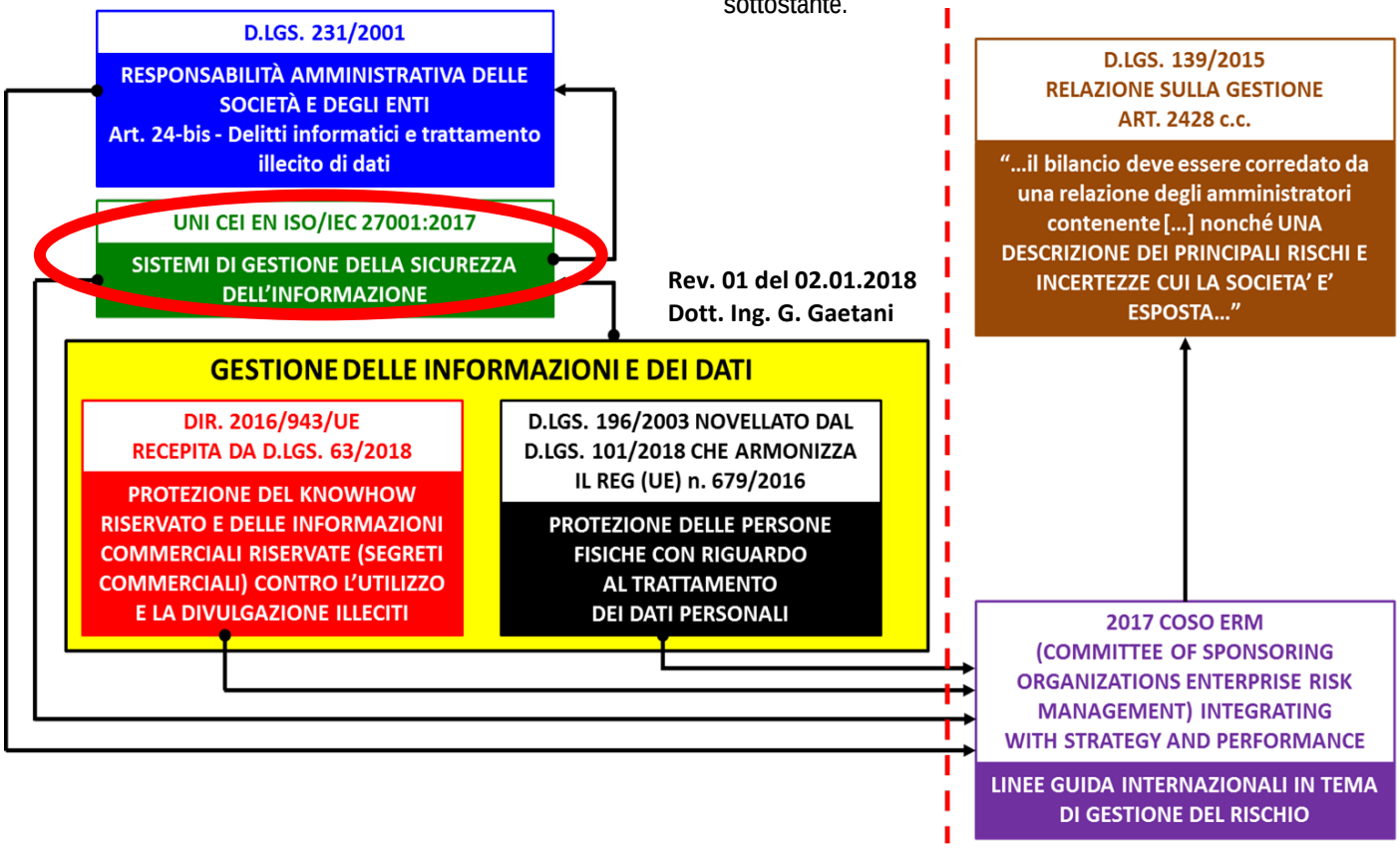
La "sicurezza delle informazioni" deve essere vista come un processo ad alto livello, indipendente dalla tecnologia, e tale da coinvolgere l'organo gestorio dell'azienda con una definizione di politica per la sicurezza (specificazione degli obiettivi che l'organizzazione si propone di conseguire) e con la progettazione di un sistema di governo (complesso di procedure attuato e mantenuto dall'organizzazione per garantire nel tempo il soddisfacimento della politica per la sicurezza).
La "sicurezza delle informazioni" si suddivide quindi in SICUREZZA ORGANIZZATIVA (progettazione, documentazione e gestione dei modelli organizzativi per monitorare le performance e i rischi i funzione di un miglioramento continuativo), SICUREZZA LOGICA O ATTIVA (individuazione delle tecniche per rendere sicure le informazioni riservate con autenticazione e autorizzazione dell'utente nel sistema; il monitoraggio viene condotto con attività di "accountability"), SICUREZZA FISICA O PASSIVA (impedimento ad utenti non autorizzati che possano accedere a risorse, sistemi, impianti, dispositivi, informazioni e dati di natura riservata, con un livello fisico e materiale tale, ad esempio, da porre i server in luoghi sicuri, dotati di sorveglianza e controllo accessi nonché individuare sistemi di protezione da danni).

Un "Sistema di gestione della sicurezza delle informazioni" (opportunamente progettato, documentato ed efficacemente attuato con il coinvolgimento attivo di tutti i portatori di interesse dell'organizzazione) consente all'azienda di mantenersi aggiornata su nuove minacce e vulnerabilità nonché di valutarle in modo sistematico; fornisce il trattamento di incidenti e perdite in ottica di prevenzione e miglioramento continuativo del sistema stesso; permette di implementare la politica e le procedure in accordo all'evoluzione dello "stato dell'arte" e del "risk management".

2. IL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI IN UNA VISIONE OLISTICA DELL'IMPRESA

Per allocare in modo organico il "Sistema di gestione della sicurezza delle informazioni" è necessario avere una visione olistica della impresa e quindi un collegamento con altri adempimenti dettati da norme tecniche e/o giuridiche.

La mappa cognitiva della "sicurezza delle informazioni" in riferimento al Sistema di Gestione (UNI CEI EN ISO/IEC 27001:2017) e ai collegamenti con la Responsabilità amministrativa degli enti (D.Lgs. 231/01) nonché alle norme giuridiche relative alla protezione delle informazioni commerciali riservate (D.Lgs. 63/2018) e alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali (D.Lgs. 196/2003 novellato dal D.Lgs. 101/2018) è rappresentata nella figura sottostante.



UNA IMPRESA DELLA CONOSCENZA E DI SERVIZI INNOVATIVI
GRUPPO 2G MANAGEMENT CONSULTING
Gruppo 2G Management Consulting s.r.l.
Largo Re Umberto, 106 • 10128 - Torino Tel. 011. 50.50.62 (r.a.) • Fax 011. 50.46.60
www.gruppo2g.com e-mail: gruppo2g@gruppo2g.com

2019 NOTIZIE
n. 003 - GENNAIO 2019
LA CONOSCENZA GENERA LE IDEE PER L'INNOVAZIONE DELLE IMPRESE
Aggiornamenti legislativi, normativi, tecnologici e organizzativi per migliorare il sistema di gestione aziendale

Nel recente passato l'approccio delle aziende è stato quello di costituire unità organizzative dedicate ad ogni singola prescrizione senza un coordinamento globale. Tale approccio ha portato a sostenere costi aggiuntivi e a generare inefficienze nell'implementazione e gestione di aspetti che, pur presentando caratteristiche diverse, richiedevano la stessa impostazione, prevedevano ruoli e responsabilità affini e necessitavano di procedure e istruzioni dalle forti analogie. Per questo motivo è importante intraprendere il cammino della integrazione delle procedure, dei modelli di analisi e delle strutture organizzative per favorire sinergie e aumentare l'efficienza interna (raggiungimento dell'obiettivo al minor costo!).

3. LA NORMA TECNICA UNI CEI EN ISO/IEC 27001:2017

La norma tecnica UNI CEI EN ISO/IEC 27001:2017 recepisce la ISO/IEC 27001:2013 incorporando due Corrigendum (emessi dall'ISO nel 2014 e 2015). Il primo corrigendum riguarda il requisito A.8.1.1.: l'inventario, la classificazione e trattamento degli "asset" riguarda ora anche le "informazioni" cui gli asset sono associati. Il secondo corrigendum riguarda il requisito 6.1.3: la Dichiarazione di Applicabilità deve specificare se sono implementati o meno i "controlli necessari", e non solo i controlli riferiti all'Annex A.

La struttura documentale della UNI CEI EN ISO/IEC 27001:2017 ricalca la direttiva operativa "ISO/IEC Directives, Part 1, Consolidated ISO supplement, 2013, Annex SL, Appendix "; infatti la complessità del sistema economico e sociale, le esigenze dinamiche del mondo industriale e delle autorità di regolazione del mercato, la proliferazione di norme tecniche per soddisfare le esigenze delle molteplici parti interessate, hanno spinto l'ISO/IEC (International Organization for Standardization/International Electro-technical Commission) ad emanare nel 2013 tale direttiva operativa chiamata anche "Struttura Generale di Alto Livello HLS".

Si tratta di una struttura comune che definisce i requisiti minimi nei Sistemi di Gestione (Management System Standard – MSS) che resterà invariata mentre saranno aggiunte sottoclausole e testi specifici per ogni aspetto (qualità, ambiente, sicurezza, rischi, compliance, sicurezza delle informazioni…).

Questa direttiva operativa della ISO/IEC nasce come una evoluzione dei sistemi di management che, nella dinamicità del mercato e della transizione del business, richiede anche una ridefinizione dell'organizzazione e quindi una capacità di innovare la gestione d'impresa.
La documentalità è costituita dal Manuale del Sistema di Gestione per la Sicurezza delle Informazioni, nonché dalle Procedure Operative per i controlli.
L'indice del Manuale è il seguente:

1	SCOPO E CAMPO DI APPLICAZIONE	
2	RIFERIMENTI NORMATIVI	
3	TERMINI E DEFINIZIONI	
4	CONTESTO DELL'ORGANIZZAZIONE	4.1 Comprendere l'organizzazione e il suo contesto 4.2 Comprendere le necessità e le aspettative delle parti interessate 4.3 Determinare il campo di applicazione del Sistema di Gestione per la sicurezza delle informazioni 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 6.2 Obiettivi per la sicurezza delle informazioni e pianificazione per consigli
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 della direzione
10	APPENDICE	A Obiettivi di controllo e controlli di riferimento

Gli obiettivi di controllo e i controlli elencati nell'allegato A sono ripresi direttamente dalla ISO/IEC 27002 (punti da 5 a 18) e allineati ad essi. Gli obiettivi di controllo e i controlli presentati in questa tabella non sono esaustivi e un'organizzazione può considerare che siano necessari obiettivi di controllo e controlli aggiuntivi.
Gli obiettivi di controllo e i controlli di questa tabella devono essere selezionati nella conduzione dei processi del sistema di gestione per la sicurezza delle informazioni, come specificato al punto 6.1.3 (Trattamento del rischio relativo alla sicurezza delle informazioni).

UNA IMPRESA DELLA CONOSCENZA E DI SERVIZI INNOVATIVI
GRUPPO 2G MANAGEMENT CONSULTING
Gruppo 2G Management Consulting s.r.l.
Largo Re Umberto, 106 • 10128 - Torino Tel. 011. 50.50.62 (r.a.) • Fax 011. 50.46.60
www.gruppo2g.com e-mail: gruppo2g@gruppo2g.com

2019 NOTIZIE
n. 003 - GENNAIO 2019
LA CONOSCENZA GENERA LE IDEE PER L'INNOVAZIONE DELLE IMPRESE
Aggiornamenti legislativi, normativi, tecnologici e organizzativi per migliorare il sistema di gestione aziendale

I punti dal 5 al 18 della ISO/IEC 27002 forniscono consigli e guida sulle migliori prassi a supporto dei controlli specificati nei punti da A.5 a A.18:

A.5 Politiche di sicurezza
A.6 Organizzazione della sicurezza delle informazioni
A.7 Sicurezza delle risorse umane
A.8 Gestione degli asset
A.9 Controllo degli accessi
A.10 Crittografia
A.11 Sicurezza fisica e ambientale
A.12 Sicurezza delle attività operative
A.13 Sicurezza delle comunicazioni
A.14 Acquisizione, sviluppo e manutenzione dei sistemi
A.15 Relazione con i fornitori
A.16 Gestione degli incidenti relativi alla sicurezza delle informazioni
A.17 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa
A.18 Conformità

Tali punti sono alla base della formalizzazione di procedure operative che documentano le decisioni prese dall'organo amministrativo e dal management per garantire l'efficace attuazione, da parte dell'intera organizzazione, del Sistema di Gestione della sicurezza delle informazioni.

Le procedure sono il vero "focus" del Sistema e costituiscono un insieme di concetti tecnico-operativi orientati alla sicurezza unitamente a suggerimenti e raccomandazioni particolari per ogni fase del processo; definiscono altresì le responsabilità funzionali per un controllo preventivo.

4. INTEGRAZIONE DELLA ISO/IEC 27001:2017 CON ART. 24-bis ex D.Lgs. 231/2001, D.Lgs. 63/2018 e D.Lgs. 196/20013

La documentalità del Sistema di Gestione (Manuale e Procedure Operative) deve essere realizzata integrando le prescrizioni relative ai "Delitti informatici e trattamento illecito dei dati" nonché la "protezione del Know How e delle informazioni commerciali riservate" e la "protezione delle persone fisiche con riguardo al trattamento dei dati personali".

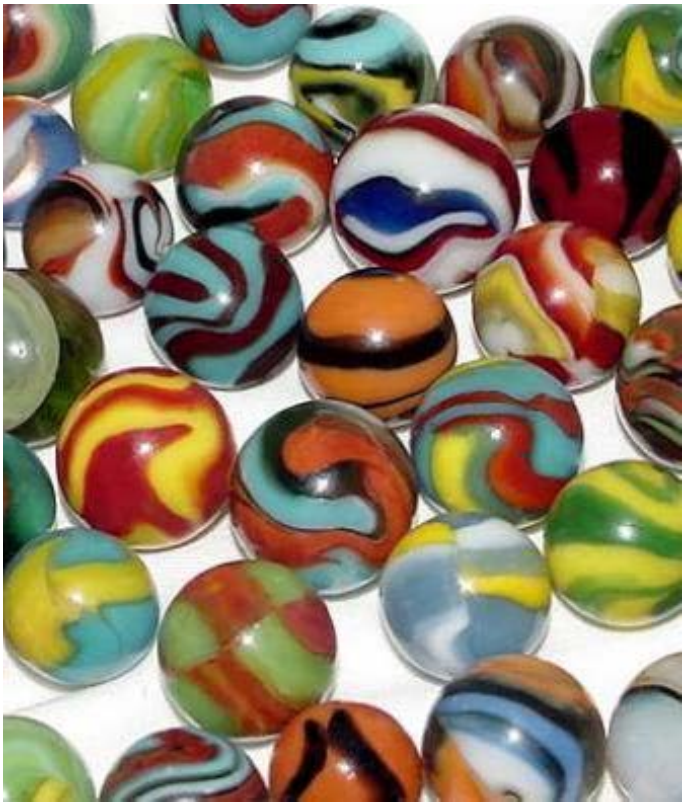
Poiché dal manuale e dalle Procedure Operative dipendono obblighi, azioni e responsabilità, la documentalità del Sistema di Gestione è una "forza sociale" capace di mobilitare le risorse umane dell'organizzazione, di spingerle ad agire nonché ad avere doveri e responsabilità per assicurare l'efficace attuazione delle decisioni prese in sede di progettazione del sistema.

La documentalità non può prescindere inoltre da una analisi e gestione dei rischi (risk management), relativi al trattamento illecito dei dati, (compresi quelli personali) nonché alla perdita di informazioni tecnico-commerciali riservate (sottrazione impropria e/o errato trattamento).

Il risk management è uno strumento di governance che mira alla gestione del rischio per mitigare l'effetto della incertezza nell'organizzazione aiutando l'organo amministrativo ed i manager a compiere le scelte (compreso le modalità di gestione della sicurezza delle informazioni) in funzione degli obiettivi della strategia competitiva.

È in questo solco che è stato pubblicato dal CoSO (Committee of Sponsoring Organizations of the Tread Commission) nel 2017 il nuovo framework "Enterprise Risk Management – Integrating Stategies and Performance" che favorisce l'allineamento tra obiettivi di performance e ERM (Enterprise Risk Management). Presenta nuovi approcci al rischio finalizzati al raggiungimento degli obiettivi in un contesto in cui la complessità del business è in continuo mutamento.

È evidente l'importanza dell'ERM nel processo di pianificazione strategica che enfatizza la visione globale della stessa ERM in ragione del fatto che il rischio gioca un ruolo fondamentale in termini di impatto sulla strategia e la performance nell'intera organizzazione.



UNA IMPRESA DELLA CONOSCENZA E DI SERVIZI INNOVATIVI
GRUPPO 2G MANAGEMENT CONSULTING
Gruppo 2G Management Consulting s.r.l.
Largo Re Umberto, 106 • 10128 - Torino Tel. 011. 50.50.62 (r.a.) • Fax 011. 50.46.60
www.gruppo2g.com e-mail: gruppo2g@gruppo2g.com

2019

NOTIZIE

n. 003 - GENNAIO 2019

LA CONOSCENZA GENERA LE IDEE PER L'INNOVAZIONE DELLE IMPRESE

Aggiornamenti legislativi, normativi, tecnologici e organizzativi per migliorare il sistema di gestione aziendale

5. IL RUOLO DEL GRUPPO 2G MANAGEMENT CONSULTING

Il Gruppo 2G Management Consulting è "un'impresa della conoscenza e di servizi innovativi" che opera oramai da 31 anni e, con i suoi attuali 22 consulenti sistemisti ed esperti, è in grado di progettare ed attivare Sistemi di Gestione rispondenti alle specifiche esigenze delle diverse tipologie e dimensioni di imprese.

Il Gruppo 2G segue sin dal 1988 l'evoluzione dei Sistemi di Gestione fornendo servizi di progettazione, documentazione ed attivazione della "Sicurezza delle Informazioni". Dal 2013, con l'introduzione della "struttura generale ad alto livello" (HLS) e con l'approccio olistico della organizzazione e gestione aziendale c'è stata una innovazione nella progettazione e documentazione dei Sistemi.

Inoltre l'evoluzione della "scienza del management", a seguito delle nuove esigenze di mercato, ha determinato la necessità per il Gruppo 2G di costituire un team multidisciplinare in grado di affrontare l'evoluzione dei Sistemi di Gestione con competenze nell'ambito delle strutture societarie, dell'organizzazione, dei processi aziendali, della legislazione d'impresa e della rilevazione dei rischi.

Un team per progettare un Sistema di Gestione aziendale in grado di ridurre risorse e costi e aumentare l'efficacia per la creazione di valore dell'impresa.

Nell'ambito delle INIZIATIVE CULTURALI promosse dal Gruppo 2G per il 2019, è stata inserita anche una ATTIVITÀ GRATUITA DI INFORMAZIONE E FORMAZIONE per i componenti del Consiglio di Amministrazione e per i Responsabili di Funzione relativamente al SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Se volete fissare un appuntamento con i nostri esperti per una presentazione del Sistema di Gestione della Sicurezza delle informazioni potete contattare il ns. Ufficio Marketing:
Sig.ra Cristina Gagliardo
Tel. 011 505062 - Fax 011 504660
e-mail: c.gagliardo@gruppo2g.com

UNA IMPRESA DELLA CONOSCENZA E DI SERVIZI INNOVATIVI

GRUPPO 2G MANAGEMENT CONSULTING

Gruppo 2G Management Consulting s.r.l.
Largo Re Umberto, 106 • 10128 - Torino Tel. 011. 50.50.62 (r.a.) • Fax 011. 50.46.60
www.gruppo2g.com e-mail: gruppo2g@gruppo2g.com