chiaro)		
DESIGNAZIONE AMMINISTRATORI DI SISTEMA		
✓ Rilevata necessità di dettagliare meglio compiti e responsabilità nei confronti degli amministratori di sistema;	La designazione degli amministratori di sistema deve avvenire su base individuale e, contestualmente all'assegnazione delle mansioni, deve essere fornito ad ogni soggetto l'elenco dettagliato degli ambiti di operatività consentiti.	B
VERIFICHE ATTIVITA'		
✓ Rilevata necessità di implementare una maggiore verifica delle attività svolte come amministratore di sistema;	L'operato degli amministratori di sistema deve essere sottoposto a verifiche periodiche, almeno annuali, al fine di verificare la sussistenza delle condizioni che hanno portato all'assegnazione della mansione di amministratore di sistema.	D
SICUREZZA ACCESSI AMMINISTRATORI DI SISTEMA		
✓ Si suggerisce di rafforzarle il metodo di accesso come amministratore di sistema	Per l'accesso amministrativo a sistemi critici si consiglia di utilizzare meccanismi di strong authentication, utilizzando ad esempio certificati digitali, smart card, token.	D

Flussi dati

RISULTANZE AUDIT ORGANIZZATIVO	REMEDIATION	PRIORITA'
GARANZIE DI RISERVATEZZA – TRASMISSIONE FLUSSI DATI DA FORNITORE A SANTER		
✓ Il flusso di trasferimento dei file potrebbe presentare problematiche di sicurezza e falle a livello di tecnologia utilizzata;	Verificare l'efficacia dei sistemi di protezione (zip + password) dei flussi attualmente utilizzati per lo scambio dei dati sensibili valutando anche l'efficacia dell'attuale separazione dei file;	A
GARANZIE DI RISERVATEZZA – ASSEMBLAGGIO FLUSSI		
✓ Non si ha l'evidenza dell'adozione di misure di sicurezza minime presso i fornitori;	Verificare presso i fornitori il processo di creazione dei flussi e l'effettiva adozione di misure di sicurezza che ne tutelino la riservatezza;	A
TRACCIABILITA' FLUSSI DATI DA FORNITORE A SANTER, DA SANTER A LI		
✓ Non si ha l'evidenza dell'adozione di misure di tracciatura relative ai flussi in ingresso	Le operazioni di scambio di dati devono essere tracciate e sottoposte a monitoraggio per permettere di identificare i soggetti	B

	interessati e i file scambiati. Il tracciamento deve essere effettuato in conformità ai requisiti di Tracciamento e Logging;	
INTEGRITA'		
✓ Non si ha l'evidenza dell'adozione di misure che garantiscono l'integrità dei flussi in ingresso	Implementare meccanismi per garantire l'integrità dei dati nelle diverse fasi del trasferimento del dato; eventuali corruzioni dei dati devono essere segnalate.	B
PROTEZIONE DA INJECTION SUI FLUSSI		
✓ Non si ha evidenza dell'implementazione di sistema che verifichino l'assenza di malicious code all'interno dei flussi in ingresso	Implementare sistemi per la verifica di codice malevolo all'interno dei flussi;	A
CONFIDENZIALITA' DEL DATO		
✓ Non si ha evidenza dell'implementazione di controlli efficaci per garantire la confidenzialità del dato su tutta la filiera di fornitura / processo gestionale;	Concordare, implementare, rilasciare in produzione e mantenere i dovuti controlli di sicurezza, per garantire l'integrità, la confidenzialità e la disponibilità del dato.	C
CONDIVISIONE		
✓ Non si ha evidenza della condivisione di chiare linee guida e dei relativi punti di controllo per gestire le fasi di trasferimento dei dati / informazioni.	Regolamentare in maniera più dettagliata i processi di trasferimento dei dati;	A

Log Management

RISULTANZE AUDIT ORGANIZZATIVO	REMEDIATION	PRIORITA'
EVENTI DA TRACCIATURA APPLICATI, SISTEMI E DB		
✓ L'audit evidenza una carenza nell'identificazione degli eventi sottoposti a tracciatura log	Definire, insieme alla committenza gli eventi e gli oggetti soggetti a tracciatura (per tutti i sistemi, applicazioni e db in particolare per quelli ritenuti critici); Sottoporre i log a un processo di classificazione e relativa gestione sicura	B
REPORTISTICA		
✓ L'audit evidenza una carenza nell'identificazione degli eventi	Implementare sul prodotto in fase di installazione (splunk) un sistema di reportistica	B

sottoposti a tracciatura log	e consultazione avanzate;	
ANALISI		
✓ L'audit evidenza una carenza nell'identificazione degli eventi sottoposti a tracciatura log	Implementare un sistema integrato che raccordi sia i log sistemistici che quelli applicativi che quelli derivanti dai sistemi di difesa attivi;	B
TRACCIATURA ATTIVITA' AMMINISTRATORI		
✓ L'audit evidenza una carenza nell'identificazione degli eventi sottoposti a tracciatura log	Implementare meccanismi per il tracciamento esaustivo delle attività eseguite dai profili amministrativi;	B
TRASFERIMENTO FILE LOG		
✓ L'audit evidenza una carenza nell'identificazione degli eventi sottoposti a tracciatura log	Implementare meccanismi per il trasferimento dei file di log al sistema di raccolta centralizzato che siano in grado di garantire l'integrità e riservatezza dei log generati.	B
SISTEMA DI COLLETTAMENTO E ANALISI		
✓ L'audit evidenza una carenza nell'identificazione degli eventi sottoposti a tracciatura log	Il sistema di raccolta centralizzato deve essere dimensionato adeguatamente in modo da garantire la disponibilità dei dati.	B
SISTEMA DI COLLETTAMENTO E ANALISI		
✓ L'audit evidenza una carenza nell'identificazione degli eventi sottoposti a tracciatura log	Devono essere previsti meccanismi/procedure periodiche per la verifica della corretta generazione dei log.	C
PROCESSO DI GESTIONE DEI LOG		
✓ L'audit evidenza una carenza nell'identificazione degli eventi sottoposti a tracciatura log	Deve essere realizzata e mantenuta aggiornata la documentazione relativa ai sistemi di raccolta dei log.	C
MEMORIZZAZIONE E BACKUP EVENT LOG		
✓ L'audit evidenza una carenza nell'identificazione degli eventi sottoposti a tracciatura log	Devono essere utilizzati dei supporti di memorizzazione esterni al sistema centralizzato di raccolta dei log di sicurezza al fine di permettere l'archiviazione per esigenze di storicizzazione dettate da normative, regolamenti, esigenze operative e/o attività di indagini e ispezioni.	B
IMMODIFICABILITA' DEI LOG		
✓ L'audit evidenza una carenza nell'identificazione degli eventi sottoposti a tracciatura log	Deve essere garantita la non modificabilità nel tempo dei log.	B
PROCEDURE LOG MANAGEMENT		

✓ L'audit evidenza una carenza nell'identificazione degli eventi sottoposti a tracciatura log	Le procedure la gestione, l'analisi e la consultazione dei log di sicurezza devono essere documentate.	C
LOG MANAGEMENT		
✓ L'audit evidenza una carenza nell'identificazione degli eventi sottoposti a tracciatura log	Devono essere implementati meccanismi di controllo per la fase di attivazione / disattivazione dei log e degli accessi logici ai file di log e di reportistica in tutte le fasi di gestione dei log stessi, limitandone l'accesso al solo personale autorizzato, preservandone la riservatezza, l'integrità e la disponibilità.	B
LOG MANAGEMENT		
✓ L'audit evidenza una carenza nell'identificazione degli eventi sottoposti a tracciatura log	Qualsiasi tipologia di report generato a partire da log deve seguire la stessa classificazione dei dati in esso contenuti, le stesse regole e misure di sicurezza per la gestione di tali dati.	B

Incident Management

RISULTANZE AUDIT ORGANIZZATIVO	REMEDIATION	PRIORITA'
PROCESSO DI GESTIONE DEGLI INCIDENTI / ESCALATION		
✓ Non è stato identificato un processo formale per la gestione degli incident e il coinvolgimento degli eventuali fornitori;	Deve essere formalizzato e implementato un processo per la Gestione degli Incidenti;	C
PROCESSO DI GESTIONE DEGLI INCIDENTI / ESCALATION		
✓ Non è stato identificato un processo formale per la gestione degli incident e il coinvolgimento degli eventuali fornitori;	Implementare un modello organizzativo per gestire il processo di incident, nominando referenti e responsabili per la gestione delle diverse attività; Il modello organizzativo per la gestione degli incidenti di sicurezza deve prevedere il coinvolgimento degli eventuali fornitori che gestiscono in outsourcing sistemi di elaborazione, apparati di rete e applicazioni informatiche dell'organizzazione. Il modello organizzativo per la gestione degli incidenti di sicurezza deve definire i ruoli e le responsabilità dei referenti in merito alle seguenti	C

	attività: L'apertura e la chiusura dell'incidente di sicurezza; Il monitoraggio e la notifica degli incidenti di sicurezza; Il coordinamento delle attività di contenimento ed eliminazione dell'incidente di sicurezza; L'esecuzione delle attività di contenimento e contrasto dell'incidente di sicurezza; L'analisi dell'incidente di sicurezza; Il coordinamento delle comunicazioni interne (verso dipendenti e dirigenti); Il coordinamento delle comunicazioni ufficiali con l'esterno (verso clienti, azionisti, Mass Media, associazioni, fornitori/partner); La gestione dei rapporti con la Pubblica Autorità.	
✓ Non è stato identificato un processo formale per la gestione degli incident e il coinvolgimento degli eventuali fornitori;	Formalizzare una procedura di escalation che comprenda i seguenti aspetti: Tempistiche di comunicazione in base alla classificazione dell'incidente; Notifica alle funzioni organizzative opportune in base alla tipologia dell'incidente e gli asset impattati; Contact list; Strumenti da utilizzare per la notifica. Prevedere una struttura/servizio di monitoraggio in tempo reale degli eventi di sicurezza. Predisorre test periodici ai fini di garantire l'effettivo funzionamento di tutte le procedure all'interno del processo di Gestione degli Incidenti.	C

Outsourcing – Gestione dei Fornitori

RISULTANZE AUDIT ORGANIZZATIVO	REMEDIATION	PRIORITA'
ANALISI DEL RISCHIO AFFERENTE AL FORNITORE		
✓ Non è stato evidenziato un processo che formalmente identifica e analizza i rischi relativi ai processi in carico ai fornitori	Analizzare il flusso / processo che coinvolge tutti gli asset informativi ritenuti sensibili (sia in formato informatico che	B

esterni comprese le possibili vulnerabilità afferenti al processo / sistemi informatici del fornitore stesso su cui vengono gestite informazioni sensibili.	fisico) erogato presso i fornitori e valutare il relativo rischio associato; definire ed implementare di conseguenza le opportune contromisure	
PROCESSO DI VERIFICA AI FORNITORI		
✓ Non è stato rilevato durante le fasi di audit un processo di verifica circa il livello di conformità / security implementato dai fornitori.	Implementare il processo di verifica / audit nei confronti dei fornitori. In particolare verificare con il fornitore il processo di gestione dei flussi	**B**
REQUISITI DI SICUREZZA FORMALMENTE RICHIESTI AL FORNITORE		
✓ Nell'affidamento dei servizi in outsourcing non sono definiti requisiti di sicurezza tecnici e protocolli comportamentali esaustivi a garantire una corretta gestione degli asset informativi ritenuti maggiormente critici in termini di riservatezza.	Richiedere formalmente le seguenti evidenze: ▪ il livello di performance della sicurezza atteso rispetto agli accordi stipulati; ▪ report di revisone periodica del livello di sicurezza ▪ le informazioni sulle minacce / incidenti di sicurezza ▪ le responsabilità di gestione della sicurezza	**D**