BASF
We create chemistry

Be Secure
Checklist de Proteção da Informação e Segurança Cibernética para Prestadores de Serviços

Guia para prestadores de serviços que trabalham na BASF

Checklist de Proteção da Informação e Segurança Cibernética

O „Checklist de Proteção da Informação e Segurança Cibernética“ é um guia para que os prestadores de serviços da BASF possam tomar precauções e implementar medidas para prevenir perda e acesso não autorizado a informações que devem ser protegidas.

A experiência demonstrou que os problemas abordados neste Checklist são elementos essenciais que desempenham um papel importante na implementação prática de proteção sempre eficaz das informações.

Este Checklist não é exclusivo. É de responsabilidade do prestador de serviço agir com responsabilidade e determinar quais medidas específicas e precauções devem ser tomadas em cada caso. Nem sempre as soluções técnicas prevalecem, as vezes é necessário o uso do bom senso.

Proteção da informação e segurança cibernética
E-mail: be-secure@basf.com
Versão: Outubro de 2019

Questões Principais

- O grupo de pessoas que irá manusear as informações sensíveis que precisam de proteção („pessoas autorizadas“) está definido?
- As pessoas autorizadas estão devidamente comprometidas a manter a confidencialidade?
- As pessoas autorizadas foram instruídas sobre proteção da informação e segurança cibernética?
- São realizadas verificações regulares para garantir que as especificações de proteção da informação estão sendo observadas adequadamente?
- O tipo e âmbito das medidas de segurança da informação implementadas estão documentados?
- Quando se manipulam dados pessoais, a Lei Geral de Proteção de Dados do seu país está sendo cumprida?
- Os padrões de software e hardware são cumpridos?

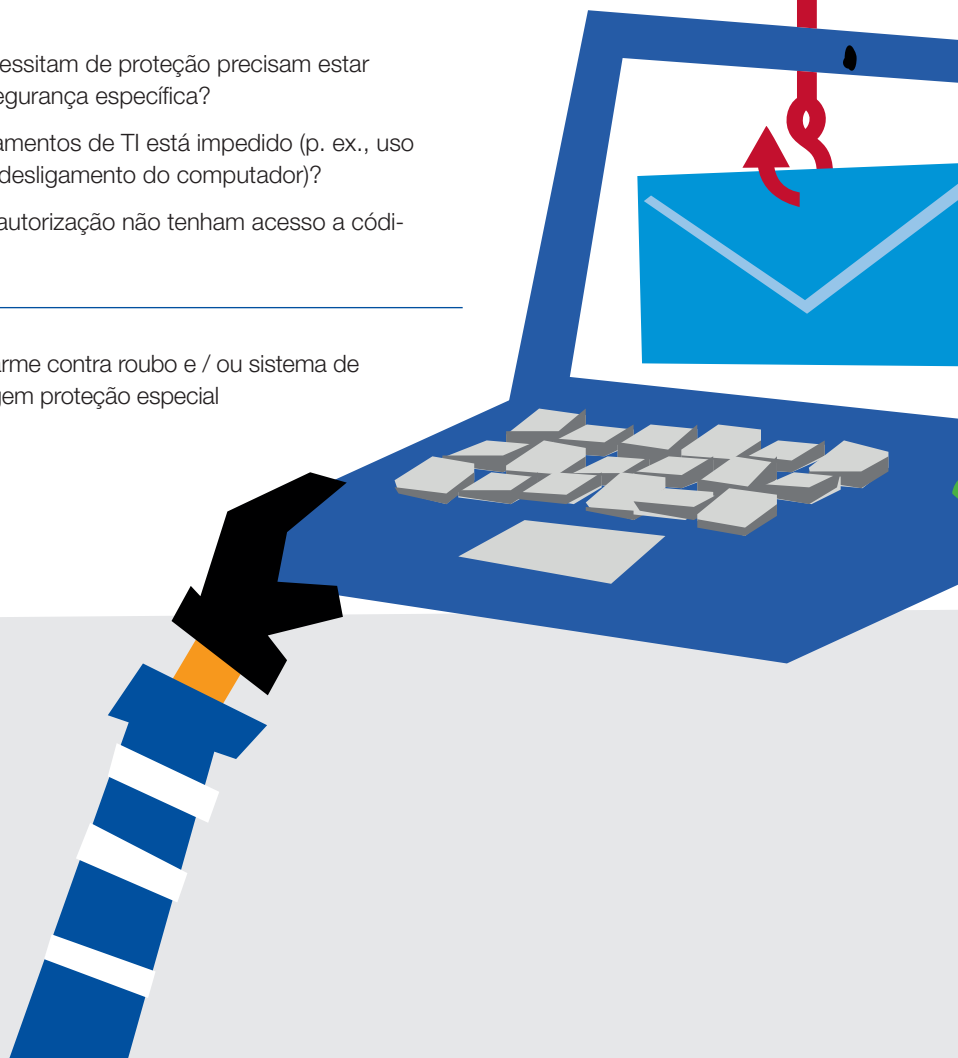
Medidas de Proteção
contra acesso não autorizado a informações sensíveis que necessitam de proteção

O acesso a informações sensíveis que necessitam de proteção é sempre efetivamente limitado às pessoas autorizadas e os direitos de acesso são revisados em intervalos regulares
e - se necessário - ajustados?

Na ausência da pessoa autorizada, são tomadas medidas de proteção adequadas?

- É garantido que, na ausência de pessoas autorizadas, pessoas sem autorização não estejam na sala que contenha documentos sensíveis? P. ex., a limpeza da sala é sempre realizada na presença da pessoa autorizada?
- As salas, armários e outros locais em que as informações sensíveis que necessitam proteção se encontram estão fechadas na ausência da pessoa autorizada?
- As informações sensíveis que necessitam de proteção precisam estar armazenadas em um local com segurança específica?
- O acesso não autorizado a equipamentos de TI está impedido (p. ex., uso de senhas seguras, bloqueios ou desligamento do computador)?
- Está garantido que pessoas sem autorização não tenham acesso a códigos de acesso ou chaves?

É necessário instalar um sistema de alarme contra roubo e / ou sistema de controle de acesso para áreas que exigem proteção especial
(como arquivos, salas de servidores)?



Medidas de proteção contra acesso não autorizado a informações sensíveis que necessitam proteção

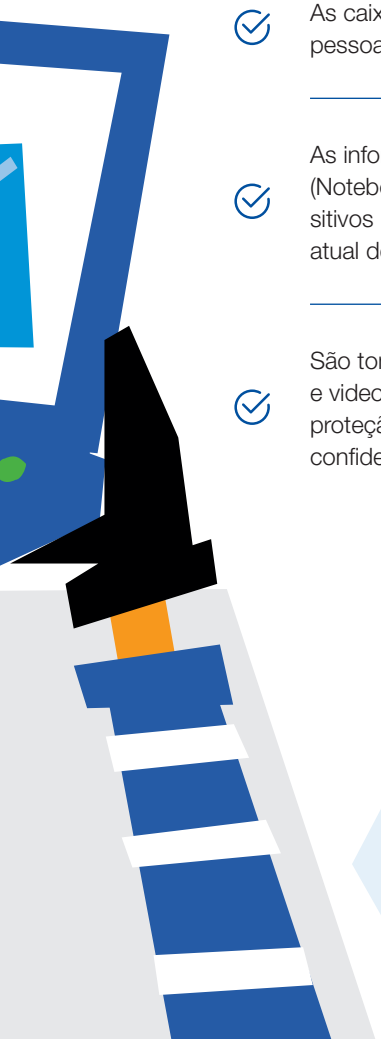
Senhas de segurança para sistemas que contenham informações sensíveis que necessitam proteção:

- As senhas utilizadas são suficientemente complexas (p. ex., com mínimo de oito caracteres e possuem uma letra maiúscula, uma letra minúscula, caracteres especiais e números) e são substituídas regularmente?
- É garantido que as senhas não são transmitidas a terceiros e que, caso sejam anotadas, não são guardadas em local de acesso livre (p. ex., são guardadas num cofre, em envelope selado, com data e assinatura, além de ser guardado em uma gaveta trancada?)
- É utilizada autenticação de dois fatores?

As caixas de correio internas estão instaladas de modo a impedir o acesso de pessoas não autorizadas às informações sensíveis que necessitam proteção?

As informações confidenciais armazenadas em portadores de informações (Notebooks, tablets, smartphones, discos rígidos, servidores, CD-ROM, dispositivos USB), estão eficazmente protegidas (p. ex., utilizando a tecnologia mais atual de criptografia)?

São tomadas medidas eficazes durante a transmissão (p. ex., por e-mail, tele e videoconferência, envio por carta) de informações sensíveis que necessitam proteção (p. ex., criptografia da comunicação, distribuição das informações confidenciais por diferentes portadores de informações)?



Medidas de Proteção
contra acesso não autorizado a informações sensíveis que necessitam proteção

As impressoras e fotocopiadoras estão configuradas de forma segura? Está garantido que não é possível a reprodução de tarefas de impressão ou cópia que contenham informações sensíveis que necessitam proteção? É tomado cuidado para garantir que os originais, impressões ou cópias sejam removidos imediatamente e não sejam deixados na impressora / fotocopiadora / aparelho de fax (se necessário usando a „função de PIN“)?

- As reuniões são conduzidas de forma a garantir que a divulgação de informações sensíveis que necessitam proteção não sejam feitas a pessoas sem autorização?
- É garantido que as informações fora da sala (p. ex. banners de identificação) não permitam conclusões sobre o conteúdo confidencial da reunião?
- É garantido que não é possível escutar do lado de fora (p. ex., no andar, salas adjacentes, janelas, portas)?
- É garantido que não é possível visualizar os documentos da reunião ou apresentação a partir do lado de fora (p. ex., fechar cortinas)?
- É garantido que, após o final da reunião, não são deixados documentos, equipamentos, suportes da apresentação (folhas de flipchart, transparências, textos no quadro branco)?
- É garantido que a sala de reuniões não esteja acessível a pessoas sem autorização em caso de ausência geral (p. ex., durante pausas)?

Eliminação qualificada de informações sensíveis que necessitam proteção

A eliminação ou apagamento de informações sensíveis que necessitam proteção é realizada de forma qualificada e segura?

- São utilizadas na eliminação fragmentadoras de papel „Cross-Cut“, com tamanho máximo das partículas de 160mm²?
- Caso sejam usados containers de recolha: Os containers de recolha estão fechados? Estão instalados de forma segura? O processo de eliminação está organizado com segurança suficiente? É respeitada a norma DIN 66399 (nível mínimo de segurança 4)?

As informações confidenciais gravadas em portadores de informações eletrônicos regraváveis (como unidades USB, cartões de memória, CD / DVD, discos rígidos, ...) serão apagadas de maneira completa e segura antes de estes serem reutilizados ou compartilhados com terceiros?

Considerações relativas à proteção da informação durante viagens e em público

- Antes da viagem, é verificada a real necessidade de levar as informações sensíveis que necessitam proteção?
- É garantido que, durante a viagem, pessoas sem autorização não visualizem as informações sensíveis que necessitam proteção (p. ex., pastas e Notebook)?
- É garantido que as pastas, Notebook, etc., estejam sempre supervisionados durante a viagem?
- É garantido que pessoas não autorizadas não podem escutar conversas ou telefonemas?
- Os Notebooks estão presos a uma estrutura fixa por meio de um cabo de segurança e, assim, protegidos contra remoção não autorizada?
- As informações sensíveis que necessitam proteção estão proibidas de serem publicadas na Internet e nas redes sociais?
- É garantido que, ao devolver o veículo de aluguel ou leasing, não estão gravados dados (p. ex., no telefone ou sistema de navegação) nem são deixados documentos no seu interior?

Notas pessoais

Notas pessoais

be-secure.basf.net
Versão: Outubro de 2019