AGGIORMANETI WEB SERVER

SCOPO E OBBIETIVI:

Questa Governance ha lo scopo di aggiornare il Web Server attualmente utilizzato in maniera sicura,
seguendo una struttura ben definita, per limitare eventuali rischi.

- Mantenere la sicurezza del Web Server, tramite l'installazione delle ultime versioni del Web Server
- Assicurare la continuità dei servizi erogati dal gruppo, e quindi minimizzare al minimo il rischio di interruzione del servizio
- Migliorare la struttura è la sicurezza del Web Server, tremite nuovi aggiornamenti e patch del server

AUTORITÀ RESPONSABILE:

- Il Responsabile del reparto IT dovrà implementare i futuri aggiornamenti del Web Server.
- Il Responsabile Della Cyber Security deve essere attivamente coinvolto e notificato di ogni cambiamento del server, durante la fase di aggiornamento.
- Il Responsabile del Web Server dovrà installare i futuri aggiornamenti e patch del sistema per garantire la massima protezione e velocità del Web-serve, Esso avrà anche un ruolo di supervisione dell'intera infratruttura.

AGGIORMANETI WEB SERVER

PROCESSO DI AGGIORNAMENTO:

Valutazione degli aggiornamenti:

- il Responsabile IT dovrà analizzare e valutare le attuali minaccie per la versione corrente del Web-server e intraprendere azioni cautelari per la protezione dei dati su di esso

Pianificazione degli aggiornamenti:

- Il Responsabile IT e il Responsabile del Web Server, dovranno periodicamente aggiornare in maniera forzata il Web Server ogni 3 anni, garantendo allo stesso momento l'ordinario funzionamento di tutta l'infrastruttura.

Implementazione degli aggiornamenti:

- il Responsabile del Web Server, dovrà seguire questa linea guida per l'implementazione degli aggiornamenti del Server:

1. Effettuare un Back-up dell'interno sistema.
2. separare e clonare il Web Server per non aver nessuna interruzione di servizio.
3. scaricare il nuovo aggiornamento o Patch.
4. implementare all'interno del server il nuovo aggiornamento o Patch.
5. passare alla fase di Testing.

AGGIORMANETI WEB SERVER

TEST DEGLI AGGIORNAMENTI:

- Prima di mettere online il Web Server con il nuovo aggiornamento di sistema, esso dovrà passare dei test di Penetration Testing interni, per garantire la stabilità e la sicurezza degli aggiornamenti implementati.

DEPLOY DEGLI AGGIORNAMENTI:

- secondo i risultati della fase precedente il Responsabile IT dovrà valutare i risultati e decidere quali aggiornamenti e patch potranno passare dalla fase di test alla fase di produzione, questo per garantire la massima sicurezza dei dati.

MONITORAGGIO E VERIFICA:

- dopo gli aggiornamenti e resi online, il server dovrà essere attivamente monitorato per rilevare eventuali problemi o rallentamenti del sistema.

DOCUMENTAZIONE:

- alla fine di tutti i processi elencati, per ogni aggiornamento o patch effettuata al Web Server, si dovrà stilare una documentazione dettagliata del motivo dell'implementazione del relativo aggiornamento, e di chi l'ha implementato