| Piano di Sicurezza | |
|---|---|
| Denominazione dell'Ente | Ente di Governo dell'Ambito della Sardegna |
| Indirizzo completo della sede principale dell'Ente a cui indirizzare la corrispondenza convenzionale | EGAS<br>Via Cesare Battisti, 14<br>09123 Cagliari |
| PEC | protocollo@pec.egas.sardegna.it |

La seguente tabella descrive le misure di sicurezza adottate dall'Ente di Governo dell'Ambito della Sardegna in attuazione delle disposizioni delle Linee Guida AgID e di quanto previsto dalla circolare AgID n. 2 del 18 aprile 2017, e in stretta correlazione con quanto previsto dal Piano di Protezione Dati adottato dall'EGAS, da aggiornare annualmente.

Per "misura" si intende l'intervento tecnico e/o organizzativo specifico posto in essere per prevenire, contrastare i ridurre gli effetti relativi ad una specifica minaccia. La colonna "modalità di implementazione" fornisce l'indicazione dello stato di attuazione e degli strumenti tecnici effettivamente utilizzati per realizzare la misura riferita alla riga.

| Descrizione misura | | Modalità di implementazione |
|---|---|---|
| 1. Inventario dei dispositivi autorizzati e non autorizzati | | |
| Gestione dei dispositivi hardware sulla rete mediante il tracciamento, l'inventariazione e l'aggiornamento tempestivo dell'inventario al fine di garantire l'accesso solo ai dispositivi autorizzati, con l'inibizione e il blocco di accesso ai dispositivi non autorizzati. | Implementazione dell'inventario delle risorse attive. | Aggiornamento annuale. Ultimo prot. 459 del 27/01/2022. |
| | Aggiornamento dell'inventario prima di collegamento dei nuovi dispositivi approvati in rete. | Implementato |
| | Gestione dell'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi stessi, mediante la registrazione almeno degli indirizzi IP | Assegnazione automatizzata tramite DHCP |
| 2. Inventario dei software autorizzati e non autorizzati | | |
| Gestione attiva mediante inventariazione, tracciamento e correzione di tutti i software sulla rete al fine di precludere l'installazione dei software non autorizzati e non gestiti. | Predisposizione di un elenco di software autorizzati e relative versioni necessarie per ogni dispositivo e di sistema, compreso il server, workstation e laptop di vari tipi in uso presso l'Ente. | I software licenziati sono installati unicamente da parte dell'Amministratore di sistema (1 utenza amministrativa). L'elenco dei software autorizzati è in fase di aggiornamento. |
| | Impedimento di installazione di software non compresi nell'elenco di software autorizzati. | Impossibilità di installare software per utenze non amministrative. |
| | Esecuzione di regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzati. | Impossibilità di installare software per utenze non amministrative. |
| 3. Protezione e configurazione di hardware e software sui dispositivi mobili, laptop, workstation e server. | | |
| Istituzione, implementazione e gestione attiva, mediante tracciamento, segnalazione e correzione, delle configurazioni di sicurezza dei laptop, server e workstation e la configurazione di una procedura di controllo delle variazioni rigorose al fine di evitare gli attacchi informatici che possono sfruttare le vulnerabilità dei servizi. | Utilizzo delle configurazioni sicure standard per la protezione dei sistemi operativi. | Implementato |
| | Definizione e impiego delle configurazioni standard per workstation, server e altri tipi di sistemi usati dall'Ente. | Implementato |
| | Il ripristino dei sistemi compromessi mediante l'utilizzo delle configurazioni standard. | Implementato |
| | Memorizzazione delle immagini di installazione offline. | Sono disponibili immagini predefinite offline per ogni sistema operativo in uso. |
| | L'esecuzione delle operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette e canali sicuri. | https |

| | | |
|---|---|---|
| | Utilizzo di strumenti di verifica dell'integrità dei file al fine di assicurare che i file critici del sistema, compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni, non siano stati alterati. | Effettuato con strumenti nativi integrati di Windows: DISM e SFC |
| 4. Valutazione e correzione continua della vulnerabilità | | |
| Acquisizione, valutazione e messa in atto delle azioni in relazione a nuove informazioni allo scopo di individuare la vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici. | Esecuzione, all'atto delle modifiche significative di configurazione, della ricerca di vulnerabilità su tutti i sistemi in rete con strumenti informatici automatizzati che forniscono all'amministratore di sistema un report con l'indicazione delle vulnerabilità più critiche. | Nessus Essentials Vulnernability Scanner |
| | Utilizzo degli strumenti di scansione delle vulnerabilità aggiornati con tutte le più rilevanti vulnerabilità di sicurezza. | Aggiornamento periodico |
| | Installazione automatica delle patch e degli aggiornamenti dei software sia per il sistema operativo che per le applicazioni. | Implementato |
| | Aggiornamento dei sistemi separati dalla rete, in particolare di quelle air-gapped in funzione delle misure adeguate al loro livello di criticità. | Implementato |
| | Verifica della risoluzione delle criticità mediante patch o opportune contromisure. Applicazione delle patch per le vulnerabilità a partire da quelle più critiche. | Implementato |
| | Definizione del piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati. | In fase di definizione |
| 5. Uso appropriato dei privilegi di amministratore | | |
| Implementazione delle regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi. | Limitazione dei privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi. | Amministratore di Sistema (1 utenza) |
| | Utilizzo delle utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato. | Accesso inibito alle singole utenze per le operazioni che richiedono privilegi dell'Amministratore di sistema. |
| | Predisposizione e aggiornamento dell'elenco di tutte le utenze amministrative, con indicazione di adeguate autorizzazioni formali. | Amministratore di Sistema (1 unità). Aggiornamento annuale. |
| | La sostituzione delle credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso prima di collegamento dei nuovi dispositivi in rete | Implementato |
| | Utilizzo di credenziali di elevata robustezza per tutte le utenze amministrative. | Credenziali alfanumeriche almeno 8 caratteri |
| | Sostituzione delle credenziali delle utenze amministrative con sufficiente frequenza (password aging). | Termine max 90 gg |
| | Inibizione dell'utilizzo delle credenziali riutilizzate a breve distanza di tempo (password history). | Inibizione delle ultime 24 password utilizzate |
| | La distinzione tra utenze privilegiate e non privilegiate degli amministratori, mediante utilizzo delle credenziali diverse. | Implementato |
| | Creazione delle utenze amministrative nominative e riconducibili ad una sola persona. | Implementato |

| | | |
|---|---|---|
| | Utilizzo delle utenze amministrative anonime (Administrator di Windows) solo per le situazioni di emergenza con la gestione che ne consente l'imputabilità a chi ne fa uso. | Implementato |
| | Conservazione delle credenziali amministrative in modo da garantirne la disponibilità e la riservatezza. | Implementato |
| | Protezione delle chiavi private dei certificati digitali utilizzati per l'autenticazione. | Implementato |
| 6. Difesa contro malware | | |
| Controllo sull'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'ente, mediante utilizzo dell'automazione per il rapido aggiornamento delle difese, raccolta dati e azioni correttive. | Installazione su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e il blocco di esecuzione di malware (antivirus locale). Aggiornamento automatico dei sistemi di protezione. | Bit Defender Gravity Zone |
| | Istallazione su tutti i dispositivi dei firewall e IPS personali. | Bit Defender Gravity Zone Firewall integrato |
| | Limitazione dell'uso dei dispositivi esterni a quelli necessari per le attività dell'ente. | Implementato |
| | Disattivazione dell'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili. | Configurazioni standard di Windows di default |
| | Disattivazione dell'esecuzione automatica dei contenuti dinamici (macro) presenti nei file. | Configurazioni standard di Office 365 di default |
| | Disattivazione dell'apertura automatica dei messaggi di posta elettronica. | Configurazioni standard di Outlook 365 di default |
| | Disattivazione dell'anteprima automatica dei contenuti dei file. | Configurazioni standard di Outlook 365 di default |
| | Esecuzione automatica di scansione anti-malware dei supporti rimovibili al momento della loro connessione. | Bit Defender Gravity Zone |
| | Esecuzione del filtro dei contenuti dei messaggi di posta prima che raggiungano la casella dei destinatari (antispam). | Configurazioni standard di Outlook 365 di default |
| | Esecuzione del filtro dei contenuti del traffico web. | Bit Defender Gravity Zone + FortiGate 40 F |
| | Esecuzione del blocco dei file la cui tipologia non è strettamente necessaria e potenzialmente pericolosa nella posta elettronica e nel traffico web (.cab). | Implementato |
| 7. Copie di sicurezza | | |
| Implementazione delle procedure e utilizzo degli strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, al fine di consentirne il ripristino in caso di necessità. | Produzione almeno settimanale di una copia di sicurezza delle informazioni strettamente necessarie al completo ripristino del sistema. | Produzione settimanale |
| | Protezione fisica e mediante cifratura delle informazioni contenute nelle copie di sicurezza che ne assicura la riservatezza. | Implementato |
| | La codifica della trasmissione e remotizzazione del backup anche nel cloud dell'ente. | In fase di implementazione |
| | Protezione dei supporti contenenti le copie di sicurezza di modo che almeno una di esse non sia permanentemente accessibile dal sistema al fine di evitare che attacchi ai supporti possano coinvolgere tutte le copie contemporaneamente. | Implementato |
| 8. Protezione dei dati. | | |
| Adozione dei processi interni, utilizzo degli strumenti e dei sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti. | Analisi dei dati al fine di individuare quelli con particolari requisiti di riservatezza e segnatamente quelli ai quali va applicata la protezione crittografica. | Aggiornamento annuale unitamente al Piano di Protezione dei Dati dell'Ente. |
| | Blocco di traffico da e verso url presenti in una blacklist. | Bit Defender Gravity Zone + FortiGate 40 F |

**Misure da adottare in caso di violazione dei dati personali.**

Come previsto dal Piano di Protezione dei Dati e dalla Procedura per la gestione di data breach adottati dall'Ente, in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 del GDPR senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

La notifica deve almeno:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Per le notifiche all'Autorità di controllo si rinvia alla "procedura per la gestione di data breach ai sensi del GDPR (Regolamento europeo 679/2016) allegato al "Regolamento sulla protezione dei dati personali" approvato con deliberazione del CIA n. 15 del 15 aprile 2020.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

La comunicazione all'interessato descrive, con un linguaggio semplice e chiaro, la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d) del GDPR:

- comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

- il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni sopra citate è soddisfatta.

Per la comunicazione di una violazione dei dati personali all'interessato si rinvia alla "procedura per la gestione di data breach ai sensi del GDPR (Regolamento europeo 679/2016) allegato al "Regolamento sulla protezione dei dati personali" approvato con deliberazione del CIA n. 15 del 15 aprile 2020.