Política Específica de Segurança de Informação para Infraestruturas

Índice

1 Sumário Executivo

A Política Específica de Segurança da Informação para Infraestruturas tem como objetivo complementar a Política de Segurança da Informação PT Portugal a nível dos Sistemas e Tecnologias da Informação e Comunicação, no sentido de regular e implementar boas práticas de segurança e proteção da informação.

A Política Específica de Segurança da Informação para Infraestruturas aplica-se a todos os Sistemas e utilizadores da rede interna – ptNet. Sendo a ptNet a rede interna do Grupo PT, este documento define as suas atribuições e regula o seu funcionamento, de forma a garantir os níveis adequados de segurança e proteção da Informação.

2 Responsabilidades

2.1 Deveres dos utilizadores

O universo de utilizadores ptNet é composto por todos os colaboradores do grupo PT, colaboradores externos em regime de outsourcing, e ainda elementos externos à PT com necessidade de acesso temporário (p.ex., fornecedores, consultores e auditores). Os utilizadores da ptNet têm as seguintes responsabilidades no âmbito da segurança:

1. Zelar pelos equipamentos que lhes estão atribuídos, tanto de forma a garantir uma utilização no âmbito para que os equipamentos lhes foram atribuídos, como pela sua segurança (e da informação neles contida) e operacionalidade;
2. O cumprimento estrito da legislação relativa a direitos de autor é da estrita responsabilidade dos utilizadores. Não é permitido o uso de equipamentos periféricos de armazenamento de dados, tais como gravadores de CD's, discos USB ou similares, para cópia de programas informáticos, dados multimédia ou de qualquer outro documento que refira proteção de propriedade (copyright), nos termos em que essa cópia não seja autorizada;
3. Assegurar a confidencialidade das credenciais de acesso que lhes são confiadas;
4. Zelar pela segurança da informação da empresa, atribuindo-lhe a classificação apropriada quando sejam os donos da mesma e respeitando a classificação da informação a que têm acesso, procedendo em conformidade no seu manuseamento, no que diz respeito à sua confidencialidade e integridade. Se no cumprimento das suas atividades, os utilizadores da ptNet ficarem na posse de informações confidenciais ou proprietárias, estes devem garantir que as mesmas serão processadas com a maior confidencialidade, não as divulgando a terceiros;
5. Salvaguardar documentos (disponibilidade) relacionados com a atividade profissional do utilizador, armazenando-os nos servidores centrais, estando assim garantida a sua salvaguarda através de processos de backup, bem como a segurança da informação em conformidade com os níveis de confidencialidade. Os processos automáticos de backup garantem a disponibilidade para reposição da informação armazenada nos servidores centrais, desde que a mesma esteja disponível para backup nos prazos definidos;

6. Apagar os documentos do utilizador dos servidores centrais cuja validade esteja excedida ou que já não sejam relevantes para o trabalho do utilizador ou para o negócio da PT. Existem quotas de espaço em disco para armazenamento da informação, atribuídas por Direção ou grupo. As quotas poderão ser alteradas a pedido, carecendo de justificação por parte da Direção respetiva;

7. Os documentos de carácter pessoal deverão ser armazenados, exclusivamente, no computador do utilizador, em espaço devidamente identificável, não devendo o total de informação ser de tal maneira elevado que possa por em causa o desempenho dos equipamentos;

8. Os utilizadores são responsáveis por não ter comportamentos de risco (manuseamento do correio eletrónico, malware, navegação em websites perigosos, etc) que coloquem em risco os sistemas ou informação da empresa. Têm ainda o dever de denunciar situações (ou suspeitas) anómalas que possam estar relacionadas com a segurança lógica das TI's, SI's ou rede da PT;

2.2 MONITORIA

A PT reserva-se ao direito de monitorizar, sem pôr em causa a confidencialidade da informação, a área de armazenamento central, de forma a verificar a sua conformidade com a política da empresa.

2.3 ARQUITECTURA

A Arquitetura da Infra-estrutura de Rede e Segurança dos Datacenters internos é da responsabilidade da Direção de IT.

A definição de arquitetura da Rede WAN e LAN é responsabilidade da Direção de IT, sendo a sua gestão operacional assegurada pela Direção de Engineering and Network;

A Direção de IT é a única entidade autorizada a efetuar pedidos aos fornecedores internos, relativos à infra-estrutura, redes ou sistemas internos, quer se trate de novas implementações, instalações, ligações, alterações, acessos, endereçamentos ou outros.

3 Âmbito

Esta Política Específica de Segurança da Informação para Infraestruturas é aplicável a todos os colaboradores, fornecedores, consultores, auditores, incluindo prestadores de serviços de entidades externas que acedem às Tecnologias de Informação, Sistemas de Informação e Redes e Plataformas de Serviço da PT e empresas participadas.

No âmbito da ptNet, o termo "utilizador" será utilizado como referência a qualquer um dos indivíduos referidos anteriormente. A Política descrita no presente documento é aplicável a todos os sistemas de informação e comunicações de dados entre sistemas que sejam propriedade ou estejam sobre gestão da PT.

É indispensável assegurar que todos os utilizadores, independentemente do seu nível hierárquico, função e/ou vínculo contratual – internos à PT ou empresas suas participadas ou afetos a entidades externas ou outros com quem a PT contratou fornecimento de Produtos/Serviços – têm conhecimento desta política e acesso adequado à informação necessária para o desempenho das suas funções, sendo exigido destes o respeito pelos controlos de segurança implementados e o cumprimento da integridade, confidencialidade e disponibilidade da informação.

A segurança da informação, ou seja a sua confidencialidade, integridade e disponibilidade da mesma, é uma responsabilidade de todos. As orientações relativas a ações de sensibilização para a segurança (*awareness*) são descritas nesta política (secção **18**).

Todo o acesso a informação, infra-estrutura ou sistemas de informação que sejam propriedade PT, por parte de colaboradores externos ou parceiros, requer a pré-assinatura de Acordos de Confidencialidade (NDA – Non Disclosure Agreement), mesmo após o término da prestação do serviço para o qual foram contratados.

A Segurança Física das Instalações do Grupo PT não é abrangida por esta Política de Segurança. O Regime Regulador neste âmbito encontra-se descrito no *Regime Regulador dos Acessos Físicos às Instalações do Grupo PT (*OS02309CE*).*

4 Classificação da Informação

A informação criada, gerida e mantida por utilizadores ptNet requer obrigatoriamente a atribuição de uma classificação de nível de sensibilidade de segurança. Esta classificação deverá ter em conta os requisitos de confidencialidade, integridade e disponibilidade, bem como a sua importância relativa para o negócio.

A informação será classificada por quem a cria ou pelo responsável pela mesma, aquando da sua publicação ou disponibilização, tendo em conta os princípios (matriz) definidos na Política de Segurança da Informação PT Portugal a nível dos Sistemas e Tecnologias da Informação e Comunicação. Sempre que um documento não seja explicitamente classificado pelo dono da informação, por defeito será considerada a classificação PT RESERVADA.

Os mecanismos de segurança utilizados na comunicação, manuseamento, armazenamento e retenção da informação dependem da classificação da mesma, de acordo com a Política de Segurança da Informação PT Portugal a nível dos Sistemas e Tecnologias da Informação e Comunicação.

Toda a informação proprietária de clientes será considerada com a classificação de “PT Confidencial”.

5 Gestão Documental

Para efeitos de Gestão Documental, será utilizado o repositório único de informação localizado no IBPMS, onde são asseguradas a disponibilidade e o controlo de acessos aos dados nele constantes, conforme níveis de segurança pré-estabelecidos.

Este repositório deve obedecer a uma política de Backups regular (*Políticas de Backup STANDARD*) e os utilizadores nele definidos deverão obedecer às definições de Utilizador e Política de Passwords constantes deste documento, de forma a garantir os requisitos de disponibilidade, integridade e confidencialidade. Este repositório deve ainda garantir o *logging* dos acessos a todos os documentos nele constante e o controlo de versões (*versioning*).

6 Gestão de Acessos

Os acessos especificamente contemplados nesta Política Específica de Segurança da Informação para Infraestruturas são:

- Acessos à ptNet (Rede Interna do Grupo PT)
- Acessos remotos
- Acessos locais

Todos os acessos acima referidos deverão cumprir as orientações constantes na Política de Segurança da Informação PT Portugal a nível dos Sistemas e Tecnologias da Informação e Comunicação, nomeadamente (ver **Anexo A - Controlo de Acessos** Locais/Remotos - Síntese):

- Acessos inativos durante 60 dias (máximo) deverão ser bloqueados;
- Sempre que tecnicamente possível e sem impacto na rastreabilidade de utilizadores, no caso de estarem inativos durante 1 ano (máximo) deverão ser removidos;
- Acessos a Sistemas e Aplicações no âmbito do SOX deverão ser objeto de revisão periódica (anual), por parte dos responsáveis pelos acessos, no sentido de reavaliar a necessidade de manutenção dos mesmos;
- É obrigatória a execução de um procedimento que reavalie periodicamente a necessidade da manutenção de acessos privilegiados, contas com privilégios de administração em todas as tecnologias, sistemas e aplicações;
- São proibidos quaisquer acessos anónimos (ex:guest);
- Todos os acessos requerem a existência de um procedimento de suporte aos pedidos de acesso e respetivas autorizações, referindo claramente de quem é a responsabilidade da aceitação dos pedidos, bem como do seu cancelamento.

6.1 Acesso à Rede (Interna) ptNet

Este tema foi considerado apenas para publicação interna da Organização.

6.2 ACESSO REMOTO

Este tema foi considerado apenas para publicação interna da Organização.

6.3 ACESSO LOCAIS

Considera-se "Acesso Local" o acesso dentro do Datacenter a sistemas, plataformas ou infra-estrutura. Os Acessos Locais podem ser atribuídos às equipas técnicas (colaboradores internos ou prestadores de serviços em regime de outsourcing) e ainda a clientes que tenham infraestrutura alojada em Datacenters PT. No caso do acesso local de clientes, as necessidades dependem dos serviços contratualizados e o acesso está restrito à sua infraestrutura e meios de acesso à mesma.

O acesso local (lógico) implica necessariamente permissões de acesso físico ao Datacenter em causa, de acordo com a política e procedimentos de acessos físicos (*Regime Regulador dos Acessos Físicos às Instalações do Grupo PT*).

6.3.1 Aprovação dos Acessos Locais

Apenas são permitidos acessos locais a sistemas, plataformas ou infra-estruturas quando devidamente justificados, e aprovados.

Existem as seguintes variantes relativamente à aprovação dos acessos locais:

- **Colaboradores Internos da PT ou empresas suas participadas**

Aplicam-se apenas as diretrizes descritas em 6.3.1 - Aprovação dos Acessos Locais. Estes acessos são necessariamente nominais.

- **Prestadores de serviços (colaboradores externos)**

Aplicam-se apenas as diretrizes descritas em 6.3.1 - Aprovação dos Acessos Locais. Estes (conjuntos de) acessos podem ser atribuídos por prestador de serviços.

- **Clientes**

O acesso dos clientes restringe-se apenas às próprias infra-estruturas e o nível do acesso deve estar contratualmente determinado e discriminado. Para além das diretrizes descritas em 6.3.1. - Aprovação dos Acessos Locais, é necessária a discriminação, justificação e aprovação do cliente, de acordo com o especificado no respetivo contrato.

6.4 CONTROLOS AUTOMÁTICOS E REAVALIAÇÃO PERIÓDICA DE ACESSOS

Deverão ser implementados os controlos automáticos de bloqueio/eliminação de acessos sem utilização, bem como os procedimentos de reavaliação periódica de acessos constantes na Política de Segurança da Informação da PT Portugal a nível dos Sistemas e Tecnologias da Informação e Comunicação, nomeadamente os constantes no Anexo A - Controlo de Acessos Locais/Remotos - Síntese.

7 Autenticação

Todos os sistemas de informação, infra-estruturas e aplicações que necessitem de autenticação de utilizadores deverão autenticar centralmente na AD (Active Directory) de topo. Não são aceitáveis novas estruturas de gestão de passwords isoladas, com exceção dos casos que, por contingências da classificação de informação, obriguem a requisitos de segurança mais elevados, nomeadamente à utilização de mecanismos de autenticação forte.

Apenas serão aceites sistemas de autenticação complementares, nas seguintes situações:

- Quando a autenticação centralizada for inviável por questões técnicas
- Em casos de incompatibilidade de determinados equipamentos, utilizar o descrito no ponto 8 da Política de Segurança da Informação PT Portugal a nível dos Sistemas e Tecnologias da Informação e Comunicação

Todos os eventos correspondentes a padrões anormais/suspeitos de autenticação devem ser enviados para a plataforma de correlação de eventos e monitorização do SOC.

8 Segurança da relação com fornecedores

A relação com os nossos fornecedores pauta-se, desde o primeiro momento, pelo respeito por diretrizes que têm como objetivo a proteção da informação da PT acedida pelos fornecedores no âmbito da sua colaboração com a PT, assim como a salvaguarda da integridade dos serviços prestados pela PT. Assim, a gestão de fornecedores deve pautar-se pelas seguintes diretrizes:

a) Acesso à Informação: o fornecedor obriga-se a aceder às informações da PT e esclarecimentos que necessite sobre qualquer matéria da consulta e negociação, abstendo-se de qualquer uso indevido da mesma, respeitando os princípios estabelecidos na Política de Segurança da Informação da PT Portugal respeitante a Sistemas e Tecnologias de Informação e Comunicação doravante denominada Política de Segurança da Informação da PT;
b) Desenho e integração de sistemas seguros: O fornecedor obriga-se a garantir que os processos de integração e desenvolvimento, no âmbito dos produtos e serviços fornecidos, respeitam os princípios estabelecidos na Política de Segurança da Informação da PT;
c) A Política de Segurança da Informação da PT é disponibilizada aos fornecedores envolvidos nos processos de seleção para aquisição de produtos e/ou serviços no momento da emissão do Caderno de Encargos ou de outra informação relevante (ex.: RFI[1], RFQ[2]) no âmbito do processo de seleção;
d) Os fornecedores envolvidos num processo de seleção para aquisição de produtos e/ou serviços, no qual o fornecedor tenha acesso a informação sensível, assinarão uma Declaração comprometendo-se com as condições gerais que constam no caderno de encargos que incluirão, entre outras, as vertentes da Confidencialidade e da Proteção de Dados.
e) Sempre que se verifique, na relação da PT com fornecedores, a necessidade de existência de suporte contratual ou instrumento legalmente equiparável, estes incluirão a obrigação de cumprimento da Política de Segurança da Informação da PT, nomeadamente no que refere a confidencialidade da informação e obrigação de proteção de dados pessoais.

[1] Request for Information

[2] Request for Quotation

9 Standards para desenvolvimento de Aplicações

Este tema foi considerado apenas para publicação interna da Organização.

10 Política de passwords

As passwords fracas são por excelência uma das vulnerabilidades mais utilizadas na tentativa de acesso não autorizado, principalmente a partir do interior das organizações.

Idealmente, as passwords devem ser fáceis de memorizar e difíceis de adivinhar. Tendo em vista este objetivo, podem ser definidas uma série de diretrizes para a construção de passwords, que permitam assegurar as características que tornam as passwords fortes:

- **Comprimento**: passwords longas são mais fortes;
- **Alfabeto**: quanto mais vasto for o alfabeto utilizado (universo de caracteres utilizados), mais forte a password (ex: utilização de minúsculas, maiúsculas, caracteres numéricos e caracteres especiais);
- **Robustez contra ataques de dicionário**: uma password não deve conter palavras existentes em dicionário.

10.1 Recomendações gerais relativas a passwords

- As passwords são pessoais e intransmissíveis, não devendo ser reveladas a terceiros, seja por intermédio de conversa, telefone, correio eletrónico ou qualquer outro meio de comunicação;
- Não deverão ser usados dados pessoais na elaboração da password, tais como nome de familiares, datas de nascimento, etc.;
- A escolha de uma password deverá ser feita de forma a ser facilmente memorizável, sem necessidade de recorrer à sua escrita em qualquer suporte físico;
- As passwords não deverão ser escritas em qualquer sistema informático (incluindo PDAs), salvo se forem cifradas;
- As passwords não deverão ser reutilizadas (pelo menos as últimas 10);
- A password inicial atribuída a um utilizador deverá ser alterada pelo utilizador após a primeira utilização (ou recuperação da mesma). As aplicações/Sistemas/Tecnologias deverão implementar esta imposição de forma automatizada sempre que tecnicamente possível;

- Após a instalação de qualquer aplicação/sistema/tecnologia na PT, dever-se-ão garantir que de imediato todas as passwords de fábrica (atribuídas por omissão pelos fornecedores) de contas com privilégios de administração são alteradas;
- O procedimento de recuperação de password, em caso de esquecimento da mesma, deve incluir a solicitação ao próprio utilizador ou interlocutor/chefia da informação que identifique o utilizador inequivocamente (ex: nome completo, numero de contribuinte, numero de cartão do cidadão/BI, morada de residência, numero de empregado, etc.)

10.2 Recomendações para construção de passwords de utilizadores

As passwords de utilizadores não podem ser fracas**,** de acordo com a definição de password fraca da Política de Segurança da Informação PT Portugal a nível dos Sistemas e Tecnologias da Informação e Comunicação.

10.3 Recomendações para construção de passwords de gestão de Infra-estrutura e Sistemas

As passwords de gestão de Infra-estruturas e Sistemas deverão ser fortes, de acordo com a definição de password forte da Política de Segurança da Informação PT Portugal a nível dos Sistemas e Tecnologias da Informação e Comunicação.

As mesmas deverão ser testadas em http://gate.pulso.telecom.pt/tools/password-tester

Mecanismos de autenticação forte poderão ser disponibilizados de forma a garantir um maior nível de segurança, sempre que a classificação de informação ou criticidade das plataformas assim o exija.

11 Logging de atividades e/ou acessos

De forma a salvaguardar contas de utilizadores e sistemas torna-se necessário, em situações de força maior, inspecionar e monitorizar atividades de comunicação na rede ou de atividade em determinados sistemas. Unicamente a Direção de IT e a Direção de Cibersegurança poderão executar ou delegar em terceiros a execução destas operações.

Preferencialmente, os logs deverão ser remetidos para um repositório centralizado sob gestão das equipas de administração respetivas. A totalidade ou apenas parte desta informação deverá ser enviada para a plataforma de correlação, que suporta a atividade do SOC (Security Operations Center) na identificação e despiste de incidentes de segurança (ver secção 17 - Security Operations Centre (SOC)).

11.1 Requisitos de logging

Os logs de atividades e/ou acessos deverão ser tão indeléveis quanto possível, ter retenção mínima de 30 dias, e incluir a seguinte informação mínima:

- Origem e destino de conexões (identificação de rede)
- Utilização de serviços
- Data e hora de acesso aos sistemas (*login* e *logout*)

Sempre que possível, os logs de atividades e/ou acessos deverão também conter:

- Alterações efetuadas ao nível de sistema
- Identificação do utilizador (*username*)

11.2 Logging de acessos

Os acessos cujo controlo de acesso é regulado na presente Política de Segurança devem obedecer aos seguintes requisitos de logging:

- ptNet: logging centralizado
- Acessos remotos: logging centralizado
- Acessos locais: no próprio sistema e replicados para o logging centralizado.

11.3 LOGGING DE PLATAFORMAS, PARA CUMPRIMENTO DE REQUISITOS LEGAIS

Devem ser estritamente garantidos os prazos de retenção para os diferentes tipos de informação, de acordo com a legislação a que a PT está obrigada. São responsáveis pela disponibilidade e integridade dos dados supracitados os administradores das plataformas respetivas (ex: RADIUS Telepac, RADIUS Prime, plataformas de mail, portal SAPO, etc.).

O âmbito desta secção abrange quaisquer plataformas que possibilitem, a um utilizador ou cliente PT, acesso à Internet com endereço IP público da responsabilidade da PT – todos estes acessos deverão ser objeto de accounting, sendo os registos conservados durante o período de retenção obrigatório por lei ou descritos em Ordem de Serviço (OS32010CAPTP).

12 Antivírus

A existência de vírus (e *malware* em geral) em estações padrão e, principalmente em servidores, são vetores de ataque por excelência que colocam em risco a segurança da informação e dos Sistemas.

Para prevenir a receção de correio eletrónico contendo malware, todas as mensagens de correio eletrónico das plataformas de e-mail corporativas deverão ser inspecionadas por um sistema de deteção e remoção automática de vírus informáticos.

12.1 Gestão Centralizada de Antivirus

O Software de Antivírus, assim como as respetivas assinaturas serão atualizados automaticamente. No entanto, e dado o constante desenvolvimento de novos vírus associado à sua rápida disseminação, a eficácia deste tipo de deteção nem sempre pode ser garantida a 100%, razão pela qual poderão ser tomadas iniciativas destinadas ao combate a ameaças particulares que podem passar por medidas direcionadas ao tratamento de identificação ou remoção de malware (ex: envio/aplicação urgente de *extradat* ou *pattern* de AV, limpeza local de workstations ou servidores, etc).

12.1.1 . Estação Padrão – Ambientes de colaboradores

Este tema foi considerado apenas para publicação interna da Organização.

12.1.2 . Ambientes de IT

Os sistemas que suportam a infra-estrutura tecnológica têm, sempre que o suportarem, de ter instalado uma ferramenta de deteção e limpeza de vírus. Deverão ainda existir as conectividades na rede interna que permitam a comunicação da plataforma centralizada de Antivírus com os sistemas.

Qualquer sistema cujo funcionamento esteja comprometido pela ação de um qualquer *malware* deverá avaliar a possibilidade de ser desconectado da infra-estrutura para evitar posteriores desenvolvimentos que se reflitam negativamente sobre a mesma.

12.1.3 . Ambiente de clientes (em Datacentre)

Os sistemas de clientes alojados em Datacentre da PT deverão possuir ferramentas de deteção e limpeza de vírus. A PT recomenda a adoção de um antivírus centralizado nos sistemas dos clientes.

Qualquer sistema cujo funcionamento esteja comprometido pela ação de um qualquer *malware* poderá ser desconectado da infra-estrutura para evitar posteriores desenvolvimentos que se reflitam negativamente sobre a mesma ou sobre os serviços prestados. Nestes casos, o cliente deverá ser avisado, pelo respetivo gestor, de qualquer alteração ou ação tomada sobre os seus sistemas ou de como afeta o seu serviço.

13 Anti-SPAM

Por definição, considera-se SPAM qualquer mensagem eletrónica, não solicitada, enviada em massa. Por oposição, designa-se por HAM qualquer mensagem eletrónica desejada. Tipicamente, o SPAM poderá consistir em correio eletrónico enviado massivamente com fins publicitários, para ataques de phishing, etc.

As plataformas Anti-SPAM permitem marcar e-mails de SPAM que são rececionados nas plataformas de e-mail (no sentido *inbound* da Internet para o as plataformas de e-mail) podendo assim ser entregues em pasta criada para o efeito.

Existem atualmente duas plataformas anti-SPAM, abrangendo os seguintes universos:

- E-mail corporativo (domínios do grupo PT)
- Domínios de clientes PT

14 Atualizações de Software

A Política de Segurança da Informação PT Portugal a nível dos Sistemas e Tecnologias da Informação e Comunicação define, no capítulo 7.4, responsabilidades numa área de atuação crítica para a segurança dos Sistemas. Em termos de impacto, a não instalação de atualizações de software relacionadas com segurança permite que uma ou várias vulnerabilidades, do domínio público, sejam exploradas para atacar (p.e., infetando com *malware*) os referidos Sistemas.

14.1 SISTEMAS

A responsabilidade da instalação de *patch*es nos vários Sistemas é da responsabilidade dos administradores de Sistemas das plataformas respetivas.

Sempre que existam impedimentos técnicos (p.e., ao nível aplicacional) que sustentem a não instalação de *patches*, as situações deverão ser consideradas exceções, e ser devidamente documentadas.

As atualizações deverão ser formalmente planeadas, de acordo com os procedimentos vigentes, que devem incluir o procedimento de *fall-back*.

No caso de sistemas de clientes, as atualizações requerem o acordo prévio do respetivo cliente. Qualquer sistema cujo funcionamento seja comprometido devido à não instalação de patches poderá ser desconectado da infra-estrutura para evitar posteriores desenvolvimentos que se reflitam negativamente sobre a mesma ou sobre os serviços prestados. Nestes casos, o cliente deverá ser avisado, pelo respetivo gestor, de qualquer alteração ou ação tomada sobre os seus sistemas ou de como afeta o seu serviço.

14.2 ESTAÇÕES DE TRABALHO

Este tema foi considerado apenas para publicação interna da Organização.

15 Sincronização de Relógios

Para se poder assegurar que todos os registos que incluem *timestamps* (ex: logs, eventos a correlacionar, dados de tráfego, etc) se referem ao mesmo referencial temporal, assegurando assim a validade legal dos mesmos, é imprescindível que todos os sistemas estejam sincronizados em termos de relógio por um referencial temporal único.

Assim, todos os sistemas têm obrigatoriamente que sincronizar os seus relógios pela plataforma de NTP (Network Time Protocol) centralizada.

Ao nível da segurança da plataforma centralizada NTP, recomenda-se:

- A utilização de uma topologia adequada e com o número suficiente de fontes de relógio que garantam a sua disponibilidade
- Sempre que tecnicamente possível, a utilização de criptografia que garanta a autenticidade e integridade da informação de relógio disponibilizada aos diversos sistemas.

16 Incidente de Segurança

16.1 Definição

Entende-se genericamente como incidente de segurança, uma ação ou conjunto de ações desenvolvidas contra um computador ou rede de computadores que resulta, ou pode resultar, no comprometimento das propriedades básicas da segurança da informação: disponibilidade, integridade e confidencialidade.

Alinhadas com o processo de gestão de incidentes, devem ser utilizadas as designações específicas:

- Incidentes de segurança: define-se como sendo qualquer violação ou ameaça eminente de violação da Política de Segurança da Informação, de Políticas de Utilização Aceitáveis de serviços prestados, ou de boas práticas de segurança adotadas pela Organização. Esta definição compreende qualquer anomalia que afete ou possa vir a afetar a segurança da informação, nomeadamente as suas propriedades essenciais: confidencialidade, disponibilidade e integridade.
- Evento de segurança de informação: é uma ocorrência, observada num sistema ou rede, indicando uma possível quebra na política de segurança de informação ou falha dos controlos.

16.2 Classificação de incidentes

É utilizada a classificação de incidentes estabelecida pelo CERT.PT e adotada pela Rede Nacional de CSIRTs, da qual a PT é membro através do seu CSIRT. Esta classificação é baseada no resultado obtido ou pretendido com o ataque.

http://www.cert.rcts.pt/images/docs/Taxonomiav2.5.pdf

16.3 Comunicação de incidentes de Segurança

Sempre que seja identificada uma situação anómala e que possa estar relacionada com a segurança lógica das TI's, SI's ou rede da PT (p.e., conhecimento de máquinas infetadas com *malware*, e-mails de *phishing* afetando a PT ou a sua imagem, roubo de credenciais, etc), esta deve ser imediatamente comunicada ao CSIRT da PT (csirt@telecom.pt).

O contacto deverá ser efetuado através de e-mail para o CSIRT PT ou, em alternativa, poderá ser criado um ticket em Onedesk, 2.7 Cibersegurança, que o reencaminhará, após identificar o respetivo interlocutor.

A informação recebida é usada no tratamento do incidente no estrito respeito pelas leis vigentes de privacidade e proteção de dados pessoais. A informação de dados pessoais não é libertada a terceiros e, em caso de real necessidade, é solicitada à pessoa/entidade relatora uma autorização expressa para o efeito.

17 Security Operations Centre (SOC)

O SOC é uma equipa centralizada na PT, especializada em Segurança de Sistemas de Informação, responsável pela deteção e resposta a incidentes de Segurança, utilizando processos e procedimentos.

Os sistemas, plataformas e tecnologias críticas para o negócio da PT, deverão estar sob a monitorização do SOC.

Adicionalmente, os eventos gerados por tecnologias de deteção de vulnerabilidades de segurança lógica, sistemas de deteção de intrusão, antivírus, firewalls e plataforma de autenticação centralizada, deverão ser enviados para a plataforma de correlação de eventos e monitoria do SOC.

18 Sensibilização para a Segurança (awareness)

A PT toma medidas de natureza técnica, contratual, administrativa e física para garantir a disponibilidade, integridade e confidencialidade da informação. No entanto, a segurança da informação é uma responsabilidade de todos (inclusivamente dos utilizadores da ptNet) os que a ela acedem.

Neste sentido foi criado foi criado o *e-Learning em Segurança da Informação*, disponível na plataforma de e-learning da PT. Não obstante, sempre que sejam identificadas necessidades de formação específica na área da Segurança da Informação, estas necessidades deverão ser endereçadas à DRH.

A PT deverá ainda divulgar e sensibilizar para a Política de Segurança da Informação PT Portugal a nível dos Sistemas e Tecnologias da Informação e Comunicação a sua comunidade alvo.

19 Exceções à Política de Segurança

Todos os pedidos de exceção à Política Específica de Segurança da Informação para Infraestruturas da PT têm que ser devidamente justificados, autorizados e documentados. Estes pedidos deverão ser enviados para a Direção de Cibersegurança.

20 Revisão da Política de Segurança

A Política Especifica de Segurança da Informação para Infraestruturas é revista anualmente, ou sempre que se justifique em termos de necessidades técnicas ou de negócio.

21 Anexo A - Controlo de Acessos Locais/Remotos - Síntese

Tabela de ACESSOS

	COLABORADORES			CLIENTES	PARCEIROS (externos)
	INTERNOS		OUTSOURCERS ou Suporte Externo subcontratado		
	Normais	Técnicos			
Locais	IF Rede do Edifício	IF Rede dos Edifícios ou DCs	IF Rede dos Edifícios ou DCs	IF Rede dos DCs e/ou Salas de Clientes	IF contratualizadas
Remotos (*)	Acesso VPN à ptNet	Acesso VPN à ptNet e redes técnicas	Acesso VPN à ptNet e redes técnicas	Acesso VPN a aplicações ou IF contratualizada	Acessos VPN a aplicações ou IF contratualizada

(*) Os acessos remotos podem ser iniciados a partir da Rede Interna (ptNet), Rede técnica, ou da Internet

Controlos automáticos e reavaliação de ACESSOS

		COLABORADORES			CLIENTES	PARCEIROS (externos)
		INTERNOS		OUTSOURCERS		
		Normais	Técnicos			
Expiração/bloqueio automáticos	Bloquear Utilizadores “adormecidos”	60 dias (de inactividade)	60 dias (de inactividade)	60 dias ou conforme período de serviços contratado	60 dias ou conforme período de serviços contratado	60 dias ou conforme período de serviços contratado
	Eliminar Utilizadores "adormecidos", a menos que impacte na rastreabilidade	1 ano (de inactividade)	1 ano (de inactividade)	1 ano ou conforme período de serviços contratado	1 ano ou conforme período de serviços contratado	1 ano ou conforme período de serviços contratado
Reavaliação periódica	Reavaliação de contas admin	Trimestral	Trimestral	Trimestral ou conforme período de serviços contratado	Trimestral ou conforme período de serviços contratado	Trimestral ou conforme período de serviços contratado
	Reconciliar acessos a sistemas e aplicações críticas	Anual	Anual	Anual ou conforme período de serviços contratado	Anual ou conforme período de serviços contratado	Anual ou conforme período de serviços contratado