0	01/03/24	PRIMA EMISSIONE	 Cini	 Beraldo
REV.	**DATA** *DATE*	**DESCRIZIONE** *DESCRIPTION*	**PREPARATO** *PREPARED*	**APPROVATO** *APPROVED*
QUALITA'	*Policy Cybersecurity_R0.doc*	**Sistema Gestione Qualità**		
COMMESSA N° *JOB NUMBER*	**IDENTIFICATIVO FILE** *FILE NAME*			
INTERPROGETTI GENOVA ENGINEERING & CONSULTING		**Policy generale di cybersecurity**		
DOCUMENTO NUMERO: *DOCUMENT NUMBER:*	**Policy Cybersecurity**		**N° TOT PAGINE INCLUSA QUESTA** *N° TOTAL OF PAGE INCLUDING THIS:*	17

Sommario

1 Note sulla sicurezza e l'aggiornamento del documento.

- Il presente documento è stato classificato come "CONFIDENZIALE" secondo le linee guida di riferimento in merito alla classificazione del dato di Sababa Security.
- Il presente documento deve essere gestito con attenzione per evitare accessi non autorizzati. Questo è valido per le versioni elettroniche come per le versioni cartacee.

2 Finalità e applicabilità

La presente Policy ha lo scopo di definire e chiarire l'impegno della direzione, gli obiettivi, i principi, i ruoli e le responsabilità in materia di sicurezza delle informazioni all'interno di Interprogetti.

La presente Policy si applica a tutti gli utenti dei sistemi Interprogetti e a tutte le persone che hanno accesso ai Sistemi Interprogetti e al Sistema Informativo ed è allineata agli obiettivi del Framework Nazionale per la Cybersecurity e la Data Protection.

NOTA IMPORTANTE: I termini della presente Informativa si applicano in tutto il mondo. In caso di conflitto tra la presente Informativa e le leggi locali applicabili, prevarranno le leggi locali. Nel caso in cui non vi sia conflitto tra la Policy e la legge locale applicabile, ma la Policy impone uno standard più elevato e/ o requisiti più onerosi rispetto alle leggi locali, prevarranno gli standard più elevati e/ o requisiti più onerosi della Policy.

3 Cyber Security

La presente Policy stabilisce che il management si impegna a fornire direzione e supporto alla sicurezza delle informazioni in conformità alle esigenze aziendali di Interprogetti e in linea con le leggi e i regolamenti in cui Interprogetti opera.

3.1 Dichiarazione di impegno per la sicurezza delle informazioni

I Sistemi Informativi ed Informatici sono Asset critici e di vitale importanza per Interprogetti.

Senza informazioni affidabili, l'attività sarebbe a rischio significativo. In Interprogetti, abbiamo il dovere nei confronti dei nostri Utenti, Clienti e Soci di garantire che la sicurezza delle informazioni che gestiamo sia trattata come alta priorità.

Interprogetti si impegna a proteggere le informazioni che elabora o memorizza in base al loro valore, sensibilità e ai rischi a cui sono esposte, e in modo coerente con i pertinenti requisiti legali, normativi e contrattuali.

I controlli di sicurezza delle informazioni sono incorporati nella cultura aziendale e, in quanto tali, è fondamentale che tutti gli utenti di Interprogetti abbiano una chiara comprensione di ciò che ci si aspetta da loro.

3.2 Obiettivi della sicurezza dell'informazione

L'obiettivo della Sicurezza delle Informazioni è quello di assistere nella protezione dei dati, nella comprensione delle minacce e dei rischi a tali dati e per assistere tutta l'azienda nel rispetto di eventuali leggi o regolamenti relativi ai dati in possesso della società.

Il raggiungimento di questi obiettivi contribuirà a garantire la continuità aziendale di Interprogetti.

3.3 Rischi coperti e conseguenti benefici

Le attività riguardanti le informazioni sono mantenute a livelli di sicurezza accettabili, in modo da garantire la triade RID:

- **Riservatezza** - La protezione di informazioni preziose o sensibili da divulgazione o modifica non autorizzata sarà garantita.
- **Integrità** - La protezione contro le modifiche non autorizzate per salvaguardare l'accuratezza e la completezza delle informazioni viene mantenuta.

- **Disponibilità** - Il trattamento delle informazioni sarà opportunamente autorizzato e accessibile agli Utenti quando richiesto.

In questo modo, i seguenti rischi possono essere ridotti a un livello accettabile:

- **Perdita di competitività** a causa della perdita di proprietà intellettuale e di know-how
- **Danni alla reputazione** dovuti alla divulgazione di informazioni fornite da clienti e partner
- **Interruzione dei processi aziendali** o di produzione attraverso la compromissione del supporto del sistema IT

3.4 Conformità legale, normativa e contrattuale

I contenuti applicabili della presente Informativa sono inclusi in qualsiasi veicolo contrattuale relativo alle informazioni o ai Sistemi Informativi di Interprogetti.

3.5 Revisione delle politiche di sicurezza delle informazioni

L'approccio di Interprogetti alla gestione della sicurezza delle informazioni e della sua attuazione può essere esaminato in modo indipendente quando ritenuto opportuno dal management o quando si verificano cambiamenti significativi della sicurezza.

La verifica indipendente (condotta da audit interni o da fornitori esterni) sarà avviata dalla direzione Interprogetti e affronterà qualsiasi necessità di modifiche all'approccio alla sicurezza, cambiamento alla Policy di sicurezza e opportunità di miglioramento.

I risultati della revisione indipendente sono registrati e comunicati al Management. Tali registrazioni devono essere conservate e diffuse secondo necessità.

3.6 Mancato rispetto dei principi della Policy

Il mancato rispetto dei principi di questa Policy potrebbe comportare azioni disciplinari fino al licenziamento incluso (per i dipendenti). Le azioni disciplinari nei confronti di terzi avverranno attraverso opportuni canali contrattuali.

4 Organizzazione della sicurezza delle informazioni

4.1 Struttura organizzativa

La struttura organizzativa di Interprogetti è descritta nel documento “Organigramma 2020.pdf “.

La Sicurezza delle Informazioni è affidata al consulente esterno indicato mediante apposito contratto, di seguito chiamato Responsabile Informatico (RI).

La gestione dei dati personali in accordo con il GDPR è affidata ad altro consulente esterno indicato mediante apposito contratto.

Interprogetti identifica una persona all’interno del proprio al quale affidare la funzione di Coadiuvatore Informatico (CI), il quale ha la responsabilità di contattare il Responsabile Informatico (RI) qualora ci fosse necessità di interventi immediati causati da incidenti informatici.

5 Principi di sicurezza delle informazioni

Tutti, in quanto semplici utenti, progettisti, Project Manager, contribuiscono alla sicurezza delle informazioni, degli asset IT e dei prodotti digitali che aderiscono a questi principi.

5.1 Conservazione ed elaborazione delle informazioni

Le informazioni aziendali sono archiviate ed elaborate solo in ambienti IT controllati o approvati da Interprogetti.

5.2 Classificazione dei Dati

Secondo gli standard di Interprogetti, i dati sono classificati come segue:

Classificazione	Livello di Rischio	Descrizione	Esempi
Dati pubblici o non classificati	Basso	Dati di origine interna o esterna a cui hanno accesso i dipendenti o il personale autorizzato di Interprogetti e che non espongono Interprogetti ad alcun rischio con la sua pubblicazione e distribuzione. Terze parti autorizzate possono far circolare tali informazioni al di fuori dell'organizzazione.	Comunicati stampa o materiale di marketing sono classificati come pubblici.
Dati di uso interno	Medio	Contenuto di uso interno e dati che sono composti da informazioni proprietarie sufficienti da rendere imprudente il rilascio al pubblico, ma tutti i dipendenti possono accedere alle informazioni. I dati o i contenuti possono essere liberamente scambiati tra dipartimenti e società controllate. (I.e. Informazioni il cui pubblico è destinato a coloro che lavorano all'interno dell'organizzazione.)	Politiche e procedure aziendali, newsletter dei dipendenti, materiali di formazione generale, informazioni di contatto sul lavoro dei dipendenti.
Dati riservati	Alto	Informazioni personali e non personali che sono destinate all'uso all'interno della società. La sua divulgazione non autorizzata potrebbe avere un impatto serio e negativo sulla società, i suoi azionisti, i suoi partner aziendali e/ o i suoi ospiti. La divulgazione non autorizzata di un singolo dato può comportare implicazioni normative o legali.	Dati personali e sensibili (DL.196/03), dati di vendita, informazioni di pianificazione strategica e rapporti di revisione.

5.3 Password e identità

Le password sono un aspetto critico della sicurezza informatica. Una password debole o compromessa può causare l'accesso non autorizzato ai nostri dati più sensibili e/ o lo sfruttamento delle nostre risorse. Tutto il personale, compresi gli appaltatori e i fornitori che hanno accesso ai sistemi Interprogetti, è responsabile di adottare le misure appropriate, come descritto di seguito, per selezionare e proteggere le loro password.

Le password sono strettamente personali, devono essere mantenute sicure, riservate secondo la normativa vigente e non devono essere riutilizzate su sistemi diversi.

Il proprietario della password deve assicurarsi che nessuno possa vedere lo schermo o la tastiera mentre digita la sua password ed è responsabile dell'utilizzo della propria password.

Le password non devono mai essere rivelate a nessuno, tramite qualsiasi supporto (telefono, chat o e-mail).

È sconsigliabile la funzione "Ricorda password" delle applicazioni (ad esempio, browser web).

Ogni individuo che sospetta che la propria password possa essere stata compromessa deve segnalare l'incidente e modificare tutte le password rilevanti.

5.4 Conservazione e archiviazione dei dati

I dati devono essere conservati e archiviati in conformità con i requisiti legali e gli orientamenti interni (politiche di backup, riferirsi all'Annex 2 – Backup Policy).

5.5 Clean Desk e Clean Screen Guideline

Tutti gli utenti che hanno accesso ai sistemi informativi Interprogetti devono adottare una linea guida "Clean Desk" e "Clean Screen" per garantire una divulgazione limitata delle informazioni quando lasciano l'area di lavoro o condividono lo schermo del desktop. (riferirsi all'Annex 1- Clean Desk & Clean Screen e uso della mail aziendale)

5.6 Apparecchiature utente non presidiate

Gli utenti devono garantire che le apparecchiature non presidiate siano protette quando non sono in uso, utilizzando, ad esempio, la disconnessione o il blocco dello schermo/la protezione con password.

5.7 Viaggiare con risorse IT e beni fuori sede

Tutte le attrezzature situate al di fuori dei siti Interprogetti devono essere protette, almeno, come sarebbe se si trovassero all'interno di un sito Interprogetti.

5.8 Personal Equipment/ "Bring your own device" BYOD

È severamente vietato l'uso di dispositivi personali per la connessione alle reti interne Interprogetti all'interno degli spazi lavorativi. È consentito collegare apparecchiature personali e dispositivi privati a reti dedicate identificate come "Reti guest".

5.9 Terze parti

Le terze parti che accedono ai sistemi informativi Interprogetti da un dispositivo non Interprogetti devono rispettare la Policy di accesso remoto (riferirsi all'Annex 5 – Policy di Accesso Remoto).

Istruzioni specifiche sulla sicurezza delle informazioni devono essere incluse per le terze parti che gestiscono attività che coinvolgono informazione di Interprogetti.

5.10 Separazione delle funzioni

Si deve fare attenzione che nessuna persona possa accedere, modificare o abusare di risorse fisiche e logiche senza autorizzazione o rilevamento (non autorizzato o non intenzionale).

I compiti e i settori di responsabilità in conflitto sono separati per ridurre tali opportunità.

5.11 Principio dei privilegi minimi

L'accesso è concesso solo per le informazioni e i beni informatici necessari allo scopo previsto.

5.12 Contatto con le Autorità / Gruppi di interesse

Interprogetti mantiene contatti con le autorità competenti (ad esempio, fornitori di telecomunicazioni) o altri forum di sicurezza specializzati e associazioni professionali.

6 Sicurezza fisica e ambientale

La presente Policy definisce i controlli di sicurezza fisica necessari per prevenire:

- accesso fisico non autorizzato,
- danni e interferenze alle informazioni
- danni e interferenze a servizi di elaborazione delle informazioni (ad esempio, Server Room, sale di rete, armadi di telecomunicazioni, ecc.)
- danni causati da azioni umane e eventi ambientali ed esterni dannosi

La protezione fisica delle risorse IT è "sicura dalla progettazione" e definita in modo da impedire l'accesso fisico non autorizzato, danni e interferenze alle strutture di elaborazione delle informazioni e delle informazioni dell'organizzazione.

Il Management è responsabile di garantire i seguenti principi in materia di sicurezza fisica e ambientale.

6.1 Secure Areas

Le aree sicure sono siti in cui si gestiscono informazioni sensibili o si riparano preziose attrezzature IT e personale per raggiungere gli obiettivi aziendali. Nel contesto della sicurezza fisica, per "sito" si intendono gli edifici, le stanze o gli uffici che ospitano tutti i servizi e le strutture (elettricità, riscaldamento, aria condizionata). Nel caso di Interprogetti si identifica la Server Room come Secure Area.

6.2 Controlli fisici di entrata

Gli spazi di Interprogetti sono protetti da controlli all'ingresso gestiti dalla reception con l'utilizzo di un registro degli ingressi per fornitori esterni.

6.3 Protezione contro le minacce esterne e ambientali

Gli spazi di Interprogetti sono protetti contro i danni causati da incendi, inondazioni, terremoti, esplosioni, disordini civili e altre forme di calamità naturali o provocate dall'uomo grazie alle soluzioni di sicurezza fisica implementate, le quali proteggono anche la sicurezza delle informazioni.

6.4 Attrezzatura Ubicazione e protezione

Le attrezzature sono protette per ridurre i rischi di minacce ambientali, accessi non autorizzati e furti.

6.5 Utility di supporto

Le apparecchiature sensibili sono protette da interruzioni di corrente e interruzioni causate da guasti nelle utility di supporto (ad esempio, UPS, HVAC ridondante, linee elettriche ridondanti).

Cablaggio di sicurezza

I cavi di alimentazione e di telecomunicazione che trasportano dati o servizi informativi di supporto sono protetti da intercettazioni o danni (ad esempio armadi chiusi a chiave)

Manutenzione dell'attrezzatura

Tutte le apparecchiature sono manutenute così da garantire la disponibilità e l'integrità in conformità dei servizi associati.

Furto o perdita di beni IT

Qualsiasi perdita o furto di apparecchiature deve essere prontamente segnalato al Coadiuvatore Informatico (CI), o al Responsabile Informatico (RI), così da adottare tutte le contromisure necessarie per limitare il rischio dovuto all'evento.

Smaltimento sicuro o riutilizzo delle apparecchiature

Le apparecchiature contenenti supporti di memorizzazione devono essere controllate per garantire che i dati sensibili o il software concesso in licenza siano stati rimossi o sovrascritti prima del riutilizzo.

In caso di smaltimento i dispositivi devono essere manomessi fisicamente così da garantire l'impossibilità di recupero di eventuali informazioni di Interprogetti.

Etichettatura di attrezzature e beni

Le apparecchiature e i beni devono essere etichettati.

7 Segnalazione di incidenti

Tutti gli incidenti, gli attacchi, i malfunzionamenti, la perdita o il furto di sistemi informatici e l'accesso non autorizzato alle risorse informative di Interprogetti devono essere segnalati dal Coadiuvatore Informatico (CI) al Responsabile Informatico (RI) nella modalità ritenuta più efficaci e se necessario seguita da mail ufficiale.

Gli attacchi di ingegneria sociale devono essere segnalati alla gestione della linea e, se pertinente per le normative locali, alle autorità locali. (riferirsi all'Annex 6 – Gestione degli incidenti di sicurezza)

8 Gestione di questa Policy

Misure di attuazione e formazione

Questa Policy deve essere comunicata localmente per garantire che i dipendenti siano informati.

Gestione delle eccezioni

Tutte le richieste di scostamento da questa Policy devono essere inviate al Management via email.

L'approvazione dell'eccezione deve essere ottenuta per iscritto.

8.1 Proprietà, manutenzione e revisione dei documenti

Titolare del documento è il Coadiuvatore Informatico (CI) interno di Interprogetti che ha la responsabilità diretta di mantenere la presente Policy, fornendo consulenza e orientamento sulla sua attuazione ed è responsabile di garantire che la presente Policy sia rivista periodicamente, aggiornata e comunicata di conseguenza secondo le esigenze della Compagnia.

La modifica dell'organizzazione per la sicurezza delle informazioni, l'introduzione di nuove tecnologie, gli incidenti o le vulnerabilità gravi nonché le modifiche al panorama delle minacce e dei rischi comporteranno una revisione e, a seconda dei casi, daranno luogo a un aggiornamento di questa Policy.

Interprogetti si riserva il diritto di modificare la presente Informativa in qualsiasi momento e comunicare le modifiche di conseguenza.

Annex 1- Clean Desk & Clean Screen e uso della mail aziendale

Clean Desk & Clean Screen

Per mantenere la sicurezza e la privacy delle informazioni personali dei dipendenti e dei membri, tutti i dipendenti devono intraprendere azioni appropriate per impedire a persone non autorizzate di avere accesso alle informazioni, alle applicazioni o ai dati.

I dipendenti sono anche tenuti a fare un controllo coscienzioso del loro ambiente di lavoro circostante per garantire che non ci sia alcuna perdita di riservatezza ai supporti di dati o documenti.

Questa Policy si applica a:

- Day Planners che possono contenere informazioni non pubbliche,
- Armadi, armadi e valigette contenenti informazioni sensibili o riservate,
- Qualsiasi dato riservato o sensibile, inclusi report, elenchi o dichiarazioni,
- Dispositivi elettronici, compresi telefoni cellulari e PDA,
- Chiavi utilizzate per accedere alle informazioni sensibili,
- Stampe contenenti informazioni sensibili,
- Dati su stampanti, fotocopiatrici e/o fax,
- Postazioni di lavoro e password,
- Supporti portatili, come CD, dischi o unità flash,
- Scrivanie o aree di lavoro, comprese lavagne bianche e scaffali.

Uso corretto della mail aziendale

La posta elettronica aziendale non è privata. Gli utenti rinunciano espressamente a qualsiasi diritto alla privacy in tutto ciò che creano, memorizzano, inviano o ricevono sui sistemi informatici di Interprogetti. Interprogetti può, ma non è obbligato a, monitorare le e-mail senza previa notifica. Tutte le e-mail, i file e i documenti - comprese le e-mail personali, i file e i documenti - sono di proprietà di Interprogetti, possono essere soggetti a richieste di registrazioni aperte e possono essere accessibili in conformità con questa Policy.

Le e-mail in arrivo vengono analizzate per gli allegati di file dannosi. Se un allegato viene identificato come avente un'estensione nota per essere associata a malware, o incline ad abusi da parte di malware o attori cattivi o altrimenti comporta un rischio maggiore, l'allegato verrà rimosso dall'e-mail prima della consegna. Il rifiuto della posta elettronica viene ottenuto attraverso l'elenco di domini e indirizzi IP associati ad attori malintenzionati. Qualsiasi e-mail in arrivo proveniente da un noto attore malintenzionato non sarà consegnato. Qualsiasi account di posta elettronica che si comporti male inviando spam verrà chiuso. Verrà eseguita una revisione dell'account per determinare la causa delle azioni.

La posta elettronica deve essere utilizzata per scopi commerciali e in modo coerente con altre forme di comunicazione aziendale professionale. Tutti gli allegati in uscita vengono scansionati automaticamente alla ricerca di virus e codice dannoso. La trasmissione di un allegato dannoso può non solo danneggiare il sistema del destinatario, ma anche danneggiare la reputazione di Interprogetti.

Le seguenti attività sono vietate dalla Policy:

- Invio di e-mail che possono essere considerate intimidatorie, moleste o offensive. Questo include, ma non è limitato a: linguaggio abusivo, osservazioni o immagini sessualmente esplicite, parolacce, osservazioni diffamatorie o discriminatorie riguardanti razza, credo, colore, sesso, età, religione, orientamento sessuale, origine nazionale o disabilità.
- Utilizzo della posta elettronica per l'invio di SPAM o altre sollecitazioni non autorizzate.
- Violare le leggi sul copyright distribuendo illegalmente opere protette.
- Invio di e-mail utilizzando l'account di posta elettronica di un'altra persona, tranne quando è autorizzato a inviare messaggi per un altro mentre serve in un ruolo di supporto amministrativo.
- Creazione di una falsa identità per aggirare la Policy.
- Falsificare o tentare di falsificare messaggi di posta elettronica.
- Utilizzo di software di posta elettronica non autorizzato.

- Disabilitare consapevolmente la scansione automatica degli allegati su qualsiasi personal computer Interprogetti.
- Aggirare consapevolmente le misure di sicurezza della posta elettronica.
- Invio o inoltro di e-mail di battute, lettere a catena o lettere false.
- L'invio di messaggi non richiesti a grandi gruppi, ad eccezione di quanto richiesto per condurre affari Interprogetti.
- Inviare o inoltrare consapevolmente e-mail con virus informatici.
- Creazione o risposta per conto di Interprogetti senza approvazione della direzione

La posta elettronica non è sicura.

Gli utenti non devono inviare password, numeri di previdenza sociale, numeri di conto, numeri di pin, date di nascita, nome da nubile della madre, ecc. a soggetti esterni alla rete Interprogetti senza crittografare i dati.

Tutte le attività degli utenti sulle risorse del sistema informativo Interprogetti possono essere soggette a registrazione e revisione. Interprogetti dispone di software e sistemi per monitorare l'utilizzo della posta elettronica.

Gli utenti di posta elettronica non devono dare l'impressione di rappresentare, dare opinioni o fare dichiarazioni per conto di Interprogetti, a meno che non siano debitamente autorizzati (esplicitamente o implicitamente) a farlo.

Gli utenti non devono inviare, inoltrare o ricevere informazioni Interprogetti riservate o sensibili tramite account di posta elettronica non Interprogetti. Esempi di non-Interprogetti} account di posta elettronica includono, ma non sono limitati a, Hotmail, Yahoo mail, AOL mail, e e-mail forniti da altri Internet Service Provider (ISP). Gli utenti con dispositivi mobili non emessi da Interprogetti devono rispettare la Policy di utilizzo e sicurezza accettabile dei dispositivi personali per l'invio, l'inoltro, la ricezione o la memorizzazione di informazioni Interprogetti riservate o sensibili.

Uso incidentale

L'uso personale incidentale dell'invio di e-mail è limitato agli utenti approvati da Interprogetti; non si estende ai familiari o ad altri conoscenti. Senza previa approvazione della direzione, l'uso accidentale non deve comportare costi diretti per Interprogetti. L'uso accidentale non deve interferire con il normale svolgimento dei compiti di lavoro di un dipendente.

Nessun file o documento può essere inviato o ricevuto che possa causare responsabilità legale o imbarazzo per Interprogetti. L'archiviazione di file e documenti personali all'interno dei sistemi IT di Interprogetti dovrebbe essere nominale.

Le email non vengono cancellate, è presente uno storico che viene utilizzato per il recupero delle informazioni.

Annex 2 – Backup Policy

Scopo dei backup e criteri generali

Il backup dei dati dei sistemi informativi aziendali ha i seguenti obiettivi:

- proteggere i sistemi (applicazioni e dati) aziendali da eventi dirompenti, come guasti hardware, eventi catastrofici, errori umani, incongruenze causate da applicazioni software, ecc.
- per consentire il ripristino dei dati sia nella loro ultima versione (di solito dopo un evento distruttivo) che in una versione precedente (di solito a causa di specifiche circostanze operative)
- per proteggere i dati degli utenti dalla cancellazione o perdita accidentale.

Per raggiungere i suddetti obiettivi Interprogetti sviluppa quanto definito al capitolo 10.2.

I criteri di backup delle applicazioni e dei dati devono prendere in considerazione i seguenti aspetti:

- **frequenza di backup** (che in caso di ripristino è inversamente proporzionale alla quantità di dati da ripristinare),
- **conservazione dei dati di backup**, che indica quanto indietro nel tempo i dati possono essere ripristinati in caso di particolari circostanze operative,
- **sito di archiviazione**, ovvero il luogo in cui vengono conservati i dati di backup. Si consiglia di NON archiviare MAI i dati di backup nella stessa posizione del sistema che lo esegue; in particolare per i sistemi On Board, i supporti di backup devono essere memorizzati nell'armadio a prova di fuoco fuori dalla sala computer. In caso di dati critici non memorizzare i supporti di backup all'interno dei locali aziendali, per proteggerli da possibili disastri (furti, incendi, inondazioni).

Creazione e retention dei backup

Al fine di garantire il risultato positivo, così come la qualità dei dati e le operazioni di ripristino del sistema, il Responsabile Informatico (RI) ha definito una Policy, descritta di seguito, che si basa sulla premessa che tutti i sistemi aziendali sono integralmente backuppati, e quindi tutti i dati disponibili sui sistemi vengono copiati su supporti di memorizzazione.

Tutti i sistemi aziendali critici della società sono soggetti a backup COMPLETO, cioè tutti i dati e le applicazioni o i file di database disponibili sul sistema vengono sottoposti a backup. Questa procedura mira ad ottenere sui supporti di memorizzazione primari e, ove possibile sul clone, l'insieme completo dei dati del sistema di configurazione, nonché tutti i dati relativi alle applicazioni.

Annex 3 - Gestione delle patch

Le patch di sicurezza sono di solito limitate modifiche software/ firmware promosse dai fornitori per correggere le vulnerabilità di sicurezza rilevate nei loro prodotti.

A causa della crescente diffusione di malware e attacchi di sicurezza, la frequenza di rilascio delle patch può essere elevata e coinvolge sia prodotti nuovi che vecchi.

Interprogetti stabilisce che ogni inizio mese il Responsabile Informatico (RI) (compatibilmente con i propri impegni) è incaricato di controllare eventuali aggiornamenti del software interessato / firmware al fine di ridurre la finestra di possibile debolezza del sistema informativo.

Le patch di sicurezza sono importanti per garantire elevati livelli di:

- sicurezza dei dati informativi;
- Manutenibilità/obsolescenza controllata;
- Controllo di configurazione/omogeneità.

Sistemi soggetti a patch

I seguenti sistemi sono soggetti a patch:

- Workstation, PC
- Server
- Dispositivi di rete

Annex 5 – Policy di Accesso Remoto

Lo scopo di questa Policy è definire le regole e i requisiti per la connessione alla rete di Interprogetti da qualsiasi host (telefoni cellulari, tablet, laptop). Queste regole e requisiti sono progettati per ridurre al minimo la potenziale esposizione da danni che possono derivare da un uso non autorizzato delle risorse aziendali. I danni comprendono la perdita di dati sensibili o riservati dell'organizzazione, la proprietà intellettuale, il danno all'immagine pubblica, il danno ai sistemi interni critici e le multe o altre passività finanziarie incorse come conseguenza di tali perdite.

L'accesso generale a Internet per uso ricreativo attraverso la nostra rete aziendale è strettamente limitato ai nostri dipendenti, appaltatori, fornitori e agenti (di seguito denominati "Utenti autorizzati"). Quando si accede alla nostra rete da un personal computer, gli Utenti autorizzati sono responsabili di impedire l'accesso a qualsiasi risorsa informatica aziendale o dati da Utenti non autorizzati.

L'esecuzione di attività illegali attraverso la nostra rete aziendale da parte di qualsiasi utente autorizzato o altrimenti) è vietata. L'Utente Autorizzato si assume la responsabilità e le conseguenze dell'uso improprio dell'accesso. Gli Utenti autorizzati non utilizzeranno le nostre reti per accedere a Internet per interessi commerciali esterni.

Procedura di accesso da remoto

L'accesso remoto sicuro sarà rigorosamente controllato con la crittografia attraverso le nostre reti private virtuali (VPN) e password secondo quanto sopra descritto.

Gli Utenti autorizzati devono proteggere il loro login e la password, anche dai membri della famiglia.

Mentre si utilizza il computer per connettersi in remoto alla rete aziendale, gli Utenti autorizzati devono garantire che l'host remoto non sia connesso a qualsiasi altra rete allo stesso tempo, ad eccezione delle reti personali che sono sotto il loro completo controllo o sotto il completo controllo di un Utente Autorizzato o di Terzi.

Tutti gli host che sono collegati alle reti interne dell'azienda tramite tecnologie di accesso remoto devono utilizzare il software anti-virus più aggiornato.

L'equipment personale utilizzato per connettersi alle reti dell'azienda devono soddisfare i requisiti delle apparecchiature di proprietà dell'azienda per l'accesso remoto, utilizzato solo in casi eccezionali previa approvazione dal responsabile della risorsa.

Annex 6 – Gestione degli Incidenti di Sicurezza

La gestione degli incidenti di sicurezza di Interprogetti è necessaria per rilevare gli incidenti di sicurezza, determinare l'entità della minaccia presentata da questi incidenti, rispondere a questi incidenti e, se necessario, informare i membri Interprogetti della violazione.

Questa Policy definisce i requisiti per la segnalazione e la risposta agli incidenti relativi ai sistemi informativi e alle operazioni di Interprogetti. La risposta agli incidenti fornisce a Interprogetti la capacità di identificare quando si verifica un incidente di sicurezza.

Questa Policy si applica a tutti i sistemi informativi e componenti del sistema informativo di Interprogetti. In particolare, comprende:

- Mainframe, server e altri dispositivi che forniscono funzionalità di elaborazione centralizzata.
- Dispositivi che forniscono funzionalità di archiviazione centralizzata.
- Desktop, laptop e altri dispositivi che forniscono funzionalità di elaborazione distribuita.
- Router, switch e altri dispositivi che forniscono funzionalità di rete.
- Firewall e altri dispositivi che offrono funzionalità di sicurezza dedicate

Nel caso in cui dati personali siano coinvolti in un incidente informatico, Interprogetti, in accordo con il GDPR, con l'ausilio del consulente esterno, si preoccuperà di contattare gli organismi preposti secondo la più attuale norma di legge.

Definizioni e terminologia

Cos'è un incidente informatico

Un incidente informatico si verifica quando avviene una violazione che minaccia la riservatezza, la disponibilità e l'integrità di un sistema di informazione o le informazioni che il sistema elabora, archivia o trasmette.

Esempi di incidenti informatici includono (ma non sono limitati a):

- Attacchi DoS (Denial of Service) che influiscono sulla disponibilità del sistema o del servizio
- Virus o malware (compresi i ransomware)
- Compromissione o divulgazione di informazioni sensibili o personali
- Compromissione delle credenziali di rete o di un account di posta elettronica.

Questo piano identifica quattro categorie di incidenti informatici che si differenziano per il livello di impatto che creano.

Incidenti informatici comuni e risposte

La seguente tabella fornisce un elenco di tipi comuni di incidenti informatici, insieme alle corrispondenti attività di risposta (che costituiscono la risposta minima tipica).

Tipo/descrizione	Iniziale risposta per ridurre al minimo possibili danni
Ransomware; uno strumento utilizzato per crittografare o bloccare i dati delle vittime fino a quando non viene pagato un riscatto.	Rimuovere immediatamente il dispositivo infetto dalla rete per limitare la diffusione del ransomware. Recuperare tutti i log disponibili relativi al dispositivo. Isolare i dispositivi mentre vengono determinate le attività di contenimento e di eradicazione.
Infezioni da malware; un virus, un worm, un cavallo di Troia o un'altra entità maligna basata sul codice che infetta con successo un host.	Rimuovere immediatamente il dispositivo infetto dalla rete per limitare la diffusione del malware. Recuperare tutti i log disponibili relativi al dispositivo. Isolare i dispositivi mentre vengono determinate le attività di contenimento e di eradicazione.
Attacchi Denial of Service (DoS) e Distributed Denial of Service (DDoS); travolge una rete ICT con traffico che non può elaborare, a volte causando il fallimento della rete.	Richiedere al fornitore di servizi gateway di identificare la natura DOS/ DDOS, vettore di attacco e implementare soluzioni adeguate. Mettersi in contatto con i servizi di gateway e team di rete per applicare filtri a bordo della rete e/o aumentare la capacità.
Phishing e Social Engineering; comunicazioni ingannevoli progettate per ottenere informazioni sensibili degli utenti (incluse le credenziali di rete).	Consultare gli utenti per confermare quali azioni hanno intrapreso e se sono state fornite informazioni personali/sensibili in risposta a un tentativo di phishing/ social engineering. Considerare la possibilità di ripristinare le password degli utenti e gli account di monitoraggio per qualsiasi accesso non autorizzato.
Violazione dei dati; accesso non autorizzato a informazioni sensibili o personali.	Contenere la perdita/fuoriuscita dei dati il prima possibile. Allertare i team di privacy, legali. Indagare sulla causa della perdita/fuoriuscita dei dati.

Vettori di attacco potenziali

Ci sono più vettori attraverso i quali può sorgere un incidente informatico. Mantenere la consapevolezza di questi vettori di minaccia supporterà Interprogetti nell'identificare potenziali punti deboli o aspetti comunemente mirati della rete e dei sistemi. Alcuni dei vettori più comuni includono:

Tipo	Descrizione
Media esterni/removibili	Un attacco eseguito utilizzando una USB contenete un malware
Attrito/usura	Un attacco DDoS contro una rete o un servizio critico
Web	Il reindirizzamento del traffico web a un URL dannoso che installa malware sul dispositivo della vittima.
Email	Attacchi di phishing che tentano di rubare informazioni e/o distribuire malware sul dispositivo della vittima.
Furto d'identità digitale	Un dominio che viene creato per imitare quello aziendale nel tentativo di ingannare le vittime (tipicamente associato ad attacchi di phishing).
Uso improprio delle tecnologie IT	Errore umano con conseguente violazione della Policy di sicurezza delle informazioni; o attacco da un insider malintenzionato con conseguente incidente di sicurezza informatica.

Ruoli e responsabilità

Sono stati definiti ruoli e responsabilità in relazione a possibili incidenti informatici:

l'utente contatta il Coadiuvatore Informatico (CI) ed il Consulente esterno IT per descrivere il possibile incidente informatico, il quale prenderà le dovute contromisure e in caso di incidente comunicherà l'accaduto al Management.

Processo di risposta all'incidente

Lista di controllo di riferimento rapido delle azioni di risposta agli incidenti:

Passi	Attività
1	Condurre un'analisi per determinare se si è verificato o si sta verificando un incidente.
2	Determinare la portata, l'impatto e la gravità dell'incidente; classificare l'incidente.
3	Coinvolgere il Responsabile Informatico (RI) per gestire gli sforzi di risposta; iniziare a documentare la situazione.
4	Sviluppare e attuare un piano d'azione per la risoluzione dei problemi che descriva dettagliatamente le attività di contenimento, eradicazione e recupero; raccogliere e registrare le prove.
5	Identificare gli stakeholder interessati: chi sarà colpito dall'incidente?
6	Sviluppare una strategia di notifica e comunicare i messaggi chiave alle parti interessate.
7	Confermare che la minaccia è stata debellata e riportare i sistemi/servizi interessati al normale funzionamento (testare i sistemi/servizi per confermare la funzionalità prevista).
8	Determinare le esigenze di comunicazione con le parti interessate.
9	Effettuare una revisione post incidente per identificare gli aspetti che hanno funzionato bene e le opportunità di miglioramento; documentare le conoscenze e le intuizioni acquisite.
10	Aggiornare il piano di risposta agli incidenti per includere i risultati e le intuizioni più importanti.