Amministratore di Sistema

Provvedimento del Garante per la protezione dei dati personali 27 novembre 2008 e successive integrazioni

CEDACRI GROUP

Obiettivi

Obiettivi di questa sessione formativa per gli Amministratori di Sistema è renderli edotti:

- dei rischi che incombono sui dati;
- delle misure disponibili per prevenire eventi dannosi;
- dei profili della disciplina sulla protezione dei dati personali;
- delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal Titolare.

"Resta parimenti ferma la necessità che, nell'individuare regole di condotta dei soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, sia svolta un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni (cfr. Allegato B) al Codice, regola n. 19.6; Parere n. 8/2001 cit., punto 9".

Le linee guida del Garante per posta elettronica e internet (G.U. n. 58 del 10 marzo 2007)

Agenda

La Legge sulla Privacy ed il provvedimento sugli Amministratori di Sistema

Gli adempimenti organizzativi

Gli strumenti e le attività di controllo

Premessa

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

"Le ispezioni effettuate in questi anni dall'Autorità hanno permesso di mettere in luce in diversi casi una scarsa consapevolezza da parte di organizzazioni grandi e piccole del ruolo svolto dagli amministratori di sistema. I gravi casi verificatisi negli ultimi anni hanno evidenziato una preoccupante sottovalutazione dei rischi che possono derivare quando l'attività di questi esperti sia svolta senza il necessario controllo."

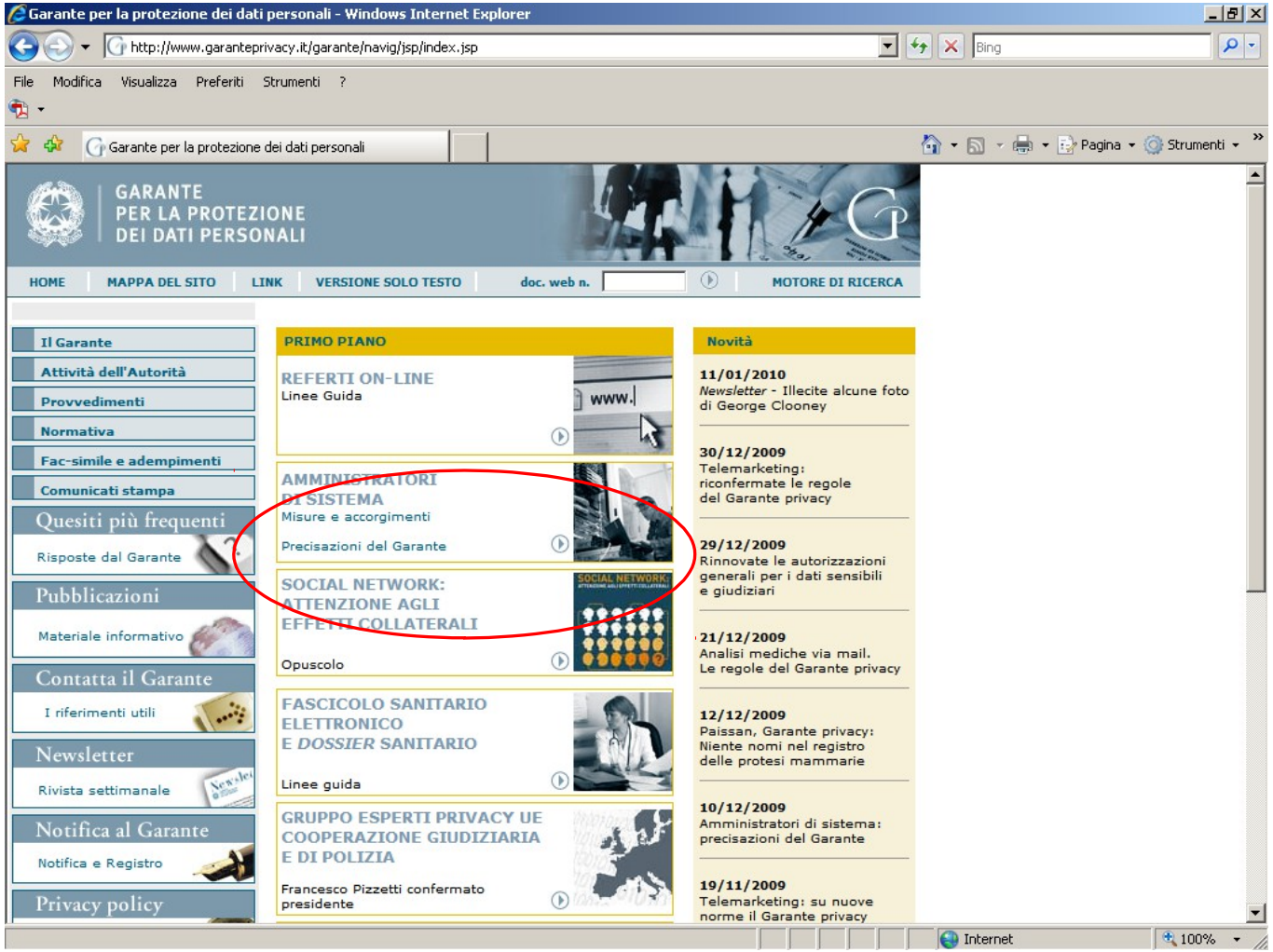
Comunicato stampa - 14 gennaio 2009

CEDACRI GROUP

Premessa

27 novembre 2008	Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema. Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico (di cui all'Allegato B) al Codice in materia di protezione dei dati personali.
14 gennaio 2009	Comunicato stampa - Amministratori di sistema: occorre massima trasparenza sul loro operato. Il Garante fissa i criteri, quattro mesi per mettersi in regola.
12 febbraio 2009	Proroga delle misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.
21 aprile 2009	Amministratori di sistema: avvio di una consultazione pubblica.
21 maggio 2009	FAQ
25 giugno 2009	Modifiche del provvedimento del 27/11/2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento.
15 dicembre 2009	Amministratori di sistema: precisazioni del Garante

Premessa


Garante per la protezione dei dati personali - Windows Internet Explorer
http://www.garanteprivacy.it/garante/navig/jsp/index.jsp
File Modifica Visualizza Preferiti Strumenti ?
Garante per la protezione dei dati personali
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
HOME MAPPA DEL SITO LINK VERSIONE SOLO TESTO doc. web n. MOTORE DI RICERCA
Il Garante
Attività dell'Autorità
Provvedimenti
Normativa
Fac-simile e adempimenti
Comunicati stampa
Quesiti più frequenti
Risposte dal Garante
Pubblicazioni
Materiale informativo
Contatta il Garante
I riferimenti utili
Newsletter
Rivista settimanale
Notifica al Garante
Notifica e Registro
Privacy policy
PRIMO PIANO
REFERTI ON-LINE
Linee Guida
AMMINISTRATORI DI SISTEMA
Misure e accorgimenti
Precisazioni del Garante
SOCIAL NETWORK: ATTENZIONE AGLI EFFETTI COLLATERALI
Opuscolo
FASCICOLO SANITARIO ELETTRONICO E DOSSIER SANITARIO
Linee guida
GRUPPO ESPERTI PRIVACY UE COOPERAZIONE GIUDIZIARIA E DI POLIZIA
Francesco Pizzetti confermato presidente
Novità
11/01/2010
Newsletter - Illecite alcune foto di George Clooney
30/12/2009
Telemarketing: riconfermate le regole del Garante privacy
29/12/2009
Rinnovate le autorizzazioni generali per i dati sensibili e giudiziari
21/12/2009
Analisi mediche via mail. Le regole del Garante privacy
12/12/2009
Paissan, Garante privacy: Niente nomi nel registro delle protesi mammarie
10/12/2009
Amministratori di sistema: precisazioni del Garante
19/11/2009
Telemarketing: su nuove norme il Garante privacy
Internet
100%

Agenda

La Legge sulla Privacy ed il provvedimento sugli Amministratori di Sistema

Gli adempimenti organizzativi

Gli strumenti e le attività di controllo

D.Lgs 30 Giugno 2003 n. 196

D.Lgs 30 Giugno 2003 n. 196

IL DECRETO LEGISLATIVO NR. 196 DEL 30 GIUGNO 2003
COSIDETTO
"CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI"
O
"CODICE PER LA PRIVACY"
VIENE EMANTO IL 30 GIUGNO 2003
ED ENTRA IN VIGORE IL 1 GENNAIO 2004

E COMPORTA L'ABROGAZIONE DELLA:

- LEGGE 675/1996
- NORME EMANATE A SEGUITO DELLA LEGGE 675

D.Lgs 30 Giugno 2003 n. 196

- NORMATIVA IN VIGORE -

- CODICE PROTEZIONE DATI PERSONALI
- ALLEGATO A) CODICE DEONTOLOGICO DI BUONA CONDOTTA
  [A1 Giornalisti; A2 scopi storici A3 scopi statistici ambito del Sistema Statistico Nazionale; A4 scopi statisti e scientifici, A5 crediti al consumo, affidabilità e puntualità pagamenti; A6 investigazioni difensive]
- ALLEGATO B) DISCIPLINARE TECNICO MISURE MINIME DI SICUREZZA TRATTAMENTO DATI
  [Ridurre al minimio i rischi di: I) DISTRUZIONE O PERDITA DEI DATI; II) ACCESSO NON AUTORIZZATO; III) TRATTAMENTO NON CONSENTITO O NON CONFORME ALLA RACCOLTA]
- ALLEGATO C) TRATTAMENTO DATI IN AMBITO GIUDIZIARIO E DI POLIZIA
- PROVVEDIMENTI DEL GARANTE

D.Lgs 30 Giugno 2003 n. 196

– IN SINTESI –

CHIUNQUE HA DIRITTO ALLA PROTEZIONE DEI PROPRI DATI PERSONALI

PER DARE EFFETTIVA APPLICAZIONE AL DIRITTO DELLA PROTEZIONE DEI DATI PERSONALI SONO PREVISTI ADEMPIMENTI:

FORMALI

SOSTANZIALI

MANCATO RISPETTO DEGLI ADEMPIMENTI PREVISITI IMPLICA:

RESPONSABILITÀ CIVILE (ex art 2050 CODICE CIVILE)

SANZIONI AMMINISTRATIVE

SANZIONI PENALI

D.Lgs 30 Giugno 2003 n. 196

– ADEMPIMENTI PRINCIPALI –

FORMALI

- NOTIFICA DEL TRATTAMENTO AL GARANTE
- INFORMATIVA ALL'INTERESSATO
- RACCOLTA DEL CONSENSO
- NOMINA E FORMAZIONE INCARICATI (E RESPONSABILI)
- CENSIMENTO TRATTAMENTI ESEGUITI
- DOCUMENTO PROGRAMMATICO SULLA SICUREZZA
- VIGILANZA E CONTROLLO

SOSTANZIALI

- ADOZIONE AGGIORNAMENTO MISURE DI SICUREZZA
  - MISURE MINIME DI SICUREZZA
    (indicate nel D.Lgs. 196/03 e allegato B . Disciplinare Tecnico).
  - MISURE DI SICUREZZA DETTATE DALL'EVOLUZIONE TECNOLOGICA
    (dalla natura dei dati, dal tipo di trattamento)

D.Lgs 30 Giugno 2003 n. 196

– SANZIONI –

ART. 161 OMESSA O INIDONEA INFORMATIVA ALL'INTERESSATO
da 6.000 a 36.000 euro

ART. 162 ALTRE FATTISPECIE
VIOLAZIONE: ART. 16 1° comma lettera, B
cessione del trattamento
da 10.000 a 60.000 euro
ART. 84 1° comma
modalità di comunicazione dati all'interessato
da 1.000 a 6.000 euro

ART 164 OMESSA INFORMAZIONE O ESIBIZIONE AL GARANTE
da 10.000 a 60.000 euro

D.Lgs 30 Giugno 2003 n. 196

– SANZIONI –

ART 167 TRATTAMENTO ILLECITO DEI DATI
RECLUSIONE DA 6 A 24 MESI
(se dal fatto deriva nocumento)
RECLUSIONE DA 6 A 24 MESI
(per comunicazione/diffusione)
RECLUSIONE DA 1 A 3 ANNI
(per reato grave al fine di trarre profitto o cagionare danni)

ART 168 FALSITÀ DELLE DICHIARAZIONI E NOTIFICAZIONI AL GARANTE
RECLUSIONE DA 6 MESI A 3 ANNI

ART 169 INADEGUATEZZA MISURE DI SICUREZZA
da 10.000 a 50.000 euro
RECLUSIONE SINO A 2 ANNI

ART 170 INOSSERVANZA DI PROVVEDIMENTI DEL GARANTE
RECLUSIONE DA 3 MESI A 2 ANNI

D.Lgs 30 Giugno 2003 n. 196

ART. 4 DEFINIZIONI - TRATTAMENTO

Qualunque operazione o complesso di operazioni effettuati con o senza l'ausilio di strumenti elettronici, concernenti:

- LA RACCOLTA
- LA REGISTRAZIONE
- L'ORGANIZZAZIONE
- LA CONSERVAZIONE
- LA CONSULTAZIONE
- L'ELABORAZIONE
- LA MODIFICAZIONE
- LA SELEZIONE
- L'ESTRAZIONE
- IL RAFFRONTO
- L'UTILIZZO
- L'INTERCONNESSIONE
- IL BLOCCO
- LA COMUNICAZIONE
- LA DIFFUSIONE
- LA CANCELLAZIONE E
- LA DISTRIBUZIONE DI DATI

ANCHE SE NON REGISTRATI IN UNA BANCA DATI

D.Lgs 30 Giugno 2003 n. 196

ART. 4 DEFINIZIONI - DATI

PERSONALI

QUALUNQUE INFORMAZIONE RELATIVA A PERSONA FISICA, GIURIDICA, ENTE O ASSOCIAZIONE, IDENTIFICATI O IDENTIFICABILI, ANCHE INDIRETTAMENTE, MEDIANTE RIFERIMENTO A QUALSIASI ALTRA INFORMAZIONE, INCLUSI I NUMERI DI IDENTIFICAZIONE PERSONALE.

SENSIBILI

I DATI PERSONALI IDONEI A RILEVARE L'ORIGINE RAZZIALE ED ETNICA, LE CONVINZIONI RELIGIOSE, FILOSOFICHE O DI ALTRO GENERE, LE OPINIONI POLITICHE, L'ADESIONE A PARTITI, SINDACATI, ASSOCIAZIONI OD ORGANIZZAZIONI A CARATTERE RELIGIOSO, FILOSOFICO, POLITICO O SINDACALE, NONCHÉ I DATI PERSONALI IDONEI A RILEVARE LO STATO DI SALUTE E LA VITA SESSUALE.

D.Lgs 30 Giugno 2003 n. 196

ART. 4 DEFINIZIONI - SOGGETTI

RELATIVAMENTE AL TRATTAMENTO DEI DATI PERSONALI SONO PREVISTI I SEGUENTI SOGGETTI:

- INTERESSATO
- TITOLARE
- RESPONSABILE
- INCARICATO

D.Lgs 30 Giugno 2003 n. 196

ART. 4 DEFINIZIONI - SOGGETTI

INTERESSATO

LA PERSONA FISICA, LA PERSONA GIURIDICA, L' ENTE O L'ASSOCIAZIONE CUI SI RIFERISCONO I DATI.

L'INTERESSATO DEVE ESSERE INFORMATO SU:

1. LE FINALITÀ E MODALITÀ DEL TRATTAMENTO;
2. LA NATURA OBBLIGATORIA O FACOLTATIVA DEL CONFERIMENTO DEI DATI;
3. LE CONSEGUENZE DELL'EVENTUALE RIFIUTO;
4. I SOGGETTI AI QUALI POSSONO ESSERE COMUNICATI I DATI O CHE POSSONO VENIRNE A CONOSCENZA IN QUALITÀ DI RESPONSABILI O INCARICATI, NONCHÉ L'AMBITO DI DIFFUSIONE DEI DATI;
5. I DIRITTI ALL'ART. 7 (x es.: cancellazioni o blocco)
6. GLI ESTREMI DEL TITOLARE E DEL RESPONSABILE .

D.Lgs 30 Giugno 2003 n. 196

ART. 4 DEFINIZIONI - SOGGETTI

TITOLARE

LA PERSONA FISICA, LA PERSONA GIURIDICA, LA PUBBLICA AMMINISTRAZIONE E QUALSIASI ALTRO ENTE, ASSOCIAZIONE OD ORGANISMO CUI COMPETONO,
ANCHE UNITAMENTE AD ALTRO TITOLARE,
LE DECISIONI IN ORDINE
ALLE FINALITÀ,
ALLE MODALITÀ DEL TRATTAMENTO DI DATI PERSONALI
E AGLI STRUMENTI UTILIZZATI,
IVI COMPRESO IL PROFILO DELLA SICUREZZA.

D.Lgs 30 Giugno 2003 n. 196

ART. 4 DEFINIZIONI - SOGGETTI

TITOLARE

AL TITOLARE COMPETONO TUTTI GLI ADEMPIMENTI FORMALI E SOSTANZIALI RICHIESTI DALLA NORMATIVA.

TRA QUESTI, IL TITOLARE, DEVE
DEFINIRE E CONTROLLARE IL RISPETTO
DELLE MODALITÀ OPERATIVE SULLA SICUREZZA,
NOMINARE GLI INCARICATI
(esclusivamente persone fisiche)
PUÒ EVENTUALMENTE
NOMINIARE I RESPONABILI
(anche persona giuridica).

D.Lgs 30 Giugno 2003 n. 196

ART. 4 DEFINIZIONI - SOGGETTI

RESPONSABILE

LA PERSONA FISICA, LA PERSONA GIURIDICA, LA PUBBLICA AMMINISTRAZIONE E QUALSIASI ALTRO ENTE, ASSOCIAZIONE OD ORGANISMO PREPOSTI DAL TITOLARE AL TRATTAMENTO DI DATI PERSONALI.

D.Lgs 30 Giugno 2003 n. 196

RESPONSABILE

È DESIGNATO FACOLTATIVAMENTE DAL TITOLARE

1. SE NOMINATO, DEVE ESSERE INDIVIDUATO TRA SOGGETTI CHE PER ESPERIENZA, CAPACITÀ ED AFFIDABILITÀ FORNISCANO IDONEA GARANZIA DEL PIENO RISPETTO DELLE VIGENTI DISPOSIZIONI IN MATERIA DI TRATTAMENTO, COMPRESO IL PROFILO DELLA SICUREZZA.
2. PER ESIGENZE ORGANIZZATIVE POSSONO ESSERE DESIGNATI RESPONSABILI PIÙ SOGGETTI, ANCHE MEDIATE SUDDIVISIONE DEI COMPITI.
3. I COMPITI AFFIDATI AL RESPONSABILE SONO SPECIFICATI PER ISCRITTO DAL TITOLARE.
4. IL RESPONSABILE EFFETTUA IL TRATTAMENTO ATTENENDOSI ALLE ISTRUZIONI IMPARTITE DAL TITOLARE IL QUALE, ANCHE TRAMITE VERIFICHE PERIODICHE VIGILA SULLA PUNTUALE OSSERVANZA DELLE DISPOSIZIONI DI LEGGE E DELLE PROPRIE ISTRUZIONI.

D.Lgs 30 Giugno 2003 n. 196

INCARICATO

LE PERSONE FISICHE, AUTORIZZATE A COMPIERE OPERAZIONI DI TRATTAMENTO DAL TITOLARE O DAL RESPONSABILE.

ART. 30 - INCARICATI

LE OPERAZIONI DI TRATTAMENTO POSSONO ESSERE EFFETTUATE SOLO DA INCARICATI CHE OPERANO SOTTO LA DIRETTA AUTORITÀ DEL TITOLARE O DEL RESPONSABILE ATTENENDOSI ALLE ISTRUZIONI IMPARTITE.
LA DESIGNAZIONE È EFFETTUATA PER ISCRITTO E INDIVIDUA L'AMBITO DEL TRATTAMENTO CONSENTITO.
SI CONSIDERA TALE ANCHE LA DOCUMENTATA PREPOSIZIONE DELLA PERSONA FISICA AD UNA UNITÀ PER LA QUALE È INDIVIDUATO L'AMBITO DEL TRATTAMENTO CONSENTITO AGLI ADDETTI DELL'UNITA' MEDESIMA.

D.Lgs 30 Giugno 2003 n. 196

PROVVEDIMENTO DEL GARANTE DEL 27 NOVEMBRE 2008

"MISURE E ACCORGIMENTI PRESCRITTI AI TITOLARI DEI TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI RELATIVAMENTE ALLE ATTRIBUZIONI DELLE FUNZIONI DI AMMINISTRATORE DI SISTEMA"

CON IL QUALE IL GARANTE

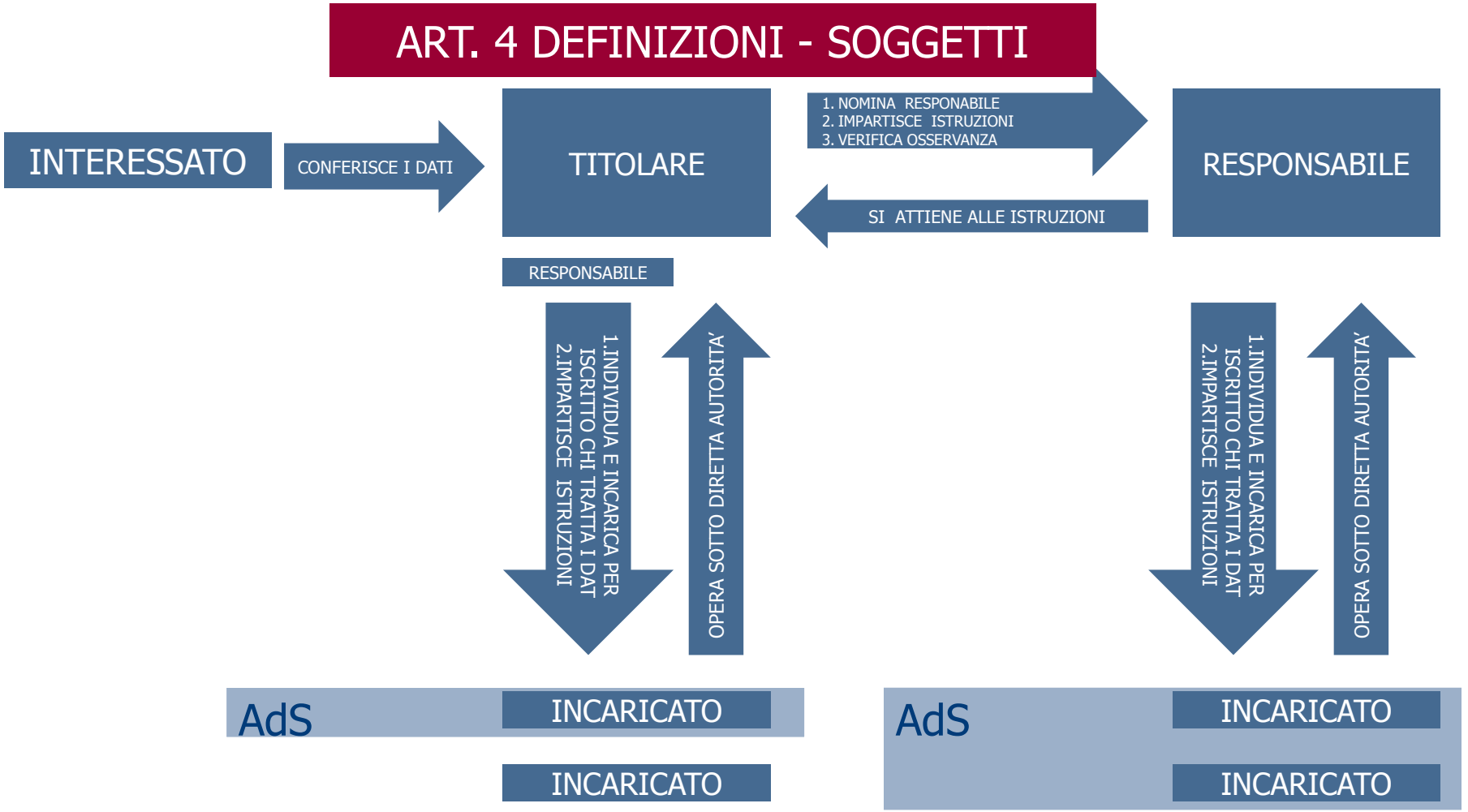
RICHIAMA I TITOLARI

A PRESTARE ATTENZIONE

AL RUOLO DEGLI AMMINISTRATORI DI SISTEMA ED IN PARTICOLARE A:

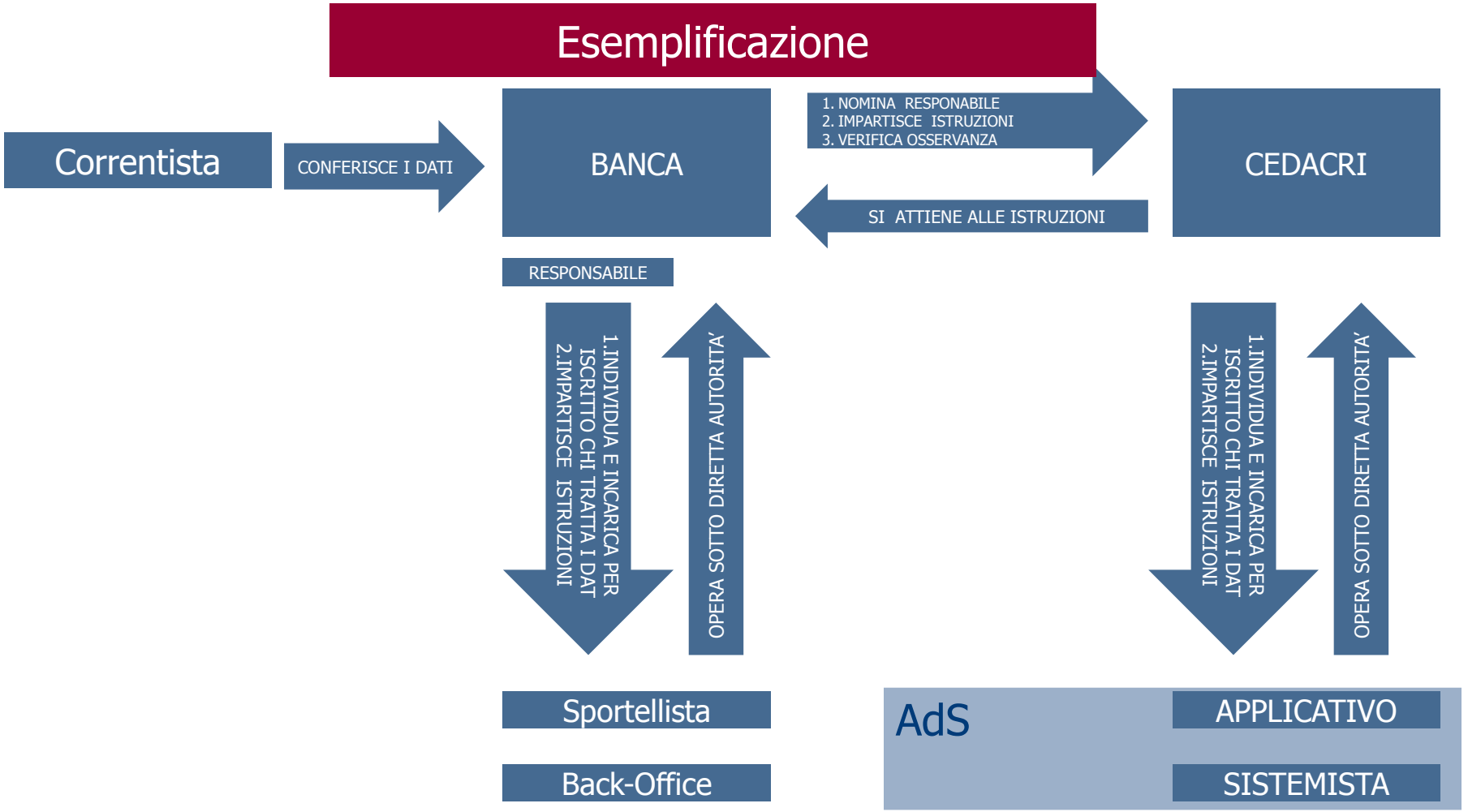
1. ADOTTARE IDONEE CAUTELE VOLTE A PREVENIRE ED ACCERTARE EVENTUALI ACCESSI NON CONSENTITI AI DATI PERSONALI
2. VALUTARE CON PARTICOLARE CURA L'ATTRIBUZIONE DI FUNZIONI TECNICHE CORRISPONDENTI O ASSIMILABILI A ADS ANCHE IN CASO DI ACCESSO FORTUITO AI DATI PERSONALI

D.Lgs 30 Giugno 2003 n. 196



CEDACRI GROUP

D.Lgs 30 Giugno 2003 n. 196



CEDACRI GROUP

Agenda

La Legge sulla Privacy ed il provvedimento sugli Amministratori di Sistema

Gli adempimenti organizzativi

Gli strumenti e le attività di controllo

Misure di sicurezza e misure del Provvedimento

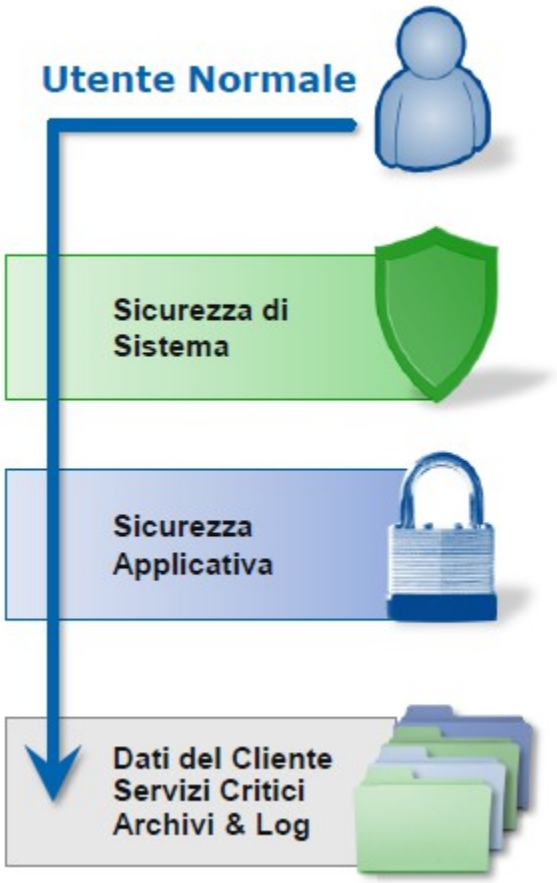
- Misure “idonee”
- Misure “minime”

complesso delle misure tecniche, informatiche, organizzative , logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell’art. 31.

Misure prescritte nel Provvedimento:

- L'Autorità ravvisa inoltre l'esigenza di individuare in questa sede alcune prime misure di carattere organizzativo che favoriscano una più agevole conoscenza, nell'ambito di organizzazioni ed enti pubblici e privati, dell'esistenza di determinati ruoli tecnici, delle responsabilità connesse a tali mansioni e, in taluni casi, dell'identità dei soggetti che operano quali amministratori di sistema in relazione ai diversi servizi e banche di dati.

Perché individuare gli Amministratori di Sistema



CEDACRI GROUP

Gli adempimenti organizzativi

CEDACRI GROUP

Gli adempimenti organizzativi

a. Valutazione delle caratteristiche soggettive

"L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza."

- L'attribuzione delle funzioni deve avvenire previa scrupolosa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato;
- Tale soggetto deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo di sicurezza;
- Si tratta di valutare il possesso di qualità tecniche, professionali e di condotta, non di requisiti morali.

Gli adempimenti tecnico-organizzativi

b. Designazioni individuali

"La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato."

- La designazione deve essere individuale e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- È sufficiente specificare l'ambito di operatività in termini più generali, per settori o per aree applicative, senza obbligo di specificarlo rispetto a singoli sistemi, a meno che non sia necessario in caso specifici.

Gli adempimenti tecnico-organizzativi

c. Elenco degli amministratori di sistema

"Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante."

- Si tratta del minimo insieme di dati identificativi utili ad individuare il soggetto nell'ambito dell'organizzazione di appartenenza;
- In caso di trattamento di informazioni di carattere personale dei lavoratori, si deve rendere nota o conoscibile l'identità degli Amministratori di Sistema.

CEDACRI GROUP

Gli adempimenti tecnico-organizzativi

d. Servizi in outsourcing

"Nel caso di servizi di amministrazione di sistema affidati in *outsourcing il titolare o il responsabile* esterno devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema."

- Occorre conservare direttamente e specificamente, per ogni evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema.

Gli adempimenti tecnico-organizzativi

e. Verifica delle attività

"L'operato degli AdS deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti."

- È da sottoporre a verifica l'attività svolta dall'AdS nell'esercizio delle sue funzioni;
- Va verificato che le attività svolte dall'AdS siano conformi alle mansioni, ivi compreso il profilo relativo alla sicurezza;
- La raccolta dei log serve per verificare anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, sistemi cui ci si è collegati, ecc.).

Gli adempimenti tecnici

f. Registrazione degli accessi

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli AdS. Le registrazioni (*access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di* verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

- Bisogna adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e degli archivi elettronici da parte degli AdS.
- Le registrazioni devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo;
- I log devono comprendere i riferimenti temporali e la descrizione dell'evento che li ha generati ed essere conservati per almeno 6 mesi.

I canali informativi

Portale	Aggiornamenti Normativi DPS Link al Sito del Garante
Newsletter	Informazioni sul Provvedimento Aggiornamenti sulle attività svolte in Cedacri
Lettera di incarico	Documento formale

Agenda

La Legge sulla Privacy ed il provvedimento sugli Amministratori di Sistema

Gli adempimenti organizzativi

Gli strumenti e le attività di controllo

La verifica delle attività

- L'attività di verifica era già prevista tra i compiti del titolare (cioè delle banche Clienti) in relazione alle attività dei responsabili
  - Art. 29, comma 5 del Codice

"Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni."

- I controlli possono essere effettuati dal Titolare o dal Responsabile da lui nominato.

- A discrezione può essere incaricata una terza parte indipendente.

I controlli da effettuare

Controllo della predisposizione dell'elenco degli amministratori, contenente gli identificativi e le relative funzioni attribuite ad ognuno

Verifica periodica della documentazione predisposta, in termini di completezza, correttezza ed accuratezza.

I controlli da effettuare

Verifica della designazione individuale degli amministratori, recante gli ambiti di operatività

Viene verificato che gli AdS siano stati designati mediante una comunicazione personale contenente gli ambiti di operatività.

La lettera verrà consegnata ai nuovi dipendenti all'atto della assunzione.

I controlli da effettuare

Valutazione delle caratteristiche soggettive della capacità e dell'affidabilità del soggetto cui sono state attribuite le funzioni di amministratore di sistema

La valutazione viene effettuata nel momento in cui il dipendente viene chiamato a svolgere un incarico che rientra tra quelli in oggetto (assunzione o spostamento di unità organizzativa).

Alla documentazione formale prodotta all'atto della assunzione si aggiunge anche una valutazione delle capacità del soggetto, legate al percorso di studi ed all'esperienza maturata.

I controlli da effettuare

Esame delle modalità di registrazione degli accessi logici agli archivi elettronici, garantendo completezza, inalterabilità, time stamping e tempi conservazione non inferiori a sei mesi

Analisi periodica degli accessi effettuati ai diversi ambienti per verificare che le attività monitorate (login/logout) siano in linea con gli incarichi assegnati e nei limiti degli ambiti di competenza.

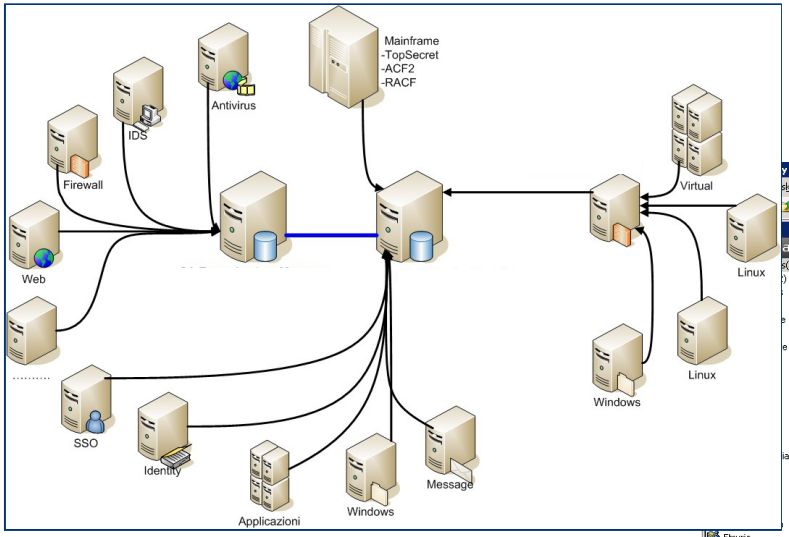
Controllo dei profili di accesso ai sistemi (autorizzazioni, permessi, ecc.) in relazioni ai compiti assegnati.

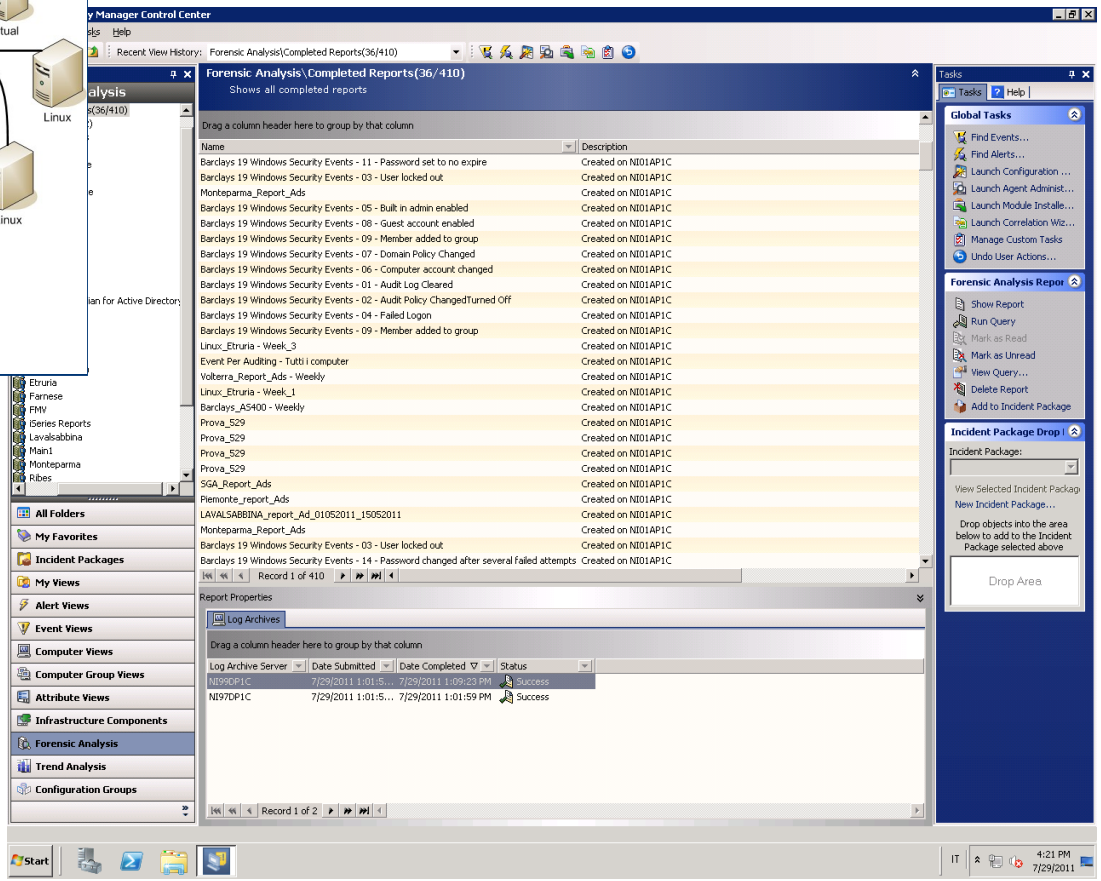
L’analisi dei log

- Gli eventi da registrare sono solo le autenticazioni informatiche;
- Plausibile la mera registrazione di log-in e log-out (quest’ultimo laddove rilevabile);
- Non è richiesto il log di attività interattive o di transazioni;
- Non si tratta di un audit log;
- Caratteristiche del log adeguate al contesto sulla base di valutazioni del titolare.

- La raccolta dei log serve per verificare eventuali anomalie e procedere alla definizione di opportuni profili di sicurezza.

La soluzione tecnologica





NetIQ Security Manager

CEDACRI GROUP