CORSO DI FORMAZIONE PER IL PERSONALE

Misure di contenimento dei rischi cyber e privacy

Comportamenti e regole operative per proteggere i dati e i sistemi dell’Amministrazione



Prefettura di Reggio Calabria · Sessione di 4 ore · 21 dicembre 2026

OBIETTIVI DEL CORSO

Al termine della sessione ciascun partecipante sarà in grado di...

01

Riconoscere le principali minacce e i comportamenti che le favoriscono

02

Proteggere le credenziali Microsoft 365 e usare l'MFA in modo consapevole

03

Gestire documenti digitali e cartacei secondo la necessità di conoscere

04

Lavorare in sicurezza in modalità agile tramite l'accesso Akamai

05

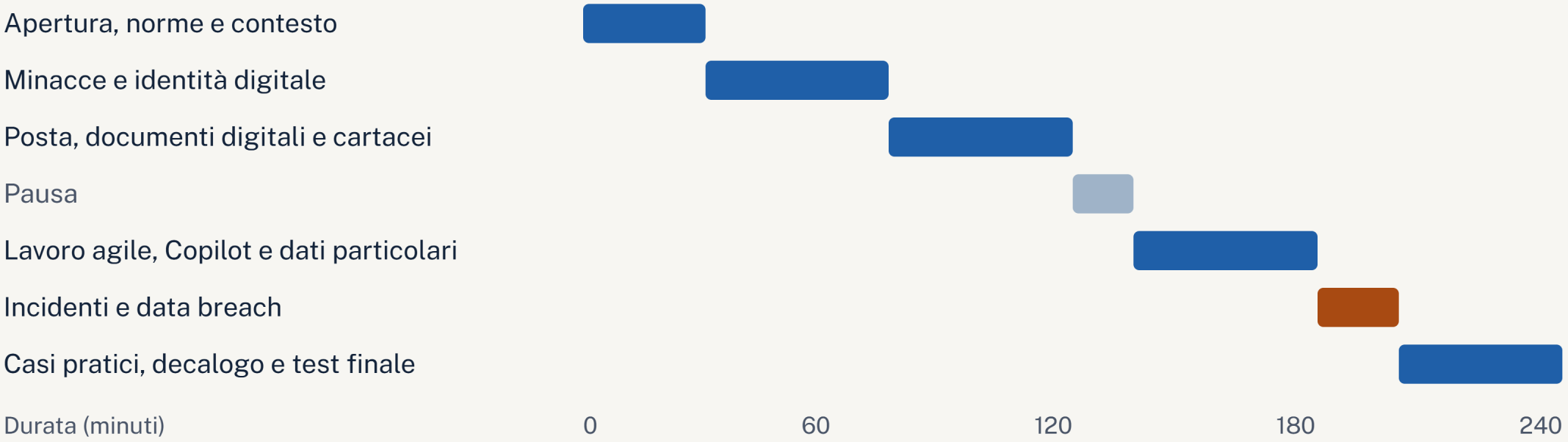
Usare Microsoft 365 Copilot nel rispetto delle regole dell'Amministrazione

06

Riconoscere un incidente o una violazione di dati e segnalarlo subito

PROGRAMMA

Quattro ore in sei tappe, con una pausa



PERCHÉ QUESTO CORSO

Sei violazioni su dieci passano da una persona

60%

delle violazioni di dati confermate coinvolge un’azione o un errore umano: un clic, un’approvazione, un invio sbagliato.

Come si manifesta l’elemento umano



Fonte: Verizon, Data Breach Investigations Report 2025. Quote sul totale delle violazioni analizzate; le categorie possono sovrapporsi.

LO SCENARIO IN ITALIA

La Pubblica Amministrazione è il settore più colpito

Eventi e incidenti gestiti da ACN nel 2025

Eventi cyber

2.729

Incidenti con impatto confermato

615

Gran parte degli attacchi viene intercettata prima che produca danni.

Incidenti gravi noti in Italia

2024

357

2025

507

Aumento del 42% in un anno; l'Italia concentra il 9,6% dei casi rilevati nel mondo.

Dopo la PA, i settori più colpiti sono le telecomunicazioni e il settore tecnologico.

Fonti: ACN, Relazione annuale al Parlamento 2025 (presentata a maggio 2026); Clusit, Rapporto 2026.

I FONDAMENTI

Tre proprietà da proteggere in ogni informazione

R

Riservatezza

Solo chi è autorizzato può conoscere il dato.

Violazione tipica: PEC con dati sanitari inviata al destinatario sbagliato.

I

Integrità

Il dato è esatto, completo e non alterato.

Violazione tipica: IBAN di un fornitore modificato da un truffatore.

D

Disponibilità

Il dato è accessibile quando serve a chi ne ha diritto.

Violazione tipica: ransomware che cifra le cartelle condivise.

QUADRO NORMATIVO

Le regole che ci riguardano

PRIVACY

GDPR

Sicurezza del trattamento; notifica delle violazioni entro 72 ore

PRIVACY

Codice privacy

Dati particolari e persone autorizzate al trattamento

CYBER

D.Lgs. 138/2024

NIS2: rischio e notifica al CERT del Ministero dell'Interno, che notifica al CSIRT Italia

CYBER

Legge 90/2024

Segnalazione degli incidenti all'ACN e referente per la cybersicurezza

CONDOTTA

Codice di comportamento

D.P.R. 81/2023: uso di strumenti, posta e social

CYBER

CAD e Cloud PA

Documento informatico e PEC; PSN per dati critici e strategici

IA

AI Act

Alfabetizzazione sull'IA per chi utilizza sistemi di IA (art. 4)

IA

L. 132/2025 e AgID

IA a supporto; la responsabilità resta del funzionario

CHE COSA PROTEGGIAMO

Dato personale è ogni informazione che identifica una persona, anche indirettamente

DATI COMUNI

Identificano la persona

- Nome, codice fiscale, indirizzo
- E-mail, telefono, IBAN
- Credenziali e indirizzi IP
- Immagini e registrazioni

DATI PARTICOLARI · ART. 9

Richiedono tutela rafforzata

- Salute e invalidità
- Appartenenza sindacale
- Convinzioni religiose e politiche
- Dati genetici e biometrici

DATI GIUDIZIARI · ART. 10

Trattati solo se previsto

- Condanne penali
- Reati e misure di sicurezza
- Carichi pendenti
- Casellario giudiziale

I PRINCIPI DEL TRATTAMENTO · ART. 5 GDPR

Sette principi guidano ogni trattamento

1
Liceità e trasparenza
Solo con una base giuridica, in modo corretto e chiaro

2
Limitazione della finalità
Per gli scopi istituzionali dichiarati, non per altri

3
Minimizzazione
Solo i dati necessari: né più né diversi

4
Esattezza
Dati corretti e aggiornati

5
Limitazione della conservazione
Per il tempo necessario, poi scarto o anonimizzazione

6
Integrità e riservatezza
Misure di sicurezza adeguate al rischio

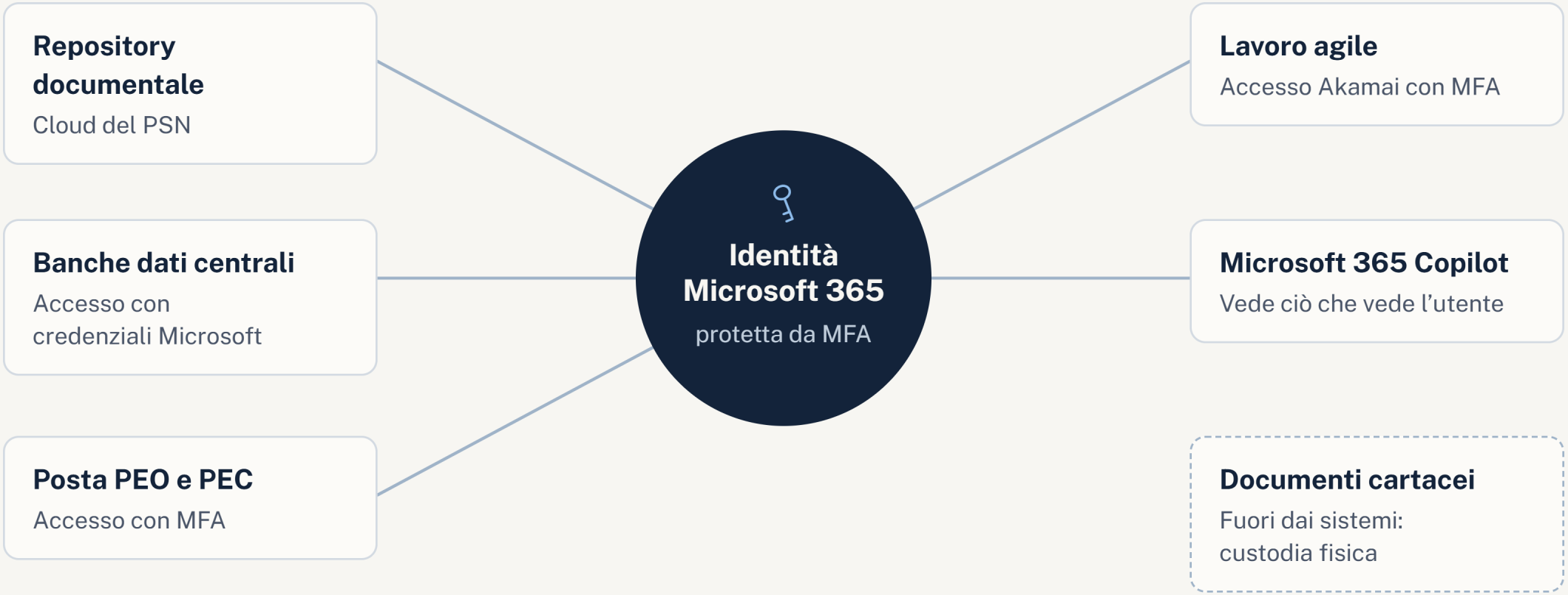
7
Responsabilizzazione
Saper dimostrare di aver rispettato le regole

PER IL DIPENDENTE

Solo i dati necessari, per lo scopo assegnato, per il tempo necessario

IL NOSTRO CONTESTO

Un’unica identità apre tutti i servizi



RESPONSABILITÀ CONDIVISA

La tecnologia protegge l’infrastruttura, non le scelte delle persone

PSN e Microsoft	Infrastruttura qualificata, cifratura, continuità e disponibilità dei servizi
Amministrazione	Configurazione di accessi e permessi, MFA, filtri della posta, regole e procedure interne
Ciascun dipendente	Custodia delle credenziali, condivisioni corrette, verifica dei messaggi, uso conforme di Copilot, segnalazione tempestiva

Un cloud qualificato non impedisce che un documento sia condiviso con la persona sbagliata: nessun livello può compensare l’errore degli altri.

CHI FA CHE COSA

Ruoli e riferimenti nella Prefettura



PARTE 2 DI 6 · 45 MINUTI

Le minacce e l’identità digitale

02

Modulo 1 · Le principali minacce e l’ingegneria sociale

Modulo 2 · Credenziali Microsoft 365 e autenticazione multifattore

MODULO 1 · LE MINACCE

L’attaccante non forza i sistemi: cerca una persona che clicchi

Phishing
E-mail o PEC che imitano Microsoft, l’ente o un fornitore

Login contraffatti
Pagine identiche che rubano password e codice MFA

Bombardamento MFA
Notifiche ripetute finché l’utente non approva

App malevole
Richieste di consenso per leggere posta e file

Telefonate e SMS
Falsi tecnici che chiedono codici o accesso remoto

Falso dirigente
Richieste urgenti di dati, pagamenti o cambi di IBAN

Ransomware
Allegati e macro che cifrano i dati e chiedono un riscatto

Errore umano
Invii sbagliati, condivisioni eccessive, accessi per curiosità

MODULO 1 · INGEGNERIA SOCIALE

Gli attaccanti fanno leva sulle emozioni, non sulla tecnica

Urgenza

«Entro 24 ore, o la casella sarà sospesa»

Autorità

«Lo chiede il Prefetto, è riservato»

Paura

«Rilevato accesso sospetto al suo account»

Curiosità

«In allegato la graduatoria riservata»

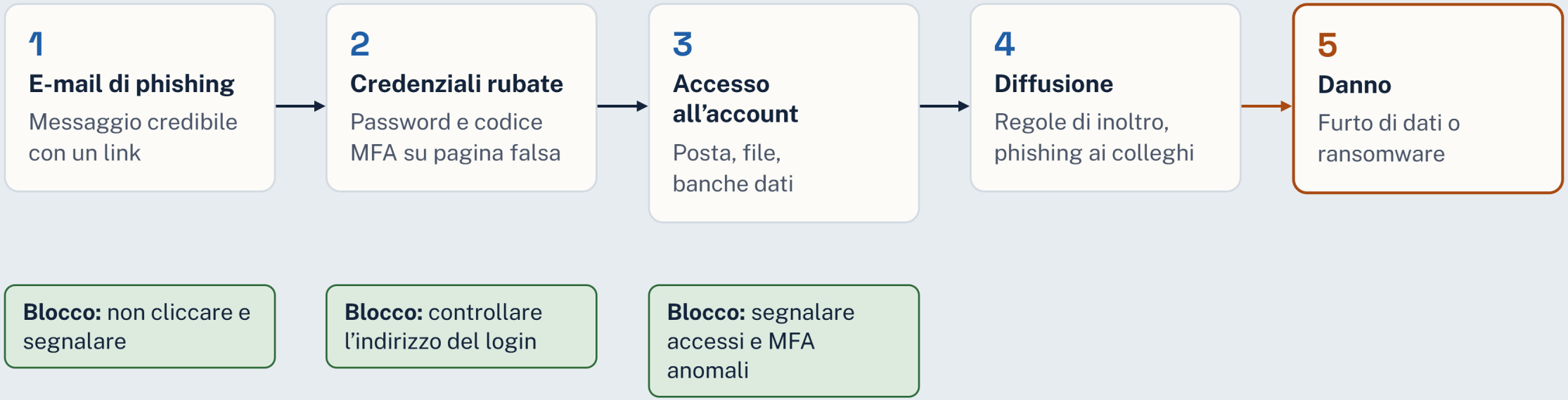
Fiducia

«Sono del servizio IT, mi serve il codice»

Un’emozione forte davanti a un messaggio è il segnale per fermarsi e verificare per altra via.

MODULO 1 · ANATOMIA DI UN ATTACCO

Dal clic al danno: la catena si interrompe all'inizio



I primi tre passaggi dipendono da un comportamento umano: è lì che ogni dipendente può fermare l'attacco.

LA REGOLA DEI TRE CONTROLLI

Prima di cliccare, aprire, approvare o inviare

1

Me lo aspettavo?

Un messaggio inatteso merita sospetto, anche da un indirizzo noto.

2

Mi mette fretta?

Urgenza e richieste di eccezioni sono le leve dell'ingegneria sociale.

3

Posso verificarlo?

Una telefonata al numero ufficiale risolve quasi ogni dubbio.

Nel dubbio: fermarsi e segnalare.

MODULO 2 · IDENTITÀ DIGITALE

Le credenziali Microsoft 365 sono personali e non cedibili

Password

- Frase lunga, almeno 14–16 caratteri
- Mai riutilizzata per servizi personali
- Mai annotata né comunicata
- Cambiata subito se esposta

Secondo fattore (MFA)

- Approvare solo accessi avviati da sé
- Verificare il numero chiesto dall'app
- Mai comunicare codici monouso
- Telefono con PIN; smarrimento segnalato

Sessione di lavoro

- Schermo bloccato: Windows + L
- Nessuna password salvata su PC condivisi
- Disconnessione a fine lavoro
- Mai le credenziali di un collega

MODULO 2 · AUTENTICAZIONE MULTIFATTORE

Due prove indipendenti per ogni accesso

Qualcosa che sapete

La password

+

Qualcosa che avete

Lo smartphone con Authenticator

=

Accesso consentito

LA CORRISPONDENZA DEI NUMERI

1. Inserite la password sul computer
2. Lo schermo mostra un numero di due cifre
3. Lo digitate nell’app solo se l’accesso è vostro

Attenzione: una pagina di login contraffatta può farsi consegnare anche il codice. Controllate sempre l’indirizzo prima di autenticarvi.

SEGNALE D’ALLARME

Una notifica MFA che non avete richiesto significa che la password è già compromessa.



1 · Rifiutate

2 · Cambiate la password

3 · Segnalate subito

MODULO 2 · ACCOUNT COMPROMESSO

Sei segnali che qualcuno sta usando il vostro account

- Messaggi inviati che non riconoscete
- Regole di inoltro o risposte automatiche mai create
- Notifiche MFA che non avete richiesto
- Avvisi di accesso da luoghi o dispositivi insoliti
- Colleghi che ricevono da voi e-mail strane
- Password improvvisamente non più valida

COSA FARE SUBITO

1. Cambiare la password
2. Chiamare l'help desk: [numero]
3. Non cancellare messaggi né regole
4. Seguire le istruzioni ricevute

PARTE 3 DI 6 · 45 MINUTI

Posta, documenti digitali e cartacei

03

Modulo 3 · Posta elettronica ordinaria e PEC

Modulo 4 · Documenti su cloud PSN, etichette e banche dati

Modulo 5 · Documenti cartacei e sicurezza fisica

MODULO 3 · POSTA ELETTRONICA ORDINARIA E PEC

Un allegato al destinatario sbagliato è già una violazione di dati

In ricezione

- Leggere l'indirizzo reale, non solo il nome visualizzato
- Passare il cursore sui link prima di cliccare
- Niente allegati inattesi, compressi o con macro
- Segnalare con il pulsante «Segnala phishing» di Outlook

In invio

- Ricontrollare i destinatari proposti in automatico
- Nessun dato particolare nell'oggetto
- Condividere dal repository o applicare l'etichetta «Riservato»
- Mai inoltrare alla posta personale

La PEC certifica invio e consegna, non la buona fede del mittente: anche una PEC può contenere phishing.

ESEMPIO ANNOTATO · MESSAGGIO FITTIZIO

Cinque segnali in un solo messaggio

Da: Supporto Microsoft 365 1
noreply@m365-sicurezza-account.example

Oggetto: URGENTE – la sua casella sarà sospesa entro 24 ore 2

Gentile utente, 3

abbiamo rilevato un accesso insolito al suo account. Per evitare la sospensione, verifichi subito password e codice di autenticazione. 4

Verifica account 5

Destinazione reale del link: https://login-microsoftonline.verifica-account.example

1 **Mittente non istituzionale**
Il nome dice Microsoft, il dominio no

2 **Urgenza e minaccia**
La fretta serve a impedire la verifica

3 **Saluto generico**
Nessun nome, nessun ufficio

4 **Richiesta del codice**
Nessuno chiede password o codici via e-mail

5 **Link ingannevole**
Il testo del pulsante non è la destinazione

ESEMPIO ANNOTATO · PEC FITTIZIA

Una PEC autentica può contenere una truffa

Da: Fornitore Beta – Ufficio Amministrazione (1)
POSTA CERTIFICATA: amministrazione@pec.fornitore-beta.example

Oggetto: Variazione coordinate bancarie – fattura n. 418/2026 (2)

Spettabile Amministrazione,

si comunica che i pagamenti dovranno essere effettuati sul nuovo conto indicato in allegato. La fattura in scadenza va saldata entro oggi. (3)

Si prega di non contattare i nostri uffici, attualmente in riorganizzazione. (4)

Allegato: Nuove_coordinate.pdf.zip (5)

1. **PEC vera, casella violata**
   La certificazione non garantisce il contenuto
2. **Cambio di IBAN**
   Si verifica sempre al telefono già in anagrafica
3. **Scadenza immediata**
   Spinge a saltare i controlli
4. **Invito a non verificare**
   Chi lo scoraggia vuole evitare la verifica
5. **Doppia estensione**
   Un .pdf.zip non è un PDF: non aprirlo

MODULO 3 · INVIO AL DESTINATARIO SBAGLIATO

Se il messaggio parte per errore: quattro mosse, subito

1

Richiamare

Usare il richiamo di Outlook se il destinatario è interno e non ha letto

2

Contattare

Chiedere al destinatario di cancellare il messaggio e di confermarlo

3

Segnalare

Help desk [numero] e, per dati personali, il RPD

4

Non attendere

Non aspettare di sapere se il messaggio è stato letto

PER PREVENIRE

- Rileggere i destinatari proposti in automatico
- Condividere un link nominativo invece dell'allegato
- Applicare l'etichetta «Riservato» ai dati personali

MODULO 4 · DOCUMENTI DIGITALI E BANCHE DATI

Chi vede un documento dipende da chi lo condivide

Condivisione corretta

- Etichetta di riservatezza Microsoft su ogni documento
- Con persone specifiche, per nome
- In sola lettura quando basta
- Con scadenza per i soggetti esterni
- Cartelle ad accesso ristretto per i dati personali
- Revisione periodica delle condivisioni attive

Da evitare

- Link «chiunque abbia il collegamento»
- Accesso aperto a tutta l'organizzazione
- Copie su disco locale, USB o cloud personali
- Estrazioni massive non previste
- Consultazioni per curiosità

Le banche dati registrano ogni accesso: ogni consultazione deve corrispondere a un procedimento assegnato.

MODULO 4 · ETICHETTE DI RISERVATEZZA MICROSOFT

Più alto il livello, più forte la protezione che segue il file

Pubblico

Nessuna restrizione: atti pubblicabili

Uso interno

Solo personale dell'Amministrazione

Riservato

Cifratura, accesso limitato, intestazione o filigrana

Riservato – dati particolari

Solo persone autorizzate; inoltro, copia e stampa bloccati

Si applica quando si crea il documento o il messaggio

Segue il file ovunque venga copiato o inviato

Non si declassa senza un motivo, che resta registrato

MODULO 5 · DOCUMENTI CARTACEI E SICUREZZA FISICA

Il fascicolo sulla scrivania vale quanto il file esposto

Scrivania pulita

Fascicoli in armadi chiusi a chiave a fine giornata e in ogni assenza

Stampa e copia

Solo se serve; ritiro immediato; nessun originale nello scanner

Distruzione sicura

Distruggidocumenti o contenitori certificati, mai il cestino

Locali e sportelli

Badge personale, nessun ingresso «a ruota», documenti non visibili al pubblico



Il GDPR tutela allo stesso modo i documenti cartacei organizzati in fascicoli e i file digitali: un fascicolo smarrito può essere una violazione di dati personali.

PARTE 4 DI 6 · 45 MINUTI

Lavoro agile, Copilot e dati particolari

04

Modulo 6 · Lavoro agile tramite Akamai

Modulo 7 · Uso responsabile di Microsoft 365 Copilot

Modulo 8 · Trattamento dei dati particolari

MODULO 6 · LAVORO AGILE TRAMITE AKAMAI

La postazione e l’ambiente restano a voi

Dispositivo dell’Amministrazione

- Lo strumento da preferire
- Impostazioni di sicurezza, antivirus e aggiornamenti invariati
- Uso esclusivo per il lavoro

Dispositivo personale · solo se autorizzato

- Sistema, browser e antivirus aggiornati
- Account utente dedicato al lavoro
- Nessun documento scaricato, salvato o stampato
- Nessuna password salvata nel browser

REGOLE COMUNI

Rete di casa protetta, mai Wi-Fi pubblico

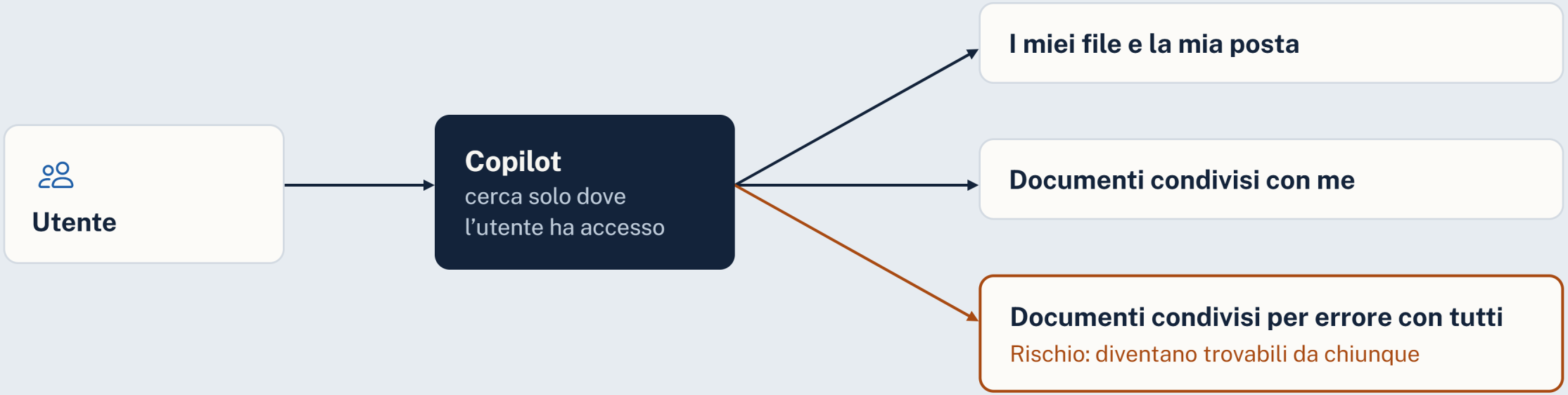
Portale dai preferiti, mai da un link ricevuto

Schermo e telefonate al riparo da terzi

Schermo bloccato e sessione chiusa a fine lavoro

MODULO 7 · MICROSOFT 365 COPILOT

Copilot vede ciò che vedete voi



Prompt e risposte non sono usati per addestrare i modelli di base

Le interazioni sono conservate e consultabili dagli amministratori

La ricerca web invia una query a Bing, fuori dal perimetro di Microsoft 365

Rispetta le etichette di riservatezza; i testi generati ereditano la più restrittiva

Fonte: Microsoft Learn, «Data, Privacy, and Security for Microsoft 365 Copilot».

MODULO 7 · REGOLE D’USO

L’IA è un supporto: la responsabilità resta di chi firma

Consentito

- Bozze di comunicazioni e documenti, da rileggere
- Riassunti di documenti e riunioni accessibili
- Schemi, riorganizzazione di testi, traduzioni
- Ricerca nei propri file e nella propria posta

Non consentito

- Servizi di IA non autorizzati per dati di lavoro
- Dati particolari non indispensabili nei prompt
- Decisioni o valutazioni su persone
- Ricerca web con dati personali o riservati
- Testi inviati senza verifica

Verificate fatti, numeri e norme sulle fonti originali, e diffidate di risposte che chiedono di cliccare link o fornire credenziali.

MODULO 7 · SCRIVERE UN PROMPT CORRETTO

Chiedere una bozza con i dati minimi, non una decisione

⚠ Da evitare

«Riassumi la pratica di [Nome Cognome], nato il [data], diabetico, e scrivi il diniego dell'istanza.»

- Dati identificativi e sanitari superflui
- Decisione affidata all'IA

✓ Corretto

«Prepara una bozza di risposta all'istanza, usando "il richiedente" al posto del nome e le motivazioni del documento allegato.»

- Pseudonimizzazione e dati minimi
- Bozza da verificare e firmare

MODULO 8 · DATI PARTICOLARI

Più il dato è delicato, più le cautele sono stringenti

Quali sono (art. 9 GDPR)

- **Salute**
- Origine etnica
- Opinioni politiche
- Convinzioni religiose
- Appartenenza sindacale
- Dati genetici
- Dati biometrici
- Vita e orientamento sessuale

Tutela analoga per i dati su condanne penali e reati (art. 10). In evidenza la salute, la categoria più frequente nei fascicoli del personale.

Misure rafforzate

- Accesso solo al personale autorizzato per il procedimento
- Etichetta «Riservato – dati particolari» e accesso nominativo
- Nelle comunicazioni «assenza giustificata», non la diagnosi
- Nessuna pubblicazione di dati sulla salute

Attenzione ai dati indiretti

L'articolo di legge di un permesso o il nome di una struttura sanitaria possono rivelare lo stato di salute.

PARTE 5 DI 6 · 20 MINUTI

Incidenti e violazioni di dati

05

Modulo 9 · Riconoscere, contenere e segnalare

MODULO 9 · CHE COS’È UNA VIOLAZIONE

Tre modi di violare la sicurezza dei dati

R

Riservatezza

Divulgazione o accesso non autorizzato

- E-mail al destinatario sbagliato
- Link aperto a tutti
- Fascicolo letto da estranei

I

Integrità

Modifica non autorizzata o accidentale

- Dati alterati in una banca dati
- IBAN di un fornitore cambiato
- Documento modificato senza traccia

D

Disponibilità

Perdita o distruzione

- Ransomware sulle cartelle condivise
- Fascicolo smarrito senza copia
- Cancellazione accidentale

Anche un errore in buona fede è una violazione: va segnalato, non nascosto.

MODULO 9 · INCIDENTI E VIOLAZIONI DI DATI

I termini sono brevi: la segnalazione interna deve essere immediata

A carico del dipendente

A carico delle strutture dell'Amministrazione (titolare, RPD, referente per la cybersicurezza)



Subito
Segnalazione interna di qualsiasi evento sospetto

24 ore
Preallarme al CERT del Ministero dell'Interno, che notifica al CSIRT Italia

72 ore
Notifica al CERT del Ministero dell'Interno e, per i dati personali, al Garante

1 mese
Relazione finale al CERT del Ministero dell'Interno

I termini decorrono da quando l'Amministrazione viene a conoscenza dell'evento: ogni ora di ritardo nella segnalazione interna li consuma.

Riferimenti: D.Lgs. 138/2024 (NIS2) per gli incidenti significativi, notificati al CERT del Ministero dell'Interno che li trasmette al CSIRT Italia; art. 33 GDPR per le violazioni di dati personali. Asse temporale non in scala.

MODULO 9 · CHE COSA FARE

Cinque passi, in quest’ordine

1

Non cancellare

Messaggi, file e tracce servono all’analisi

2

Contenere

Scollegare dalla rete, rifiutare l’MFA, revocare la condivisione

3

Segnalare subito

Help desk [numero] o referente cyber; per i dati personali anche il RPD

4

Cambiare la password

Se le credenziali possono essere state esposte

5

Collaborare

Fornire le informazioni richieste, con riservatezza

CHE COSA SEGNALARE, ANCHE SOLO SE SOSPETTO

- Clic su un link sospetto
- Notifiche MFA non richieste
- Invio al destinatario sbagliato
- Condivisione errata
- Smarrimento di PC, telefono o fascicoli
- Postazione con comportamenti anomali
- Copilot che mostra dati altrui
- Estranei in locali riservati

PARTE 6 DI 6 · 40 MINUTI

Casi pratici, decalogo e test finale

06

Sette casi da discutere

Il decalogo operativo

Il test di verifica dell’apprendimento

CASI PRATICI

Sette situazioni reali da discutere insieme

CASO 1

La casella in scadenza

Una PEC di un'altra PA chiede di confermare le credenziali

CASO 2

Le notifiche notturne

Alla quarta richiesta MFA, una collega approva

CASO 3

Il completamento automatico

Un elenco di permessi per assistenza va a un omonimo esterno

CASO 4

Copilot troppo informato

Il riepilogo include valutazioni di un altro ufficio

CASO 5

Il bar della stazione

Una pratica sanitaria aperta sul Wi-Fi pubblico

CASO 6

Il fascicolo dimenticato

Certificati medici lasciati sul bancone dello sportello

CASO 7

Il dirigente al telefono

Una voce credibile chiede un'estrazione sulla casella personale

METODO

5 minuti per caso: segnali, comportamento corretto, prevenzione

CASO 1 DI 7 · SOLUZIONE

La casella in scadenza

Una PEC di un’altra amministrazione avvisa che la casella Microsoft 365 sarà disattivata entro 24 ore e chiede di confermare le credenziali da un link. La pagina è identica a quella abituale.

SEGNALI

- Urgenza e minaccia di sospensione
- Credenziali richieste tramite link
- Mittente estraneo ai servizi informatici

COMPORTAMENTO CORRETTO

- Non cliccare e segnalare il messaggio
- Indicare che la casella dell’altra PA è forse violata
- Se già cliccato: cambiare password e chiamare l’help desk

PREVENZIONE

- Accedere sempre dai preferiti
- Controllare l’indirizzo della pagina di login

CASO 2 DI 7 · SOLUZIONE

Le notifiche notturne

Alle 23:00, senza stare lavorando, una dipendente riceve tre richieste di approvazione su Authenticator. Alla quarta approva per far cessare le notifiche.

SEGNALI

- Richieste MFA non avviate da lei
- La password è già nota all'attaccante

COMPORTAMENTO CORRETTO

- Rifiutare sempre
- Avendo approvato: segnalare subito, anche fuori orario, al cellulare del referente
- Cambiare la password

PREVENZIONE

- Password unica e lunga
- Mai approvare «per far smettere»

CASO 3 DI 7 · SOLUZIONE

Il completamento automatico

Un funzionario invia l’elenco dei beneficiari di permessi per assistenza a familiari disabili. Outlook sostituisce il collega con un omonimo di un ente esterno.

SEGNALI

- Dato sulla salute in allegato
- Destinatario non ricontrollato

COMPORTAMENTO CORRETTO

- Segnalare subito all’help desk e al RPD
- Chiedere al destinatario di cancellare il messaggio
- Non attendere di sapere se è stato letto

PREVENZIONE

- Link nominativo dal repository
- Etichetta «Riservato – dati particolari»
- Ricontrollo dei destinatari

CASO 4 DI 7 · SOLUZIONE

Copilot troppo informato

Chiedendo a Copilot di riassumere le pratiche dell'ufficio, un dipendente ottiene anche valutazioni del personale di un altro ufficio.

SEGNALI

- Copilot rispetta i permessi: il documento è condiviso troppo
- Etichetta assente o inadeguata

COMPORTAMENTO CORRETTO

- Non usare né diffondere l'informazione
- Segnalare al responsabile e all'help desk

PREVENZIONE

- Condivisioni nominative
- Etichette corrette
- Revisione periodica dei permessi

CASO 5 DI 7 · SOLUZIONE

Il bar della stazione

In attesa del treno, un dipendente si collega ad Akamai dal Wi-Fi gratuito del bar e rivede una pratica con dati sanitari, con altre persone al tavolo accanto.

SEGNALI

- Rete pubblica
- Schermo visibile a terzi
- Dati particolari a vista

COMPORTAMENTO CORRETTO

- Rinviare l'attività
- Se indispensabile: hotspot del telefono e luogo riservato

PREVENZIONE

- Lavorare sui dati particolari solo in ambienti riservati
- Filtro privacy per lo schermo

CASO 6 DI 7 · SOLUZIONE

Il fascicolo dimenticato

Dopo un ricevimento al pubblico, un fascicolo con certificati medici resta sul bancone dello sportello durante la pausa pranzo.

SEGNALI

- Dati sulla salute incustoditi
- Area accessibile al pubblico

COMPORTAMENTO CORRETTO

- Riporre subito il fascicolo in armadio chiuso
- Se mancante o consultato da terzi: segnalare come possibile violazione

PREVENZIONE

- Scrivania pulita a ogni allontanamento
- Sportello senza documenti a vista

CASO 7 DI 7 · SOLUZIONE

Il dirigente al telefono

Una voce credibile, che si presenta come un dirigente, chiede con urgenza di inviare alla sua casella personale un’estrazione della banca dati per una riunione riservata.

SEGNALI

- Urgenza e riservatezza imposta
- Canale insolito, destinazione esterna
- Possibile voce sintetica

COMPORTAMENTO CORRETTO

- Non procedere
- Richiamare il numero ufficiale della segreteria
- Segnalare il tentativo

PREVENZIONE

- Nessuna estrazione verso caselle personali
- Verifica sempre su un canale indipendente

DECALOGO OPERATIVO

Dieci regole da portare con sé

01 **Le credenziali sono soltanto mie.** Mai comunicate, mai prese in prestito.

02 **Approvo solo ciò che ho richiesto.** L'MFA inattesa si rifiuta e si segnala.

03 **Mi fermo prima di cliccare.** Me lo aspettavo? Mi mette fretta? Posso verificarlo?

04 **Accedo dall'indirizzo ufficiale.** Dai preferiti, mai da un link ricevuto.

05 **Consulto solo ciò che mi serve.** Ogni accesso è tracciato.

06 **Condivido con persone, non con link aperti.** E revoco ciò che non serve.

07 **Controllo i destinatari.** Niente dati particolari nell'oggetto, niente posta personale.

08 **Scrivania pulita, schermo bloccato.** Carta distrutta in modo sicuro.

09 **L'IA mi supporta, non decide.** Strumenti autorizzati, dati minimi, verifica.

10 **Segnalo subito, anche il dubbio e anche il mio errore.**

IN SINTESI

Segnalare subito, anche il dubbio e anche il proprio errore.

CONTATTI

Help desk informatico
[numero]

Referente cybersicurezza
[Nome Cognome] ·
cell. [numero]

RPD / DPO
[Nome Cognome]

Fuori orario
Cellulare del referente

Ora il test finale: 12 domande a risposta multipla, superamento con 9 risposte corrette.