[OneDrive - Office 365]

O Microsoft OneDrive for Business é uma solução de armazenamento de arquivos em nuvem. Os arquivos são armazenados em servidores espalhados pelo mundo em um modelo que assegura sua disponibilidade em caso de falhas. Diversos padrões de proteção são adotados pela Microsoft para melhorar a segurança das informações armazenadas nele. Entretanto, sendo o OneDrive uma solução de armazenamento e compartilhamento de informações em nuvem, alguns pontos são importantes para segurança de nossas informações:

- Os arquivos armazenados em nuvem podem ser acessados de qualquer local e em qualquer horário;
- É possível acessar os dados de diversas formas, inclusive a partir de redes que não apresentem níveis adequados de segurança;
- É de responsabilidade de cada um a gestão dos direitos de acesso aos arquivos. As pessoas devem decidir quando e com quem um arquivo deve ser compartilhado, bem como remover o acesso quando o mesmo não for mais necessário;
- Você pode optar por salvar os arquivos em uma área exclusiva sua ou em uma área para trabalhar em grupo;
- Os arquivos armazenados na área pessoal e seus respectivos compartilhamentos são removidos quando a pessoa é desligada da instituição. Isso não ocorre com os arquivos armazenados em área de grupo.

[Uso aceitável do OneDrive]

O OneDrive é mais uma das opções que a TI ASAV disponibiliza para você armazenar seus arquivos de trabalho. Dependendo do tipo de informação que você tem no arquivo, um local pode ser mais indicado que outro:

- Informações sabidamente confidencias ou protegidas por leis específicas NÃO devem ser armazenadas no OneDrive, por exemplo:
    - Arquivos que contenham dados cadastrais de alunos e empregados como: CPF, Endereço, RG, endereço, salários, renda, etc.;
    - Arquivos que contenham dados acadêmicos de alunos como: resultado de avaliações, pareceres, etc;
    - Arquivos que contenham dados financeiros como: mensalidades, bolsas, dívidas, etc;
- Outros tipos de informações podem ser armazenados desde que observada as recomendações de Uso seguro do OneDrive.

[Uso seguro do OneDrive]

Use o compartilhamento com muita atenção

- Por padrão os arquivos são compartilhados com direitos de "Edição". Caso não seja essa sua intenção você precisa alterar;
- Evite ao máximo compartilhar pastas inteiras, de sempre preferência por compartilhar os arquivos de forma individual, facilitando seu gerenciamento.
- Revise o item e os destinatário antes de compartilhar o arquivo. Não seria legal compartilhar algum material importante de seu trabalho com direitos de "Edição" para uma pessoa desconhecida!
- Os arquivos colocados na pasta "Compartilhado com Todos" são **compartilhado com todos**. "Todos" inclui funcionários, professores e alunos.
- Lembre-se que uma vez que o arquivo é compartilhado com outra pessoa ela pode fazer download ou compartilhar outros como o mesmo nível de permissão que ela tem.

Revise seus compartilhamentos com frequência

- As pessoas mudam de setor e função. Eventualmente uma informação que você compartilhou e era necessária para o trabalho de outra pessoa deixa ser. Assim, é importante que você revise seus compartilhamentos de tempos em tempos e revogue os que não são mais necessários.

Sincronize apenas com computadores seguros

- Você pode sincronizar os arquivos armazenados em sua área pessoal do OneDrive com seu computador para trabalhar *offline*. Neste caso uma cópia de cada um dos arquivos será gravada em seu computador e sincronizado com a nuvem;
- Você deve fazer isso apenas em computadores seguros e observando as orientações a seguir.

Proteja seu computador

- Tenha sempre um antivírus instalado e atualizado;
- Mantenha o firewall habilitado e controlando as conexões;
- Não trabalhe usando um usuário com direitos de administração.
- Mantenha os aplicativos atualizados;
- Mantenha seu computador protegido com uma senha;
- Comunique a área de tecnologia caso perca seu computador ou ele seja furtado;
- Consulte a área de tecnologia caso observe algum problema ou desconfie de algo estranho;

Proteja seu celular

- Sempre proteja seu celular com senha, PIN ou biometria;
- Apenas instale aplicações de locais conhecidos e seguros;
- Tenha uma cópia de segurança de seus dados importantes;
- Comunique a área de tecnologia caso perca seu celular ou ele seja furtado;
- Mantenha o sistema operacional e aplicativos atualizados.

Cuidado com redes públicas

- Redobre sua atenção ao utilizar redes públicas como: aeroportos, praças e lan houses;
- Evite acessar sites que armazenem informações importantes suas e colocar seu usuário e senha em formulários de autenticação.