Politica sulla sicurezza dell' informazione in Azienda riguardo l'utilizzo dei telefoni cellulari

Questo documento ha come obiettivo quello di aiutare le aziende ad attuare una Politica sulla Sicurezza delle Informazioni (ISO/IEC 27002) riguardo l'uso dei telefoni cellulari.

- **SCOPO**

Lo scopo di questo documento è quello di definire gli standard per l'uso del telefono cellulare nell' -Azienda- al fine di proteggere le informazioni riservate. Questi standard sono stati stabiliti per minimizzare i danni, agli individui e all' -Azienda-, derivanti da una involontaria esposizione di informazioni riservate e comunicazioni confidenziali.
I danni includono la perdita di informazioni riservate e confidenziali riguardanti l'-Azienda- e gli individui, la perdita della proprietà intellettuale, danni all'immagine aziendale, danni all'infrastruttura o l' aumento dei pericoli per i dipendenti dell' -Azienda-.

- **CAMPO DI APPLICAZIONE**

Questa politica è rivolta a tutti i dipendenti dell' -Azienda-, imprenditori ed agenti quando usano il telefono cellulare per questioni aziendali o per trattare di affari aziendali (sia se il cellulare è di proprietà / pagato dall'azienda che non).

- **LINEE GUIDA**

1. **Generale**
   I cellulari consentono agli impiegati di portare avanti il business aziendale in modo più efficace ed efficiente. Tuttavia, come per tutti gli altri sistemi di comunicazione elettronici (come le e- mail), anche i cellulari offrono la possibilità a criminali e ad altri malfattori di ottenere l'accesso ad informazioni riservate dell' -Azienda-.
   E' responsabilità di tutti gli impiegati, imprenditori ed agenti dell'-Azienda- intraprendere un percorso formativo responsabile, per garantire la sicurezza delle loro chiamate su telefoni cellulari e seguire le linee guida consigliate in questo documento.

2. **Informazioni riservate e confidenziali**

   Il criterio su quando l' informazione debba essere considerata riservata o confidenziale non è stato precisamente definito (nota: in alcune aziende, le varie tipologie di informazioni sono definite formalmente e questa parte del documento può non essere necessaria o appropriata). Tuttavia, si può considerare riservata ogni tipo di informazione che, se comunicata in maniera inappropriata, può cagionare un danno materiale all'-Azienda- o ai sui dipendenti. L'informazione descritta in questa categoria può riguardare:

- Informazioni classificate formalmente da un atto ufficiale (es: Confidenziale, Riservato, Segreto).
- Informazioni caratterizzate da disposizioni governative come Sarbanes-Oxford o HIPPA.
- Informazioni ricevute da altri sotto l'accordo di NON DIVULGAZIONE o contrassegnate come private o confidenziali.
- Dati finanziari (es: le previsioni di vendita).
- Informazioni commerciali riguardanti lo status, le operazioni e il lavoro interno al business aziendale.
- Informazioni riguardanti la proprietà intellettuale dell'-Azienda-.
- Informazioni che incidono sulla privacy degli individui, come informazioni personali protette da un sistema di sicurezza dei dati o riguardanti le leggi sulla privacy, come i Regolamenti di Conservazione dei Dati.
- Informazioni che incidono sulla sicurezza degli individui: per esempio i piani di viaggio in zone dove la sicurezza personale è nota per essere un problema.

3. **Rischi di valutazione (sostituisci con le regole formali se disponili)**

In assenza di una formale classificazione dell'informazione, gli impiegati possono utilizzare alcuni criteri per determinare la riservatezza dell'informazione comunicata.
Alcuni di questi criteri sono:

- La segretezza e la riservatezza dell' informazione.
- La longevità dell' informazione (informazioni che diventano velocemente obsolete possono avere un grado di rischio relativamente basso).
- Urgenza della comunicazione (confrontare la potenziale perdita derivante dal non comunicare l'informazione con la perdita se fosse intercettata).
- Probabilità di essere intercettati (prendere in considerare il luogo in cui si effettua la chiamata e i fattori ambientali).

4. **Gestione del telefono**

I telefoni cellulari sono intrinsicamente aperti allo sfruttamento e all' intercettazione. Per ridurre la probabilità di tali rischi e minimizzare il pericolo dell' intercettazione:

- Mai lasciare il cellulare incustodito (es: nelle stanze di hotel), dove può essere facilmente manomesso. Bastano pochi secondi perchè il telefono venga compromesso.
- Imposta sempre un PIN / una password per il tuo telefono, che si attivi sia al momento dell' accensione sia quando il telefono è in modalità stanby.
- Assicurati che il Bluetooth, gli Infrarossi e gli altri metodi di trasferimento dati siano disattivati quando non usi il cellulare, richiedi una password / un PIN e connettiti solo a sorgenti sicure.

- Non installare software o allegati alle e-mail sul tuo cellulare, a meno che non sia del tutto certo che vengano da fonti sicure.
- Quando non lo usi, rimuovi la batteria dal tuo cellulare durante incontri riservati per ridurre il rischio di una intercettazione contro la tua piattaforma.

5. **Luoghi della chiamata**
   Devi assicurarti che tu e la persona con cui stai parlando siate in un ambiente sicuro prima di iniziare una discussione confidenziale o prima di trasmettere informazioni riservate via cellulare. Un ambiente sicuro è un ambiente in cui hai la certezza che non sarai ascoltato di nascosto. Per evitare dubbi, i trasporti pubblici (aerei, treni), le aree di attesa pubbliche, i ristoranti e gli altri posti pubblici non dovrebbero essere usati come luogo per discutere di informazioni riservate. E' una ipotesi sbagliata quella di considerare che le persone attorno a te non abbiano alcun interesse nell' ascoltare le tue conversazioni.

6. **Pratica nella chiamata**

   Per ridurre il rischio di una intercettazione telefonica:
   - Non pensare mai che la tua conversazione sia al sicuro, specialmente quando fai chiamate internazionali. In alcuni stati, i cellulari non hanno alcun sistema di cifratura e sono molto soggetti alle intercettazioni.
   - Fai in modo che i possibili intercettatori ottengano informazioni incomplete e inutili dalla tua conversazione (es: riferisciti a "quel cliente che hai incontrato la scorsa settimana", piuttosto che dire il suo vero nome).
   - Dove le parole in codice sono frequentemente utilizzate, per esempio riguardo i nomi dei clienti, assicurati che queste siano usate uniformemente. Sii coerente, non mischiare parole in codice con i nomi dei clienti.
   - Per le conversazioni che trattano di informazioni confidenziali e riservate, utilizza un software per la cifratura delle chiamate sicuro. L'uso di un software per cifrare le chiamate è obbligatorio per le conversazioni che trattano di informazioni riservate e confidenziali all'estero.
   - Non pensare che le chiamate di " routine " siano meno riservate di quelle " importanti ". Infatti, le chiamate giornaliare riguardo le vendite o quelle col management di solito contengono molte informazioni riservate e confidenziali per i potenziali ascoltatori.
   - Durante una chiamata in conferenza, fai particolare attenzione al fatto che tutti i partecipanti siano in un ambiente sicuro e che tutti gli interlocutori siano autenticati.
   - Se non fosse possibile stabilire una chiamata riservata, non dare informazioni confidenziali. Cerca di organizzarti in modo tale da poter iniziare una conversazione riservata in seguito.