PHISHX

Como realizar o descarte seguro de dados

Descarte seguro

Diariamente armazenamos e movimentamos uma grande quantidade de dados e informações dentro de nossos dispositivos. No contexto corporativo, essas informações podem ser muito valiosas, contendo dados considerados sensíveis e confidenciais.

Com a entrada em vigor de leis de proteção de dados, as organizações têm buscado elaborar métodos para lidar com essas informações de forma segura. Sendo assim, para atuar em conformidade com a legislação, e com as normas técnicas, o estabelecimento de políticas para o descarte seguro de dados é essencial.

A destruição segura de dados envolve métodos para tornar a informação inacessível. E aqui vamos saber um pouco mais sobre essas formas para garantir a segurança dos dados descartados.

Tipos de mídia

Antes de tudo, vamos saber um pouco mais sobre os tipos de mídia que existem.

Os discos rígidos, na sigla em inglês, HDD, hard drives disks, ainda são as principais formas utilizadas para armazenar informações em dispositivos. Eles utilizam um prato magnético para armazenar as informações, que é dividido em vários setores e trilhas que guardam dados que compõem os arquivos. Essas informações são lidas através de um braço mecânico, que percorre toda a área do disco.

Quando você salva um documento em seu dispositivo, ele é armazenado no disco rígido. Assim, ao excluir um arquivo, os dados armazenados no chamado HD passam a ser sobrepostos.

Porém, existem métodos que possibilitam a recuperação dessas informações. Isso faz com que seja essencial a adoção de processos para descartar os dados com mais segurança após seu tempo de uso.

Diferentes dos discos rígidos, os SSDs, Unidades de Estado Sólido em português, não utilizam formas mecânicas para armazenar as informações. Assim, os SSDs armazenam dados em chips, tornando o processo totalmente eletrônico.

Além disso, muitas mídias digitais, como servidores antigos, equipamentos que não são mais utilizados, como CDs, DVDs e mídias removíveis, como pen drives, podem conter informações sensíveis.

Como descartar dados de forma segura

É comum que as pessoas acreditem que após excluir um arquivo em um dispositivo, os dados desapareçam. Mas existe uma diferença entre o descarte de dados e a destruição segura de informações.

Existem algumas técnicas para descartar essas mídias eletrônicas, mas vale lembrar que algumas são válidas para apenas uma parte delas. Vamos saber porque.

Sobrescrever e criptografar: Você pode utilizar ferramentas para sobrescrever as informações, que consiste em gravar sequências de dados para tornar os arquivos incompreensíveis. Ou utilizar métodos para criptografar dados excluídos, assim você garante que eles não sejam recuperados.

Desmagnetização: O descarte seguro de dados armazenados em discos rígidos também pode ser realizado através de uma técnica chamada desmagnetização. Ela expõe o dispositivo a um campo magnético, que inutiliza o disco, destruindo informações sem necessidade de utilizar um software.

Destruição física: Você também pode optar pela destruição física do dispositivo e das informações não eletrônicas. Assim, você garante que as informações sejam completamente destruídas ou inutilizadas, e os dados não poderão ser recuperados.

Documentos físicos

Proteger os arquivos físicos e digitais que mantemos armazenados deve ser uma prioridade. Quando você descarta um arquivo, seja jogando um papel no lixo ou arrastando um documento para a lixeira do seu dispositivo, ele ainda pode ser acessado. Por isso, deletar e jogar fora não é o suficiente.

Para descartar documentos físicos, como papéis e até mesmo mídias como CDs e DVDs, é importante garantir a destruição completa e impossibilitar a recuperação de informações.

Assim, considere utilizar uma fragmentadora de papel para descartar documentos. Para descartar CDs e DVDs que possam conter informações sensíveis, você pode utilizar uma toalha para cobrir e quebrar essas mídias. Assim, você se protege de fragmentos.

Tenha atenção

Sempre que for destruir algum tipo de dado ou mídia que pertence a sua organização, tenha certeza de que você está agindo de acordo com as normas e políticas de segurança. Assim, você se certifica de que está seguindo os processos determinados pelas equipes de segurança da informação.

E lembre-se, caso o seu computador pessoal precise de assistência técnica, é possível remover o disco rígido, ou utilizar processos para criptografar suas informações. Dessa forma, você garante que seus dados estejam protegidos.