CitNOW

Política de segurança informática e dos dados

Última atualização:
17 de setembro de 2017

www.**citnow**.com

Versão Portuguesa

Sistema(s) empresarial(ais) da CitNOW: Todas
Referências: ISO/IEC 27001 e 27002

Índice

Anexo

1. Política de segurança da informação

1.1 Descrição geral

As informações são um recurso fundamental na nossa organização. As informações que armazenamos incluem: nomes, endereço de e-mail, número de telemóvel e matrícula do veículo do cliente; informações do eVHC do cliente; dados administrativos, pessoais e financeiros; rede de computadores e sistemas de base de dados; código e scripts informáticos. Independentemente do modo como as informações são recolhidas, acedidas ou utilizadas, garantiremos que estão protegidas através de medidas de segurança adequadas, permitindo-nos cumprir os nossos objetivos comerciais, as legislações aplicáveis e as nossas obrigações contratuais.

1.2 Objetivo

O nosso objetivo de segurança consiste em proteger a nossa organização contra problemas de segurança como, por exemplo: acesso não autorizado aos sistemas, violação da confidencialidade (pessoas que obtêm ou divulgam as informações de forma inadequada), integridade (informações alteradas ou erroneamente validadas, quer de modo deliberado ou acidental) e disponibilidade (informações não disponíveis quando são necessárias) ou qualquer outra questão que possa afetar de modo negativo as nossas atividades comerciais ou as atividades comerciais dos nossos clientes e fornecedores.

1.3 Âmbito de aplicação

A presente política abrange todos os computadores, servidores e software utilizados por nós.

1.4 Política

1.4.1 Abordagem

Iremos:

Aplicar todas as medidas de segurança razoáveis, adequadas, práticas e eficazes para proteger os nossos processos e recursos, com vista a alcançar o nosso objetivo de segurança.

Utilizar um ISMS, de acordo com a ISO/IEC 27001, como um enquadramento destinado a orientar a nossa abordagem à gestão da segurança.

Analisar continuamente a nossa utilização das medidas de segurança, para que possamos melhorar o modo como protegemos o nosso negócio.

Proteger e gerir os nossos recursos de informação para que possamos cumprir as nossas responsabilidades contratuais, legislativas e de privacidade.

1.4.2 Responsabilidades

Todos os nossos funcionários, antigos e atuais, permanentes e temporários, agirão sempre de modo responsável, profissional e consciente da segurança, mantendo o reconhecimento e o cumprimento da presente Política.

Todos os funcionários respeitarão os recursos de informação de terceiros, quer tal proteção seja ou não exigida contratual ou juridicamente.

Todos os funcionários com responsabilidade de supervisão são obrigados a promover de modo ativo as melhores práticas entre o respetivo pessoal supervisionado.

O nosso CISO, diretamente subordinado ao nosso CEO, é responsável por garantir que as informações na nossa organização estão adequadamente protegidas e o nosso objetivo de segurança é alcançado. O CISO e o Painel de segurança são autorizados pelo CEO a exercer atividades e ações adequadas que contribuam para alcançar o nosso objetivo de segurança e sejam consistentes com a presente Política de segurança da informação.

O CISO pode, periodicamente, delegar determinadas atividades a indivíduos responsáveis; além disso, é responsável por atribuir recursos suficientes para que possamos alcançar o nosso objetivo de segurança.

1.4.3 Práticas

Identificaremos os nossos riscos de segurança e respetivas prioridades relativas, respondendo aos mesmos de imediato e implementando proteções adequadas, eficazes e práticas.

Todas as informações (incluindo informações de terceiros e dados pessoais) serão protegidas por controlos de segurança e procedimentos de tratamento adequados à respetiva sensibilidade e criticidade.

Nos casos autorizados para tal, as informações serão disponibilizadas fora da nossa organização a terceiros. Os proprietários das informações serão responsáveis por identificar as pessoas a quem as suas informações podem ser divulgadas e manterão registos completos e precisos de tal divulgação.

Garantiremos que as nossas atividades podem prosseguir com uma interferência mínima ou outro impacto negativo no caso de ocorrência de qualquer forma de interferência ou incidente de segurança.

Os incidentes de segurança efetivos ou suspeitos serão imediatamente comunicados ao Painel de segurança, que gerirá o incidente e tomará medidas para uma análise do incidente e lições consequentes a serem aprendidas. Os incidentes de segurança relacionados com dados pessoais deverão ser geridos em conformidade com a Lei de privacidade aplicável.

Os procedimentos e as normas documentados, em conjunto com educação e formação, apoiarão a presente Política.

A conformidade com a Política será regularmente monitorizada pelo Painel de segurança, que se reunirá com regularidade.

O nosso CISO permitirá uma revisão anual da presente Política pelo Painel de segurança. A Política será revista em relação à integridade, à eficácia e à utilidade. A eficácia será avaliada pela nossa capacidade de evitar incidentes de segurança e de minimizar os impactos resultantes.

O nosso CISO aprovará todas as novas versões da Política de segurança da informação. Todos os nossos funcionários são responsáveis por identificar formas de melhorar a Política de segurança da informação.

As sugestões relativas à melhoria devem ser enviadas ao Painel de segurança. No caso de serem necessárias alterações imediatas, será convocada uma reunião extraordinária do Painel de segurança; caso contrário, as sugestões serão abordadas na reunião para a revisão anual da Política.

1.4.4 Reconhecimento da política

Será disponibilizada uma cópia da presente Política a todos os funcionários atuais ou aquando da respetiva entrada para a nossa organização. Secções individuais da Política serão atualizadas conforme necessário e disponibilizadas no Podio, o nosso site da intranet. Todos os nossos funcionários devem estar familiarizados e respeitar a Política de segurança da informação em todos os momentos. Os membros do Painel de segurança serão responsáveis, em primeira instância, pela interpretação e pela clarificação da Política de segurança da informação. Os funcionários que necessitem de informações adicionais relativas a qualquer aspeto da presente Política devem abordar as respetivas necessidades junto de um membro do Painel de segurança.

1.4.5 Aplicabilidade e execução

A presente Política aplica-se a todos os nossos funcionários e indivíduos que utilizem as respetivas instalações e informações. A conformidade com a Política fará parte do contrato de trabalho e todos os funcionários serão responsáveis pelas suas ações relacionadas com a segurança da informação.

O incumprimento da Política de segurança da informação poderá prejudicar a nossa capacidade de alcançar os nossos fins e os objetivos de segurança, bem como poderá prejudicar a reputação profissional da organização. O incumprimento, como sanção última, será tratado como uma questão disciplinar. O nosso CISO será responsável por todas as decisões relativas à execução da presente política, utilizando os procedimentos disciplinares à sua disposição conforme adequado.

Incentivaremos a adoção e a aplicação da presente Política de segurança da informação por terceiros que cooperem em negócios conjuntos.

2. Política de segurança de servidores

2.1 Descrição geral

Os servidores não protegidos e vulneráveis continuam a ser o principal ponto de entrada de intervenientes de ameaças mal-intencionados. As políticas de instalação de servidores consistentes, a propriedade e a gestão da configuração constituem aspetos básicos corretamente aplicados.

2.2 Objetivo

O objetivo da presente política é estabelecer normas para a configuração básica do equipamento de servidor interno que seja propriedade e/ou utilizado pela nossa organização. A implementação eficiente da presente política minimizará o acesso não autorizado às nossas informações e tecnologia proprietárias.

2.3 Âmbito de aplicação

Todos os funcionários, contratantes, consultores, colaboradores temporários e outros trabalhadores da nossa organização e das nossas subsidiárias têm de cumprir a presente política. A presente política aplica-se a equipamento de servidor que é propriedade, utilizado ou arrendado por nós ou se encontra registado no domínio de rede interna que é propriedade nossa.

2.4 Política

2.4.1 Requisitos gerais

Todos os servidores instalados na nossa organização devem ser propriedade de um grupo operacional que seja responsável pela administração do sistema. Quaisquer servidores que tratem de dados de clientes devem ser propriedade do grupo de DevOps. Devem ser estabelecidas e mantidas orientações de configuração aprovada dos servidores por cada grupo operacional com base nas necessidades comerciais e aprovadas pelo Painel de segurança. Os grupos operacionais deverão monitorizar a conformidade da configuração e implementar uma política de exceção adaptada ao respetivo ambiente. Cada grupo operacional deve estabelecer um processo para alteração das orientações de configuração, incluindo a análise e a aprovação pelo Painel de segurança. Os seguintes pontos devem ser satisfeitos:

- Todos os servidores devem estar registados junto do DevOps. No mínimo, as seguintes informações são necessárias para identificar positivamente o ponto de contacto:
- Contacto(s) e localização do servidor e contacto de reserva
- Versão/sistema operativo e hardware
- Principais funções e aplicações, se aplicável
- As informações fornecidas ao DevOps devem ser mantidas atualizadas
- As alterações de configuração para servidores de produção devem seguir os procedimentos de gestão de alterações adequados

Para efeitos de segurança, conformidade e manutenção, o pessoal autorizado poderá monitorizar e examinar o equipamento, os sistemas, os processos e o tráfego da rede.

2.4.2 Requisitos de configuração

A configuração do Sistema operativo deverá ser efetuada de acordo com as orientações aprovadas pelo Painel de segurança.

Os serviços e as aplicações que não serão utilizados devem ser desativados sempre que possível.

O acesso aos serviços deverá ser registado e/ou protegido através de métodos de controlo de acesso como, por exemplo, uma firewall de aplicação Web, se possível.

As correções de segurança mais recentes devem ser instaladas no sistema logo que possível, à exceção dos casos em que a aplicação imediata possa interferir com os requisitos comerciais.

As relações de confiança entre sistemas constituem um risco de segurança e a respetiva utilização deverá ser evitada. Não utilize uma relação de confiança quando outro método de comunicação for suficiente.

Utilize sempre princípios de segurança padrão com, no mínimo, o acesso exigido para executar uma tarefa. Não utilize uma raiz quando for suficiente uma conta não privilegiada.

Caso esteja disponível uma metodologia para uma ligação de canal seguro (ou seja, tecnicamente viável), o acesso privilegiado deve ser executado através de canais seguros (por exemplo, ligações de rede encriptadas através de SSH ou IPsec).

Os servidores deverão estar fisicamente localizados num ambiente de acesso controlado.

É especificamente proibida a utilização de servidores nos nossos escritórios.

2.4.3 Monitorização

Todos os eventos relacionados com a segurança em sistemas críticos ou sensíveis devem ser registados e os registos de auditoria devem ser guardados do seguinte modo:

- Todos os registos relacionados com a segurança serão conservados online no servidor durante uma semana, no mínimo.
- Em seguida, os registos deverão ser configurados para transferência para o servidor de registos global para arquivo e armazenamento.

Os eventos relacionados com a segurança serão comunicados ao Painel de segurança, que analisará os registos e os incidentes. As medidas corretivas serão determinadas conforme necessário. Os eventos relacionados com a segurança incluem, entre outros:

- Ataques de procura de portas abertas
- Prova de acesso não autorizado a contas privilegiadas
- Ocorrências anómalas não relacionadas com aplicações específicas do sistema anfitrião

2.5 Conformidade com a política

2.5.1 Avaliação da conformidade

O Painel de segurança verificará a conformidade com a presente política através de vários métodos, incluindo inspeções periódicas, relatórios da ferramenta de negócio, auditorias internas e externas e feeback ao proprietário da política, entre outros.

2.5.2 Exceções
Qualquer exceção à política deve ser previamente aprovada pelo Painel de segurança.

2.5.3 Incumprimento
Um funcionário que tenha, comprovadamente, violado a presente política poderá estar sujeito a uma ação disciplinar, incluindo a cessação da relação laboral.

3. Política de controlo e eliminação de recursos de TI

3.1 Descrição geral
Todos os funcionários e membros do pessoal com acesso a sistemas informáticos da organização devem cumprir a política de controlo de recursos de TI definida a seguir, de modo a proteger a segurança da rede, a integridade dos dados, bem como os sistemas informáticos de controlo e os recursos da organização. A política de controlo de recursos não só permitirá a monitorização da localização dos recursos da organização e do respetivo utilizador, mas também protegerá quaisquer dados armazenados nesses recursos. Além disso, a presente política de recursos abrange a eliminação de recursos.

Os recursos de TI não deverão ser confundidos nem monitorizados em conjunto com outros recursos da organização como o mobiliário, por exemplo. Um dos principais motivos para monitorizar os recursos de TI, além do controlo e da monitorização do recurso, é a segurança informática. Uma política especial de monitorização de recursos de TI permitirá à organização tomar medidas para proteger os recursos ligados em rede e os dados.

A presente política definirá as medidas a serem tomadas quando um recurso é movido de um edifício para outro ou de uma localização para outra. Além disso, estipulará uma base de dados de monitorização de recursos a ser atualizada para que a localização de todos os equipamentos informáticos seja conhecida.

A presente política ajudará os administradores de rede a proteger a mesma, uma vez que terão conhecimento do utilizador e do computador que se encontram em cada estação no caso de um worm infetar a rede. Além disso, esta política abrange a possibilidade de os dados num computador a serem movidos entre instalações seguras poderem ser dados sensíveis e terem de ser encriptados durante a transferência.

3.2 Objetivo e responsabilidade

A presente política destina-se a proteger os recursos da organização na rede através do estabelecimento de uma política e de um procedimento para o controlo de recursos. Estas políticas ajudarão a impedir a perda de dados ou de recursos da organização, bem como reduzirão o risco de perda de dados devido a um planeamento deficiente.

O CTO é responsável, em última instância, pelo desenvolvimento, pela implementação e pela execução da presente política.

3.3 Monitorização de recursos

Esta secção define os recursos de TI que devem ser monitorizados e em que medida deve ocorrer tal monitorização.

3.4 Tipos de recursos de TI

Esta secção classifica os tipos de recursos sujeitos a monitorização.

1. Estações de trabalho de secretária
2. Computadores portáteis
3. Telemóveis e tablets
4. Impressoras, fotocopiadoras, telecopiadoras e equipamentos multifunções
5. Dispositivos de mão
6. Scanners
7. Servidores
8. Firewalls
9. Routers
10. Comutadores
11. Dispositivos de memória

3.4.1 Monitorização de recursos

Os recursos com um custo inferior a £ 100 não serão especificamente monitorizados, incluindo os componentes informáticos, tais como placas gráficas ou placas de som. No entanto, os recursos com dados armazenados, independentemente do custo, serão monitorizados. Esses recursos incluem:

1. Discos rígidos
2. Unidades de armazenamento temporário
3. Bandas com dados armazenados, incluindo dados de cópias de segurança do sistema
4. Apesar de não serem especificamente monitorizados, outros dispositivos de armazenamento, incluindo discos CD-ROM e disquetes, encontram-se abrangidos pela presente política para efeitos de eliminação e de armazenamento Seguro.

3.4.2 Dispositivos com pouca memória

Os recursos de armazenamento com pouca memória não serão monitorizados por localização, porém, por administrador. Esses recursos incluem:

1. Disquetes
2. Discos CD-ROM
3. Cartões de memória

Caso estes tipos de dispositivos sejam permitidos para alguns funcionários, o administrador do dispositivo deve inscrever-se para a receção desses dispositivos na posse daqueles. Além disso, todos os funcionários devem concordar em tratar os cartões de memória, as disquetes e os discos CD-ROM de forma responsável e em respeitar estas orientações:

1. Nunca guardar dados sensíveis nos dispositivos sem autorização. Caso sejam guardados dados sensíveis nos mesmos, deve ser obtida uma permissão especial e o dispositivo de memória deve ser guardado num local seguro.
2. Nunca guardar dados dos clientes nos dispositivos.

3. Nunca utilizar esses dispositivos para trazer programas executáveis externos à rede sem autorização e sem efetuar, em primeiro lugar, uma análise do programa com um programa antivírus e um verificador de software maligno aprovados e atualizados. Qualquer programa trazido para a rede será previamente abordado com o departamento de TI para autorização.

Consulte a Política de suportes de dados amovíveis para obter mais informações.

3.5 Requisitos da monitorização de recursos

1. Todos os recursos devem ter um número de ID. Será atribuído um número de monitorização interno aquando da aquisição do recurso ou a utilização dos números de ID do Fabricante deve ser especificada na presente política.
2. Será criada uma base de dados de monitorização de recursos para monitorizar os recursos. Aquela incluirá todas as informações relativas à tabela da Lista de verificação da transferência de recursos e a data da mudança dos recursos.
3. Após a aquisição de um recurso, será atribuído um ID ao recurso e a respetiva informação deverá ser introduzida na base de dados de monitorização de recursos.

3.6 Procedimento de transferência

3.6.1 Lista de verificação da transferência de recursos

Quando um tipo de recurso indicado na lista de Tipos de recursos é transferido para uma nova localização ou um novo administrador, a Lista de verificação da transferência de recursos de TI deve ser preenchida pelo administrador do recurso e aprovada por um representante da organização autorizado. O administrador é a pessoa ao cuidado da qual se encontra o recurso. Caso este seja uma estação de trabalho, o administrador é o utilizador mais comum da mesma. No que diz respeito a outros equipamentos, o administrador é a principal pessoa responsável pela manutenção ou supervisão do equipamento.

O administrador deve preencher o formulário da Lista de verificação da transferência de recursos e indicar se o recurso é um novo recurso, será movido para uma nova localização ou um novo administrador ou será eliminado. As seguintes informações devem ser preenchidas:

1. Tipo de recurso
2. Número de ID
3. Nome do recurso
4. Localização atual
5. Administrador designado
6. Nova localização
7. Novo administrador
8. Localizações dos dados sensíveis

Após o administrador preencher e assinar o formulário da Lista de verificação da transferência de recursos, este deve ser assinado por um representante autorizado.

3.6.2 Introdução de dados

Após o preenchimento da Lista de verificação da transferência de recursos, esta será dada ao gestor da base de dados de monitorização de recursos. O gestor da base de dados de monitorização de recursos garantirá que as informações dos formulários são introduzidas na base de dados de monitorização de recursos no prazo de uma semana.

3.6.3 Verificação da base de dados

Os gestores responsáveis pela gestão de projetos que afetem a localização de equipamento deverão verificar, com periodicidade, se os recursos recentemente movidos foram adicionados à base de dados. A base de dados deverá fornecer uma lista de transferências recentes que possa ser facilmente verificada. Os gestores deverão verificar a base de dados semanalmente para garantir que os recursos transferidos nas últimas duas ou três semanas estão incluídos na mesma.

3.7 Transferências de recursos

A presente política aplica-se a quaisquer transferências de recursos, incluindo o seguinte:

1. Aquisição de recursos
2. Realocação de recursos
3. Alteração do administrador do recurso, incluindo a saída ou a substituição de um funcionário
4. Eliminação de recursos, incluindo:
5. Devolução de recursos ao fabricante ou revendedor devido a uma devolução na garantia
6. Devolução de um recurso arrendado ao proprietário

Em todos estes casos, a lista de verificação da transferência de recursos tem de ser preenchida.

3.8 Limpeza da memória dos suportes de dados

Na transferência de recursos para outro administrador, quaisquer informações confidenciais no dispositivo devem ser protegidas e/ou destruídas. O método de destruição dos dados depende da sensibilidade dos dados no dispositivo e do próximo utilizador do dispositivo (dentro da organização e respetivos controlos ou fora da organização).

3.9 Eliminação de recursos

A eliminação de recursos constitui um caso especial, uma vez que devem ser removidos quaisquer dados sensíveis do recurso durante ou antes da eliminação. O gestor do utilizador do recurso deve determinar o nível de sensibilidade máxima dos dados armazenados no dispositivo. A seguir é indicada a medida para o dispositivo com base na sensibilidade dos dados, de acordo com o procedimento de avaliação dos dados.

1. Nenhuma (dados não classificados) – Nenhum requisito para eliminar os dados, porém, no interesse da prudência, eliminar normalmente os dados através de quaisquer meios, tais como limpeza da memória, destruição física ou desmagnetização.
2. Baixa (dados sensíveis) – Eliminar os dados através de quaisquer meios tais como limpeza eletrónica da memória, destruição física ou desmagnetização.
3. Média (dados confidenciais) – Os dados devem ser eliminados através de uma tecnologia aprovada para garantir que não são legíveis utilizando técnicas especiais de alta tecnologia.

4. Alta (dados secretos) – Os dados devem ser eliminados através de uma tecnologia aprovada para garantir que não são legíveis utilizando técnicas especiais de alta tecnologia. As tecnologias aprovadas encontram-se especificadas num documento relativo ao Procedimento de eliminação de dados em suportes de dados por tipo de recurso, incluindo::

    1. Disquete
    2. Cartão de memória
    3. Disco CD-ROM
    4. Banda de armazenamento
    5. Disco rígido
    6. Memória RAM
    7. Memória ROM ou dispositivos de memória ROM

3.10 Utilização de suportes de dados

A presente política define os tipos de dados que podem ser armazenados em suportes de dados amovíveis, bem como se tais suportes de dados podem ser removidos de uma instalação fisicamente segura e em que condições tal será permitido. Os suportes de dados amovíveis incluem:

1. Disquete
2. Disco de memória
3. Disco CD-ROM
4. Banda de armazenamento

A seguir é indicada a política para o dispositivo com base na classificação da sensibilidade dos dados armazenados no dispositivo, de acordo com o procedimento de avaliação dos dados.

1. Dados não classificados – Os dados podem ser removidos com a aprovação do gestor de primeiro nível, sendo a permissão perpétua ao longo da relação laboral com o funcionário, salvo no caso de revogação. O dispositivo pode ser enviado para outros escritórios através de qualquer correio público ou privado.
2. Dados sensíveis – Os dados apenas podem ser removidos de áreas seguras com a permissão de um diretor ou de um gestor de nível superior e as aprovações são válidas para uma única vez.
3. Dados confidenciais – Os dados apenas podem ser removidos de áreas seguras com a permissão de um vice-presidente ou de um gestor de nível superior. Devem existir algumas precauções de segurança documentadas para o método de transporte e no destino.
4. Dados secretos – Os dados apenas podem ser removidos de áreas seguras com a permissão de um presidente ou de um gestor de nível superior. Devem existir algumas precauções de segurança documentadas para o método de transporte e no destino.
5. Dados muito secretos – Os dados nunca podem ser removidos de áreas seguras.

3.11 Dispositivos propriedade dos funcionários

A presente política define os tipos de dispositivos propriedade dos funcionários que podem ser utilizados pelos funcionários nas instalações da empresa.

1. Os telemóveis pessoais podem ser utilizados nas instalações, porém, não devem ser ligados por Wi-Fi à rede da empresa.
2. Não é permitida a utilização de outros dispositivos propriedade dos funcionários nas instalações da empresa nem devem ser ligados à rede com fios ou Wi-Fi da empresa.

3.12 Execução

Uma vez que a segurança e a integridade dos dados, em conjunto com a proteção dos recursos, são fundamentais para o funcionamento da organização, os funcionários que não cumpram a presente política poderão estar sujeitos a uma ação disciplinar, incluindo o despedimento. Qualquer funcionário com conhecimento de qualquer violação da presente política deve comunicar a mesma ao respetivo supervisor ou a outro representante autorizado.

3.13 Formação de funcionários e reconhecimento da política

ada funcionário da organização deve ter conhecimento das políticas e dos procedimentos em vigor relacionados com a Segurança informática, bem como deve receber formação relativa a essas políticas e procedimentos, no mínimo, anualmente. Os funcionários devem assinar uma declaração de reconhecimento de que têm conhecimento da política e cumprirão os respetivos requisitos.

4. Política de suportes de dados amovíveis

4.1 Descrição geral

Os suportes de dados amovíveis são uma fonte conhecida de infeções por software maligno e estão diretamente associados à perda de informações sensíveis em muitas organizações.

4.2 Objetivo

O objetivo da presente política é minimizar o risco de perda ou exposição das informações sensíveis que conservamos, bem como reduzir o risco de infeções por software maligno nos computadores que utilizamos.

4.3 Âmbito de aplicação

A presente política abrange todos os computadores e servidores utilizados na nossa organização.

4.4 Política

Os nossos funcionários apenas podem utilizar suportes de dados amovíveis nos computadores de trabalho que sejam propriedade nossa. Os nossos suportes de dados amovíveis não podem ser ligados ou utilizados em computadores que não sejam propriedade nossa ou arrendados por nós sem permissão explícita do nosso Painel de segurança.

As informações sensíveis apenas deverão ser armazenadas em suportes de dados amovíveis sempre que tal seja necessário para o exercício das suas funções ou na prestação de informações exigida por outras agências estatais ou federais. Os dados de clientes nunca devem ser armazenados em suportes de dados amovíveis.

Poderão ser solicitadas, caso a caso, exceções à presente política, as quais apenas podem ser aprovadas pelo Painel de segurança.

4.5 Conformidade com a política

4.5.1 Gestão de conformidade

O Painel de segurança verificará a conformidade com a presente política através de vários métodos, incluindo inspeções periódicas, relatórios da ferramenta de negócio, auditorias internas e externas e feeback ao proprietário da política, entre outros.

4.5.2 Exceções

Qualquer exceção à política deve ser previamente aprovada pelo Painel de segurança.

4.5.3 Incumprimento

Um funcionário que tenha, comprovadamente, violado a presente política poderá estar sujeito a uma ação disciplinar, incluindo a cessação da relação laboral.

5. Política de vírus e códigos maliciosos

5.1 Descrição geral

A presente política e procedimento abrangem a nossa Política de vírus e códigos maliciosos.

5.2 Objetivo

O objetivo da presente política é explicar a abordagem que deverá ser adotada na nossa organização para impedir vírus e código malicioso, bem como as medidas a tomar no caso de uma infeção.

5.3 Âmbito de aplicação

A presente política abrange todos os computadores e servidores utilizados na nossa organização.

5.4 Política

Uma vez que os atacantes estão, atualmente, a passar de ataques que são um incómodo ou uma destruição para uma atividade motivada por um ganho financeiro, os ataques por código malicioso tornaram-se sofisticados e uma preocupação considerável para as organizações. Um ataque por código malicioso de grande escala, frequentemente referido como um surto de código malicioso, pode causar uma interferência e prejuízos generalizados a uma organização, bem como exigir um tempo e um esforço de recuperação prolongados. Por conseguinte, é fundamental implementar medidas preventivas adequadas, tais como a implementação de ferramentas de proteção e deteção, para proteger uma organização contra ataques por código malicioso.

No entanto, não existe uma proteção completamente impenetrável no mundo da segurança da informação. Além disso, é importante que a organização desenvolva um procedimento sólido de incidentes de segurança da informação para que o pessoal esteja melhor preparado para lidar com surtos de código malicioso de forma mais organizada, eficiente e eficaz.

Um procedimento de resposta a incidentes deverá ser composto por três fases principais: “Planeamento e preparação”, “Resposta” e “Resultado”. Esta secção define os passos das fases “Resposta” e “Resultado”, importantes para gerir na íntegra um surto de código malicioso. Para obter mais informações acerca da fase “Planeamento e preparação”, consulte a secção da política “Gestão de incidentes de segurança para empresas”.

A fase de "Resposta" é composta pelos cinco passos a seguir:

- Deteção e identificação
- Encaminhamento
- Contenção
- Erradicação
- Recuperação

5.4.1 Deteção e identificação

5.4.1.1 Determinação com exatidão da ocorrência de um surto de código malicioso

O objetivo deste passo é determinar se ocorreu um surto de código malicioso. Os sinais típicos de um surto de código malicioso incluem uma ou todas as afirmações a seguir:

- Os utilizadores queixam-se de acesso lento à Internet, esgotamento dos recursos do sistema, acesso lento ao disco ou arranque lento do sistema.
- Foram gerados vários alertas pelo Sistema de deteção de intrusões baseado num anfitrião (HIDS) ou pelo programa antivírus ou de deteção de código malicioso.
- Existe um aumento significativo da utilização da rede.
- Foram detetadas várias entradas de violação de acesso nos registos do router ou nos registos da firewall de perímetro.
- Foi detetado um pico de tráfego SMTP de devolução externa com origem num endereço IP interno.
- Foi detetado um grande número de procura de portas abertas e de tentativas de falha na ligação.
- O administrador do sistema observa um desvio anormal nos fluxos típicos do tráfego de rede.
- Os controlos de segurança, tais como o programa antivírus e as firewalls pessoais, foram desativados em muitos sistemas anfitriões.

- Existe uma instabilidade geral do sistema e este falha.

Após a deteção de qualquer um dos sintomas acima indicados, os membros do pessoal de TI deverão verificar e validar imediatamente todas as atividades suspeitas para determinar se ocorreu um surto. Após a confirmação da ocorrência de uma falha na segurança por código malicioso, é importante recolher informações acerca do código malicioso, uma vez que tal será fundamental para o procedimento de contenção e de erradicação.

As informações acerca do código malicioso podem ser obtidas nos websites dos fabricantes de programas antivírus, caso o código malicioso exista há algum tempo, através da análise dos alertas do programa antivírus e de deteção de código malicioso e da análise dos ficheiros de registo da firewall e do router. As questões a seguir podem ajudar a identificar as características do código malicioso:

- De que tipo de código malicioso se trata (worm de rede, worm de e-mail em massa, vírus ou trojan, etc.)?
- Como ocorre a propagação do código malicioso (através de ataque a um serviço de rede vulnerável? Através do envio de e-mails em massa?
- Se a propagação do código malicioso ocorrer através do ataque a um serviço vulnerável, qual a vulnerabilidade que está a ser explorada? Foi lançada uma correção para combater a vulnerabilidade? Quais são os serviços ou as portas alvo do ataque?
- O código malicioso introduz backdoors no sistema infetado?
- De que modo o código malicioso pode ser removido do sistema infetado? Estão disponíveis ferramentas de remoção?

5.4.1.2 Realização de avaliações preliminares

Após a identificação do surto, os membros do pessoal de TI devem avaliar o respetivo âmbito, os danos e o impacto para gerir eficientemente o surto.

5.4.1.3 Registo de todas as medidas tomadas

Os membros do pessoal de TI devem registar todas as medidas tomadas para gerir o surto e quaisquer resultados correspondentes. Tal pode facilitar a identificação e a avaliação de incidentes, bem como fornecer provas para uma ação judicial ou outra informação útil para fases de gestão de incidentes seguintes. O registo deverá ser realizado ao longo de todo o procedimento de resposta a incidentes de segurança.

5.4.1.4 Contenção

A terceira medida da resposta a um incidente por código malicioso é a contenção. A seguir são indicadas as atividades a serem realizadas na fase de contenção:

5.4.1.5 Identificação de sistemas infetados

A identificação clara dos sistemas infetados é sempre o primeiro passo da contenção. Infelizmente, trata-se de um procedimento muito complicado devido à natureza dinâmica do atual ambiente informático. A seguir são apresentadas algumas sugestões que podem ajudar a identificar os sistemas infetados num ambiente controlado:

- Realizar uma análise de vírus completa em todos os sistemas com as assinaturas de vírus mais recentes e sistemas de deteção e reparação de vírus atualizados. Uma vez que nenhum programa antivírus ou ferramenta de deteção de código malicioso pode, por si só, detetar todos os tipos de código malicioso, poderá ser necessário utilizar mais do que uma ferramenta de análise de vírus para garantir que todos os códigos maliciosos são detetados
- Analisar todos os ficheiros de registo dos routers e das firewalls
- Fornecer instruções aos utilizadores sobre como identificar infeções
- Configurar os IPS ou IDS para identificarem atividades associadas a infeções
- Realizar rotinas de análise para a procura de tráfego de rede correspondente às características do código malicioso

5.4.1.6 Contenção do surto

A contenção do surto pode ser efetuada de várias formas; a seguir são apresentadas as táticas comuns:

- Através da utilização de ferramentas automáticas
  A contenção da propagação de código malicioso pode ser efetuada através de ferramentas automáticas, tais como programas antivírus ou ferramentas de deteção de código malicioso, IDS e IPS. Caso o código malicioso não seja detetado pelos sistemas de proteção antivírus existentes, incluindo com a assinatura mais recente aplicada, deverá ser solicitado o apoio dos fabricantes de programas antivírus para a criação de uma nova assinatura que abranja o código malicioso.

- Através da desativação da conectividade
  Um surto de código malicioso pode ser eficientemente contido através da desativação rápida dos sistemas infetados da infraestrutura de rede global, o que pode ser alcançado ao aplicar controlos de acesso em dispositivos de rede ou ao desligar fisicamente cabos de rede. Em alguns casos, para conter a propagação de código malicioso a outras secções da organização, poderá ser necessário desligar temporariamente da rede básica os segmentos de rede em causa. No entanto, esta estratégia de contenção afetará, certamente, o funcionamento de outros sistemas não infetados no segmento.
- Através da desativação de serviços
  O código malicioso poderá propagar-se através dos serviços da rede, por exemplo, unidades partilhadas da rede. O bloqueio temporário ou até mesmo a desativação dos serviços da rede utilizados pelos códigos maliciosos ajuda a conter os incidentes.
- Através da eliminação da vulnerabilidade
  O código malicioso poderá propagar-se através do ataque a serviços da rede vulneráveis. Ao abordar as vulnerabilidades que foram exploradas pelo código malicioso, tais como ao aplicar correções de segurança em sistemas vulneráveis, os canais de propagação podem ser eliminados, contendo, deste modo, a propagação. Além disso, algumas configurações incorretas, tais como a perda de controlos de acesso em unidades partilhadas da rede, podem ser aproveitadas pelo código malicioso. Ao reparar quaisquer configurações incorretas, é possível contar a propagação de um código malicioso.

- Através da participação dos utilizadores
  A participação dos utilizadores é importante para o procedimento de contenção num ambiente em que apenas está disponível um número limitado de membros do pessoal do suporte técnico para gerir um surto, por exemplo, em pequenas sucursais remotas ou num ambiente de escritório não controlado. Os utilizadores deverão obter instruções claras sobre o modo de identificação de infeções e as medidas a serem tomadas em caso de confirmação de infeção de um sistema, tais como a execução de ferramentas de remoção de vírus no sistema infetado.

5.4.1.7 Manutenção de registos de todas as medidas tomadas

É importante manter um registo sólido de todas as medidas tomadas nesta fase, pois algumas medidas de contenção poderão exigir modificações temporárias da configuração ou das definições da infraestrutura e dos sistemas da rede. Essas modificações terão de ser eliminadas após o incidente.

É importante compreender que deter novas infeções pelo código malicioso não impede, necessariamente, danos adicionais nos sistemas infetados. Por exemplo, a infeção pode ser contida através da desativação da conectividade da rede. Contudo, o código malicioso poderá ainda estar a eliminar ativamente ficheiros do sistema infetado.

Por conseguinte, um procedimento de erradicação completa deverá ser executado logo que possível ou em paralelo com o procedimento de contenção.

5.4.2 Erradicação

A erradicação de um surto de código malicioso deverá visar a eliminação do código malicioso de todos os sistemas e suportes de dados infetados, bem como a reparação da causa da infeção. Antes de executar o procedimento de erradicação, recomenda-se a recolha de todas as informações necessárias, incluindo todos os ficheiros de registo, que possam ter de ser eliminadas ou repostas durante o procedimento de limpeza e serão úteis para investigações subsequentes.

As ferramentas de remoção e o programa antivírus ou de análise de código malicioso são normalmente utilizados como o principal meio de erradicação.

Todavia, em alguns casos, poderá ser necessário reconstruir do zero os sistemas infetados. Por exemplo, se o código malicioso tiver sido transferido e introduzido num backdoor dos sistemas infetados, a reconstrução de todos os sistemas poderá ser a medida mais fiável a tomar para restaurar a integridade dos sistemas. A reconstrução de um sistema inclui, em geral, as seguintes medidas:

- Reinstalação do sistema a partir de uma fonte de confiança como, por exemplo, um disco de instalação do sistema ou uma imagem do sistema limpa e de confiança.
- Proteção dos sistemas recentemente instalados, tais como verificação e garantia de que as assinaturas de vírus mais recentes e os sistemas de deteção e reparação de vírus atualizados, bem como as correções de segurança necessárias, foram aplicados em cada equipamento.
- Restauro dos dados a partir de suportes de dados de cópia de segurança limpos e conhecidos.

5.4.3 Recuperação

O principal objetivo da medida de recuperação é, claramente, restaurar o funcionamento normal em todos os sistemas. Num surto de código malicioso, a recuperação do funcionamento e dos dados dos sistemas infetados poderá já ter sido efetuada como parte do procedimento de erradicação. Além do restauro dos sistemas infetados, a eliminação de quaisquer medidas de contenção temporária, por exemplo, ligações de rede suspensas, é outro aspeto principal do procedimento de recuperação.

Antes da eliminação das medidas de contenção, uma medida importante é uma avaliação do risco de segurança de pré-produção para garantir que não é detetada qualquer infeção e a causa da infeção inicial foi retificada.

Todas as partes relacionadas deverão ser notificadas antes de os serviços suspensos serem retomados. Os membros do pessoal de TI deverão restaurar funções e servidores específicos, fase por fase, de modo controlado e por ordem de pedido, por exemplo, os serviços mais essenciais ou os serviços que servem a maioria devem ser retomados em primeiro lugar. Após serem retomados os serviços suspensos, é importante verificar se a operação de restauro foi concluída com êxito e todos os serviços estão a funcionar normalmente. Poderão ser implementadas medidas de monitorização adicionais para detetar qualquer atividade suspeita nos segmentos de rede em causa.

5.4.4 Consequências

O restauro dos sistemas infetados para o funcionamento normal não assinala o fim de um surto de código malicioso. É igualmente importante executar a medida de seguimento necessária. Tal poderá incluir uma avaliação completa do dano causado, melhorias do sistema para impedir uma nova ocorrência do incidente, atualizações às políticas e procedimentos de segurança e uma investigação do caso para uma ação judicial subsequente. As atividades nesta fase podem incluir o seguinte:

- Análise da eficácia dos procedimentos e mecanismos existentes de proteção contra vírus/código malicioso, incluindo controlo e gestão central da distribuição de assinaturas de vírus e atualização dos sistemas de deteção e reparação, análise de vírus programada regular, etc.
- Atualização das políticas, das orientações e dos procedimentos relevantes sempre que necessário.
- Execução das novas medidas de segurança introduzidas na política, nas orientações ou nos procedimentos revistos para proteger os sistemas contra ataques futuros.
- Alerta dos utilizadores para cumprirem as melhores práticas de segurança, tais como não abrirem e-mails de origem desconhecida/suspeita, atualizarem as correções de segurança e as definições de vírus regularmente e sempre que necessário, etc.

6. Procedimento de gestão de incidentes

6.1 Objetivo

O objetivo da presente política é garantir uma deteção rápida de eventos e falhas de segurança, bem como reagir e responder rapidamente a incidentes de segurança.

6.2 Âmbito de aplicação e utilizadores

A presente política aplica-se a todo o âmbito de aplicação do Sistema de gestão da segurança da informação (ISMS), ou seja, a todos os funcionários e outros recursos utilizados no âmbito do ISMS, bem como a fornecedores e outros indivíduos externos à organização que entrem em contacto com os sistemas e as informações no âmbito do ISMS.

Os utilizadores da presente política são todos os nossos funcionários, bem como todas as pessoas supramencionadas.

6.3 Referência

- Norma ISO/IEC 27001, cláusulas A.7.2.3, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6 e A.16.1.7
- Norma ISO/IEC 27001, cláusulas 16.1.1, 16.1.2, 16.1.7 e 18.1.2

6.4 Política

Um incidente de segurança da informação consiste em “um único ou vários eventos de segurança da informação indesejados ou inesperados com uma grande probabilidade de comprometer as atividades comerciais e ameaçar a segurança da informação” (ISO/IEC 27000:2009).

6.4.1 Política

Um incidente de segurança da informação consiste em "um único ou vários eventos de segurança da informação indesejados ou inesperados com uma grande probabilidade de comprometer as atividades comerciais e ameaçar a segurança da informação" (ISO/IEC 27000:2009)

6.4.2 Procedimento de gestão de eventos ou falhas de segurança

A pessoa que recebeu a informação acerca de uma falha ou um evento de segurança analisa a informação, estabelece a causa e, se necessário, sugere uma medida preventiva e corretiva.

Nas situações que envolvam serviços online ou os PII do cliente, o Responsável pela segurança deve decidir se os clientes, aos quais a falha ou o evento de segurança diz respeito, devem ser informados (caso o cliente não seja o autor da comunicação inicial). Caso seja necessário informar os clientes, as notificações devem ser efetuadas, logo que possível, por telefone ou pessoalmente, de acordo com os procedimentos acordados.

6.4.3 Gestão de incidentes menores

Caso tenha sido comunicado um incidente menor, a pessoa que recebeu a informação, em coordenação com o pessoal do cliente e conforme necessário ou exigido, deve tomar as seguintes medidas:

1. Tomar medidas para conter o incidente
2. Analisar a causa do incidente
3. Tomar as medidas corretivas necessárias para eliminar a causa do incidente
4. Informar as pessoas envolvidas no incidente e o Responsável pela segurança sobre o procedimento de gestão do incidente

A pessoa que recebeu a informação acerca de um incidente menor deve registar o incidente junto do Responsável pela segurança por e-mail e referir um defeito no Jira para alertar a equipa de desenvolvimento.

6.4.4 Gestão de incidentes importantes

No caso de incidentes importantes que possam interferir nas atividades por um período de tempo inaceitável, será executado um dos procedimentos a seguir referidos:

Durante o horário de funcionamento:

1. Convocação de uma reunião de emergência com o Painel de segurança
2. Avaliação do incidente no que diz respeito à segurança e à gravidade
3. Tomada de uma decisão com base na melhor forma de atuação
4. Execução da medida
5. Logo que possível, realização de uma análise da causa do incidente, que será revista pelo Painel

Fora do horário de funcionamento:

1. Reunião dos recursos técnicos disponíveis pela primeira pessoa a ser notificada do incidente
2. Avaliação do incidente no que diz respeito à segurança e à gravidade, bem como análise do facto de uma tentativa de resolução fora do horário poder causar mais danos se os recursos adequados não estiverem disponíveis
3. Tomada de uma decisão com base na melhor forma de atuação
4. Execução de uma medida minima

5. Durante o horário de funcionamento, realização de uma avaliação mais pormenorizada com medidas adicionais, se necessário
6. Logo que possível, realização de uma análise da causa do incidente, que será revista pelo Painel

6.4.5 Aprendizagem a partir dos incidentes

O Painel de segurança deve analisar todos os incidentes menores de três em três meses e introduzir os incidentes recorrentes, ou aqueles que possam tornar-se incidentes importantes na próxima vez, no Registo de incidentes.

O Painel de segurança deve analisar cada incidente registado no Registo de incidentes (identificando o tipo, a relação e o custo do incidente) e, se necessário, sugerir uma medida preventiva ou corretiva.

6.4.6 Ações disciplinares

O Responsável pela segurança deve instaurar um processo disciplinar por cada violação das regras de segurança, em conjunto com o departamento de RH.

6.4.7 Recolha de provas

O Painel de segurança definirá as regras relativas à identificação, recolha e preservação da prova que será aceite como tal em ações judiciais e de outra natureza.

Nas situações que envolvam os PII do cliente, o Responsável pela segurança definirá, em conjunto com o cliente do serviço na nuvem, o procedimento para identificar, recolher e preservar a prova que será aceite como tal em ações judiciais e de outra natureza.

6.5 Gestão dos registos mantidos com base neste documento

Nome do registo	Localização de armazenamento	Pessoa responsável pelo armazenamento	Controlos para a proteção de registos	Período de conservação
Registo de incidentes	DropBox da empresa	Painel de segurança	Apenas os membros do painel têm o direito de editar o registo	5 anos
Regras para identificação, recolha e preservação de provas	DropBox da empresa	Responsável pela segurança	Apenas o Responsável pela segurança tem o direito de editar e publicar as regras	Os registos são armazenados durante um período de 5 anos

Apenas o Responsável pela segurança pode conceder acesso aos registos a outros funcionários.

6.6 Validade e gestão de documentos

Este documento é válido a partir de 5 de outubro de 2017.

O proprietário deste documento é o Responsável pela segurança, que deve verificar e, se necessário, atualizar o documento, no mínimo, de seis em seis meses.

Na avaliação da eficácia e da adequação do presente documento, devem ser tidos em conta os seguintes critérios:

- Número de falhas ou incidentes que não foram comunicados às pessoas autorizadas
- Número de incidentes que não foram geridos da forma mais adequada
- Número de incidentes que não foram registados no Registo de incidentes
- Número de incidentes cuja prova para uma ação judicial era inadequada
- Número de violações das regras de segurança em que não foi instaurado qualquer processo disciplinar

As versões anteriores deste procedimento devem ser armazenadas durante um período de cinco anos, salvo indicação em contrário num requisito legal ou contratual.

7. Política de cópias de segurança

7.1 Objetivo

O objetivo do presente documento é garantir que são criadas cópias de segurança em intervalos definidos e as mesmas são testadas regularmente.

7.2 Âmbito de aplicação e utilizadores

Este documento aplica-se ao âmbito completo do Sistema de gestão da segurança da informação (ISMS), ou seja, a todas as tecnologias de informação e comunicação abrangidas pelo âmbito de aplicação.

Os utilizadores do presente documento são os nossos funcionários.

7.3 Referência

- Norma ISO/IEC 27001, cláusula A.12.3.1

7.4 Política

7.4.1 Procedimento de cópia de segurança

As cópias de segurança devem ser criadas para todos os sistemas de software, dados e vídeos.

A criação de cópias de segurança é um processo automático que faz parte dos sistemas de software desenvolvidos e instalados por nós. O diretor de DevOps é responsável, em última instância, por garantir que as cópias de segurança foram efetuadas e armazenadas com êxito.

São automaticamente criados registos do procedimento de cópia de segurança nos sistemas onde a cópia de segurança é efetuada.

O software do sistema é armazenado em vários repositórios e utiliza Git, tornando possível regressar às versões anteriores como parte do sistema.

Os dados são automaticamente replicados para bases de dados secundárias de outros servidor noutros centros de dados. As cópias de segurança de binários são efetuadas de hora em hora e armazenadas no Amazon S3. As cópias de segurança noturnas são efetuadas diariamente e armazenadas no Amazon S3.

Os vídeos são duplicados no Amazon S3 assim que são processados. Aqueles permanecem no servidor primário e no S3 durante cinco dias, no mínimo. Após a respetiva eliminação do servidor primário, são armazenados apenas no S3, contudo, este está configurado para oferecer elevada redundância.

7.4.2 Testes das cópias de segurança

O repositório do sistema de software é testado diariamente pelos programadores que trabalham no mesmo.

As cópias de segurança de dados são testadas diariamente, uma vez que a cópia de segurança é restaurada num servidor de transição que age como parte do procedimento de implementação.

As cópias de segurança de vídeos são constantemente testadas, uma vez que os vídeos são reproduzidos a partir do sistema de cópia de segurança após o período inicial de cinco dias e um script de anomalias destaca quaisquer vídeos não copiados para a cópia de segurança no S3.

7.4.3 Gestão dos registos mantidos com base na presente política

O repositório do sistema de software é testado diariamente pelos programadores que trabalham no mesmo.

Nome do registo	Localização de armazenamento	Pessoa responsável pelo armazenamento	Controlos para a proteção de registos	Período de conservação
Registos do procedimento de cópia de segurança – formato eletrónico	Sistema que executa o procedimento de cópia de segurança	Diretor de DevOps	Os registos são só de leitura, não podendo ser eliminados ou editados	Os registos são armazenados durante um período de dois anos

7.4.4 Validade e gestão de documentos

Este documento é válido a partir de 5 de outubro de 2017.

O proprietário deste documento é o CTO, que deve verificar e, se necessário, atualizar o documento, no mínimo, uma vez por ano.

Na avaliação da eficácia e da adequação do presente documento, devem ser tidos em conta os seguintes critérios:

Número de testes de cópia de segurança sem êxito

As versões anteriores desta política devem ser armazenadas durante um período de cinco anos, salvo indicação em contrário num requisito legal ou contratual.

Anexo

I. Detalhes do Painel de segurança

O painel de segurança inclui, no mínimo, as seguintes funções:

- Diretor de administração responsável pelo desenvolvimento e pela segurança (CTO)
- Diretor de segurança da informação (CISO)
- Responsável pela arquitetura do software
- Diretor de DevOps
- Chefe de desenvolvimento

O painel deve reunir-se mensalmente.

O painel analisará quaisquer incidentes comunicados no mês anterior, incluindo quaisquer relatórios de controlo do incidente, e as alterações recomendadas ao sistema, às práticas, aos procedimentos ou às políticas.

O painel analisará os incidentes em relação a uma lista de clientes e, caso algum tenha sido afetado, contactará o cliente em causa através do método acordado.

II. Registo de incidentes

Os incidentes são classificados nos seguintes tipos:

- Relacionados com a informação (diretamente relacionados com a tecnologia de informação ou comunicação)
- Não relacionados com a informação (todos os outros incidentes)

Informação acerca dos incidentes:

O Registo de incidentes é um documento Google.

N.º	Data do incidente	Breve descrição (nome) do incidente	Pessoa responsável pela gestão do incidente	Descrição pormenorizada – impactos, duração, sistemas/dados afetados pelo incidente, etc.	Custos [na moeda local] – diretos e indiretos	Referência ao Formulário da medida corretiva
1						
2						
3						
4						