POLITICA AZIENDALE SULLA SICUREZZA INFORMATICA

SUOLO E SALUTE con la presente Politica aziendale sulla sicurezza informatica intende contribuire alla massima diffusione della cultura della sicurezza in Azienda, evitando che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza dei sistemi informatici/informativi e nel trattamento dei dati. La sicurezza informatica è finalizzata *"alla salvaguardia della riservatezza, integrità e disponibilità delle informazioni gestite dall'organizzazione".*

Premessa

Il presente documento contiene la descrizione della struttura del sistema informatico e dell'architettura informativa, nonché delle pratiche di sicurezza e privacy e della strategia dei controlli.

Parte integrante del documento è rappresentata dal "Regolamento per la sicurezza informatica" dove sono esplicitamente elencate le misure organizzative e comportamentali che i dipendenti, i collaboratori a qualsiasi titolo dell'Azienda, sono chiamati ad osservare per contrastare i rischi informatici.

Destinatari

Il Sistema informatico risponde ad usi ed obiettivi aziendali e l'operatore che lo utilizza deve orientare il suo comportamento al perseguimento di tali scopi; deve altresì rispettare i principi etici e di correttezza, nonché la privacy e la segretezza dei dati trattati secondo le normative vigenti.

Sono destinatari del presente documento tutti i collaboratori di SUOLO E SALUTE con rapporto di lavoro subordinato (di qualsiasi tipologia) e coloro che svolgano, a qualsiasi titolo, attività per conto di SUOLO E SALUTE, accedendo al sistema informatico di quest'ultimo.

Responsabilità

La società gestisce la specifica attività tramite uno specifico ufficio IT (Information Tecnology) con sede a Lamezia Terme.

STRUTTURA E LOGISTICA

La società svolge attività di controllo e certificazione. L'ambito di operatività è il settore agro-alimentare e la missione aziendale è il miglioramento continuo della gestione e della qualità di servizi che la società è in grado di fornire e propone i propri servizi a tutti i soggetti presenti sui mercati nazionali ed internazionali con competenza, senza discriminazioni, in piena trasparenza, affidabilità ed imparzialità in accordo alle disposizioni previste dalle norme UNI CEI ENISO/IEC 17021:2006 e ISO/IEC 17065:2012.

L'attività della società viene svolta attraverso 16 uffici territoriali e tre aree principali: Direzione Generale, con sede a Bologna, Direzione Amministrativa, con sede a Fano, e Direzione Software (IT) con sede a Lamezia Terme.

La struttura è organizzata con server interni sui quali è configurato il gestionale aziendale

(WinSuolo) oltre che la gestione delle presenze del personale. I server interni sono configurati per comunicare tra di loro tramite VPN e per effettuare un backup notturno con copia fisica su server online oltre che con copie incrociate tra i vari server.
E' in fase di realizzazione una piattaforma web che sostituirà l'attuale gestionale aziendale. In hosting esterno, invece, vengono gestiti il sito ufficiale e la piattaforma e-learning, la contabilità generale e fiscale, l'archiviazione ottica della documentazione, le ispezioni informatizzate per il biologico, le transazioni per il biologico; infine, sempre su server esterni, vengono gestiti vari servizi di consultazione dei dati (documenti giustificativi e certificati di conformità, approvazione etichette).

Accesso ai locali server

L'accesso ai locali dove sono collocati i server interni, ai fini della riduzione dei rischi derivanti dall'ingresso di soggetti non autorizzati, per la tutela della sicurezza delle persone, dell'edificio, delle attrezzature e dei dati è riservato ad un referente di ciascun ufficio, nominato dal responsabile dello stesso.
Le persone esterne, autorizzate all'accesso per manutenzione degli hardware e/o l'aggiornamento dei software sono regolati da contratto e gli accessi sono registrati su apposita scheda.

Protezione e Antivirus

L'antivirus è un software creato per prevenire, rilevare ed eventualmente rendere inoffensivi codici dannosi e malware per un computer come virus, adware, backdoor, BHO, dialer, fraudtool, hijacker, keylogger, LSP, rootkit, spyware, trojan, worm o ransomware. L'*antivirus* viene costantemente aggiornato ed ha in continua esecuzione le funzioni di scansione in tempo reale. Per un miglior utilizzo l'utente deve avviare con regolarità la scansione dei dispositivi del PC (dischi fissi, CD, DVD *o* altri supporti di memorizzazione), per verificare la presenza di *virus*, *worm* e quant'altro. Per evitare la diffusione di virus è inoltre utile controllare tutti i file che si ricevono o che vengono spediti tramite posta elettronica facendoli verificare dall'*antivirus* correttamente configurato a tale scopo.
Generalmente un antivirus non è in grado di proteggere un computer da tutte le minacce informatiche esistenti in quanto ci sono delle attività (gestione della posta elettronica, consultazione di siti web) che posso sfuggire al controllo dell'antivirus. A tale scopo, la società ha posto in essere una piattaforma di "Security Awareness" (Consapevolezza della Sicurezza) per far sì che tutti i collaboratori abbiano una buona conoscenza e un corretto atteggiamento nei confronti della protezione dei beni fisici e soprattutto informativi della società.

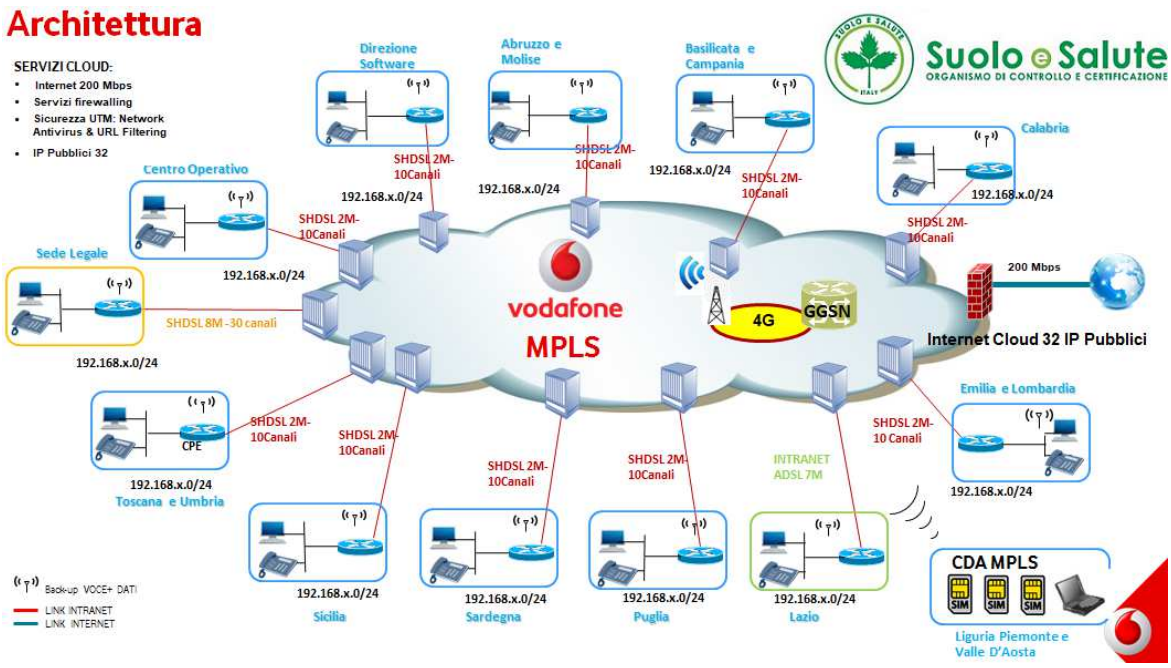
Sito web, servizi online e piattaforma e-learning

Attraverso un server dedicato, in hosting esterno, la società rende fruibile il proprio sito web, alcuni servizi di consultazione online e una piattaforma e-learning.

Accesso ad internet

L'azienda ha posto in essere, già da qualche anno e in collaborazione con Vodafone, una

struttura informatica in cloud per garantire la sicurezza della rete aziendale, per limitare l'accesso a determinati siti (url filtering) e per monitorare l'accesso al web. Grazie ad infrastrutture di ultimissima generazione Rete Unica Dati (MPLS) offre avanzati servizi di sicurezza in grado di garantire elevati standard di protezione dei dati scambiati tra le sedi dell'azienda e attraverso Internet. La soluzione di accesso ad Internet "da Rete Vodafone" identifica il caso di Firewall On Cloud e prevede il raggiungimento della Rete Pubblica attraverso un network firewall situato all'interno dei Data Center di Vodafone. Sulla base delle nostre specifiche esigenze è stato identificato e configurato all'interno del network firewall un dominio virtuale, denominato VDOM, completamente dedicato alla ns azienda. In virtù della ridondanza geografica dei Data Center e del concetto di security in Cloud, il firewall risulta nativamente in alta affidabilità, pertanto, in caso di disservizio, tale soluzione è in grado di garantire la continuità del servizio. Inoltre, essendo il firewall un servizio di managed security, la ns azienda è sollevata dalle ordinarie attività di manutenzione e di gestione dello stesso, demandando la complessità operativa al fornitore del servizio.



Infine, l'azienda ha messo a disposizione di ogni singolo pc, notebook, smartphone un antivirus: Eset EndPoint Antivirus (per pc e notebook) e Lookout for work (per smartphone), entrambi con gestione centralizzata delle licenze tramite piattaforma online.

SICUREZZA, PRIVACY e CONTROLLI

Premesso che una sicurezza informatica aziendale totale, cioè garantita al 100%, è un'utopia, è comunque sempre bene ricordare che non esiste protezione senza una "politica della security", intesa come disegno strategico tale da definire, organizzare la riservatezza e integrità informatica e gestire tutti gli aspetti ad essa collegati**,** da quelli tecnici a quelli di management e di business, incluse la confidenzialità e disponibilità dei dati.

La politica aziendale è riassunta nello slogan: consapevolezza, competenza e perizia, perchè si

ritiene che l'attività di prevenzione debba essere prevalente rispetto all'attività di controllo.

Sicurezza e Privacy

L'Azienda si impegna pertanto a potenziare in misura crescente tale attività di prevenzione, in particolare tramite azioni di sensibilizzazione e di diffusione dei principi e delle regole da osservare nell'utilizzo della strumentazione informatica, nell'adozione di specifiche soluzioni tecnologiche e di ogni altra misura ritenuta idonea a tal fine.

La piattaforma di "Security Awareness" per la *Consapevolezza della Sicurezza* è sicuramente lo strumento principale per far sì che tutti i collaboratori abbiano una buona conoscenza e un corretto atteggiamento nei confronti della protezione dei beni fisici e soprattutto informativi della società.

La diffusione del "regolamento per la sicurezza informatica" che riassume l'insieme delle buone pratiche indispensabili per preservare la salvaguardia della riservatezza, dell'integrità e della disponibilità delle informazioni aziendali quale strumento per sviluppare la *Competenza di Sicurezza* di ciascun operatore dell'azienda.

L'Amministrazione si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto delle normative vigenti, della presente politica della sicurezza e delle buone pratiche indicate nel regolamento al fine di verificare la perizia, da parte degli attori coinvolti, nella pratica della sicurezza.

Controlli

I controlli sono effettuati per le seguenti finalità:

a) evitare che vengano compiuti comportamenti impropri e/o potenzialmente dannosi per l'Amministrazione che possano comportare anche l'irrogazione di sanzioni disciplinari;

b) evitare o comunque ridurre i rischi di un coinvolgimento civile e penale dell'Azienda, per concorso di reato, nel caso di illeciti nei confronti di terzi commessi mediante l'utilizzo improprio dei beni messi a disposizione dall'Amministrazione stessa;

c) tutelare l'immagine dell'Azienda e di coloro che vi prestano la propria attività.

In nessun caso sono effettuati controlli mirati e ripetuti nei confronti di soggetti specifici con finalità discriminatorie o persecutorie o volutamente sanzionatorie; i controlli sono in ogni caso effettuati rispettando la dignità e la libertà personale dei soggetti sottoposti a controllo, nonché garantendo la riservatezza dei dati personali raccolti durante la procedura di controllo. I dati sono conosciuti soltanto dai soggetti preventivamente designati quali responsabili e incaricati del trattamento.

I controlli vengono effettuati dal Responsabile della Direzione Software nel rispetto delle normative vigenti e dello Statuto dei Lavoratori

Aggiornamento e revisione

Il presente documento è soggetto a revisione con frequenza periodica.

Allegati

Regolamento per la sicurezza informatica.