omnisblue

MANUAL DA SEGURANÇA DA INFORMAÇÃO

Sumário

1. Histórico de revisão do documento

Abaixo são registrados as versões e atualizações deste documento.

Versão	Data	Autor	Alterações
1.0	06/01/2023	Daniel Zaitz	Versão inicial do documento.
1.1	20/01/2023	Adilson Taub	Revisão do documento.
1.2	14/02/2023	Daniel Zaitz	Revisão do Documento.
1.3	16/06/2023	Anderson Matiucci	Revisão do Documento.

2. Missão

A área de Segurança da Informação tem como objetivo proteger os ativos de informação da OMNISBLUE contra o uso não autorizado, divulgação, modificação, dano ou perda, gerenciando riscos e ajudando a viabilizar os serviços de Tecnologia da Informação. A segurança da informação é um processo cultural e um diferencial competitivo para empresas de qualquer ramo de atuação.

A nossa missão é ajudar a empresa a manter um nível aceitável de risco de segurança da informação, seguindo os padrões globais, políticas de segurança, e outras regulamentações.

3. Objetivo

As Diretrizes de Segurança da Informação têm como objetivo nortear as ações de segurança ligadas às informações e regulamentar a utilização dos recursos de processamento da informação de propriedade ou controlados pela Omnisblue. O detalhamento das determinações contidas nas diretrizes está distribuído entre o Manual de Segurança da Informação, as Políticas e os Padrões de Segurança da Informação da empresa.

Conhecendo as informações deste manual, os usuários estarão preparados para:

- Minimizar os riscos de fraudes;
- Evitar vazamento de informações corporativas;
- Evitar contaminação e disseminação de vírus;
- Mitigar os riscos de comprometimento dos dados e sistemas corporativos por agentes internos ou externos.

4. Determinações

- O Manual de Segurança da Informação deve ser conhecido e seguido por todos os indivíduos que utilizam os recursos de processamento da informação de propriedade ou controlados pela OMNISBLUE, sendo de responsabilidade de cada um o seu cumprimento. Os demais documentos que compõem as Políticas de Segurança da Informação devem ser conhecidos de maneira oportuna, de acordo com as atividades de cada colaborador;
- É dever de todos os colaboradores, zelar pela segurança das informações corporativas do OMNISBLUE e de seus clientes;
- Os documentos produzidos por intermédio dos recursos de processamento da informação na OMNISBLUE são de propriedade da OMNISBLUE. O mesmo se aplica aos programas desenvolvidos por funcionários, terceiros ou prestadores de serviço;
- Toda informação gerada com recursos do OMNISBLUE deve ser classificada quanto a sua confidencialidade, de maneira a ser adequadamente protegida quanto ao seu acesso e uso. A classificação das informações deverá ser realizada de acordo com a Política de Classificação da Informação;
- Todo usuário de recursos de informação deve possuir identificação única, pessoal e intransferível;
- Informações corporativas e recursos de informação do OMNISBLUE devem ser utilizados de maneira lícita, ética e de acordo com as políticas de segurança da informação. Funcionários, terceiros e prestadores de serviço devem entrar em contato com a área de Segurança da Informação antes de se envolverem em quaisquer atividades que não estejam explicitamente cobertas pelas políticas de segurança;
- Qualquer indício de fraude, sabotagem, desvio ou falha na segurança da informação deverá ser imediatamente notificado a um representante da Segurança da Informação;
- Todos os indivíduos que trabalhem ou prestem serviços para o OMNISBLUE devem ter acesso físico e lógico liberado somente aos locais e recursos necessários ao desempenho de suas atividades e funções;
- Uma pessoa não deve possuir o controle exclusivo e completo de uma transação ou processo de negócio;
- O OMNISBLUE deve manter planos que garantam a continuidade das operações em situações de crise e o retorno à situação de normalidade;

- Todos os recursos de processamento da informação do OMNISBLUE devem ser avaliados quanto à sua aderência aos padrões de Segurança da Informação. A avaliação deve ser conduzida durante todo o processo de desenvolvimento do recurso até sua implantação;
- Os usuários não devem possuir expectativa de privacidade com relação às informações tratadas, enviadas ou armazenadas através dos recursos de informação do OMNISBLUE. Todas as ações efetuadas neste ambiente estão passíveis de monitoramento. Ao utilizar os recursos do OMNISBLUE, o usuário estará automaticamente consentindo com o monitoramento do sistema;
- O OMNISBLUE mantém todos os usuários responsáveis por suas ações enquanto utilizando os recursos de informação da empresa. A não observância dos preceitos destas Diretrizes e do conjunto de Políticas do OMNISBLUE bem como a apropriação ou utilização indevida dos recursos computacionais da empresa implicará na aplicação de sanções administrativas e na adoção de medidas legais cabíveis.

5. Responsabilidade dos colaboradores

- É dever de todos os indivíduos que trabalham ou prestam serviços para a OMNISBLUE, conhecer, entender e aderir às Diretrizes de Segurança da Informação bem como as informações contidas neste manual. É responsabilidade de cada usuário manter-se informado sobre atualizações e mudanças nos referidos documentos que se encontram disponíveis no Portal na página da Segurança da Informação;
- Todo colaborador deve participar do Programa de Conscientização de Segurança assim que iniciar suas atividades a serviço do OMNISBLUE;
- Todo colaborador deve conhecer suas responsabilidades dentro do Plano de Continuidade de Negócios da empresa;
- É dever de todos os colaboradores assegurar que a segurança da informação é parte do processo de planejamento de todas as tarefas e projetos;
- Todos os usuários devem manter as informações da organização fora do alcance de pessoas não autorizadas, mantendo seu local de trabalho limpo e organizado e as informações em qualquer meio, físico ou lógico, devidamente guardadas e seguras;
- Os usuários não devem comentar detalhes técnicos sobre sistemas ou mecanismos de segurança utilizados pela empresa com pessoas não autorizadas, mesmo que elas sejam de sua confiança.

6. Acesso aos sistemas

- Toda demanda de concessão de acesso deverá ser encaminhada ao Departamento de Infraestrutura através do formulário publicado no sharepoint;
- Todas as solicitações de acesso devem ser aprovadas pelo superior imediato do colaborador e pelo dono do perfil solicitado, de forma a assegurar que o acesso solicitado é o mínimo necessário para os requerimentos de negócio e função do solicitante e que não fere os princípios de segregação de funções onde os mesmos sejam possíveis e praticáveis;
- É responsabilidade do requerente, zelar pela veracidade das informações providas no formulário SAS - Solicitação de Acesso a Sistemas;
- Antes de obter acesso aos sistemas de informação do Omnisblue, terceiros, prestadores de serviço ou parceiros comerciais necessitam assinar o TERMO DE RESPONSABILIDADE PARA USO DE RECURSO CORPORATIVO disponível no sharepoint e enviá-lo para o Departamento de Infraestrutura;
- Os IDs fornecidos a terceiros, prestadores de serviço ou parceiros comerciais, possuirão data de expiração máxima de 90 dias. Esta data poderá ser reduzida de acordo com o período de permanência do profissional na empresa ou estendida, sempre que necessário, através de solicitação formal;
- Os Gerentes devem notificar os Administradores de Segurança imediatamente sobre usuários que mudaram de área, cargo ou função ou deixaram a organização, para que as ações apropriadas sejam efetuadas;
- Nos casos de mudança de área, o novo gerente deve solicitar formalmente os novos acessos requeridos pela nova função do funcionário;
- É proibido tentar acessar recursos adicionais aos que foram atribuídos a você pelo seu superior imediato. Qualquer acesso não autorizado será considerado falta grave;

- Os IDs de usuários serão bloqueados após 60 dias de inatividade e removidos após 90 dias de bloqueio a menos que o usuário em questão solicite que a conta seja reativada, provando sua identidade e que o relacionamento de negócios com a empresa não mudou durante o período de inatividade.

7. Senhas

- Todo usuário deve estar ciente de que seu ID de usuário e senha não devem ser compartilhados. Qualquer infração ou anormalidade no sistema será atribuída ao proprietário da credencial (ID de usuário) em uso;
- É obrigatório o uso de oito (8) caracteres para a formação de uma senha de acesso;
- Após cinco (5) tentativas incorretas de acesso ao sistema, a senha do usuário será bloqueada, devendo ser reativada, seja através do OMNISBLUE, ou após trinta (30) minutos de espera para senhas de rede;
- Os usuários devem verificar a notificação que é feita no início de uma sessão (quando fornecida pelo sistema em uso) referente aos dados da última utilização do sistema e notificar seu superior caso suspeite que seu ID de usuário tenha sido utilizado por terceiros;
- Todas as senhas possuem noventa (90) dias de validade. Após este prazo, o usuário é obrigado a alterá-las, não sendo permitido repetir as doze (12) últimas senhas utilizadas no sistema;
- circunstância: <seu próprio usuário, (ex:. <SP10001>), <senha>, <password>, <OMNISBLUE123> ou <OMNISBLUEinformatica>;
- Usuários nunca devem escrever ou gravar uma senha de forma desprotegia e guardá-la próxima ao dispositivo ao qual ela pertence. Senhas devem ser protegidas com o mesmo nível de proteção dado à informação que elas protegem. Para mais detalhes sobre níveis de proteção, ver a Política de Classificação da Informação disponível na página da Segurança da Informação no Portal;
- As senhas devem ser alteradas sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha.

É responsabilidade do usuário, escolher uma senha forte que não seja baseada em nada que alguém possa facilmente adivinhar ou obter usando informações relativas à pessoa, por exemplo, nomes, números de telefone e datas de aniversário.

8. Acesso Remoto

- Não é permitido o acesso remoto à rede ou ao serviço de correio eletrônico do OMNISBLUE a menos que haja necessidade de negócio claramente justificada e aprovada pelo Departamento de Infraestrutura;
- Não é permitida a utilização de linha discada para conexões entre o OMNISBLUE e pontos remotos, devem ser utilizadas somente conexões aprovadas. Havendo necessidade incontornável e justificada pela necessidade do negócio de estabelecer uma conexão remota através de linha discada, uma solicitação aprovada pela gerência do solicitante deverá ser submetida à Área de Segurança da Informação para aprovação;

9. Uso de Software

- Qualquer software, independentemente de sua condição comercial, deverá ser homologado e instalado exclusivamente pelo Departamento de Infraestrutura;
- Será considerada falta grave e passível de sanções administrativas a utilização e instalação de softwares não aprovados pelo Departamento de Infraestrutura;
- Todo o desenvolvimento ou compra de softwares estão absolutamente restritos à área de TI responsável;
- Todo o software comercial está sujeito à legislação local de direitos autorais. Seu uso deve ser regulamentado por uma licença comercial, gerenciada pelo Departamento de Infraestrutura;

- Os colaboradores devem atentar para o fato de que ferramentas do tipo “shareware” também acarretam sanções legais em caso de uso prolongado sem a aquisição da respectiva licença;
- São proibidas cópias não autorizadas de software do Omnisblue, seja para uso pessoal ou para terceiros;
- Cada colaborador deve assegurar o controle de seus próprios recursos, notificando a área de Infraestrutura em caso de dúvidas ou anormalidades.

10. Uso de Internet e Comunicação

- A Internet é uma ferramenta disponibilizada pelo OMNISBLUE aos seus colaboradores para uso estritamente profissional. Todo e qualquer acesso deve estar relacionado às atividades da empresa, incluindo comunicação com clientes e fornecedores, pesquisa tecnológica e empresarial, além de eventuais tópicos definidos como estratégicos pela alta administração. Fica vedado o seu uso para fins pessoais ou para assuntos que não estejam relacionados com o negócio da empresa;
- Não é permitido fazer cópias através da Internet de programas e softwares que não tenham sido aprovados pelo Departamento de Infraestrutura. O mesmo se aplica aos arquivos anexados enviados ou recebidos através do correio eletrônico;
- O OMNISBLUE não se responsabiliza por ações ou transações efetuadas pelos colaboradores através da Internet. Não utilize as facilidades de comunicação de modo impróprio ou que viole a legislação em vigor. Em caso de ações legais, o OMNISBLUE poderá ser obrigado a fornecer evidências para serem utilizadas em corte judicial;
- É proibida a divulgação, publicação e/ou hospedagem de quaisquer informações corporativas do OMNISBLUE na Internet, seja através de sites e/ou mensagens eletrônicas, incluindo o upload de arquivos proprietários e imagens do ambiente corporativo, sem autorização explícita da empresa;
- Nenhum colaborador pode expressar opiniões em nome da organização através de listas públicas ou privativas de discussão/distribuição ou quaisquer outros canais de comunicação eletrônica, a não ser que explicitamente autorizado pela alta administração;
- Serão considerados ofensivos e passíveis de sanções administrativas os acessos a sites que hospedem materiais pornográficos, criminosos, de violência explícita ou quaisquer materiais que estejam contra a legislação vigente do país, bem como o uso do correio eletrônico para a disseminação de tais materiais ou quaisquer comentários que possam denegrir a imagem da organização ou de seus clientes;
- Cada usuário que tenha sua própria conta de correio eletrônico, não deve compartilhá-la ou utilizá-la em listas públicas ou privativas de discussão/distribuição. Nenhum usuário deve enviar correio eletrônico de maneira que pareça ter sido enviado por outro usuário;
- Não é permitido enviar ou repassar mensagens do tipo “corrente” a partir dos recursos computacionais do OMNISBLUE. O mesmo vale para mensagens sobre vírus ou outras ameaças à segurança das informações;
- Os usuários não devem acessar links contidos em mensagens eletrônicas (e-mails) de origem duvidosa. Deve-se tomar um cuidado extra com relação às mensagens recebidas de remetentes externos;
- As mensagens em caráter de comunicado geral devem ser enviadas pela Área de Marketing da instituição;
- Os meios de comunicação eletrônica de propriedade do OMNISBLUE e serão passíveis de monitoramento.

11. Uso das estações de trabalho

- É proibida a conexão de equipamentos (notebooks e desktops) de propriedade de funcionários, terceiros ou parceiros comerciais à rede do OMNISBLUE a menos que haja aprovação formal do Departamento de Infraestrutura. É proibido o armazenamento ou processamento de dados da Empresa em computadores ou recursos de informática de propriedade particular;
- A troca/sincronismo de dados entre recursos de computação móvel e computadores do OMNISBLUE, ligados à rede ou não, é proibida a menos que o recurso móvel seja de propriedade do OMNISBLUE e devidamente identificado com número de patrimônio;
- As solicitações de utilização de recursos de computação móvel devem ser direcionadas à Gerência do Solicitante através do formulário SAC – Solicitação de Autorização para Conexão de Recurso de Computação Móvel disponível na página da Segurança da Informação no sharepoint e devem ser liberadas mediante a comprovação da necessidade do negócio;
- Microcomputadores (desktops e notebooks) que possuam tecnologia wireless ou correlata somente poderão ser utilizados dentro das instalações do OMNISBLUE se estiverem configurados de acordo com o padrão da empresa;
- A perda ou roubo de qualquer equipamento móvel de propriedade do OMNISBLUE deve ser imediatamente comunicada à área de Infraestrutura;
- Todas as estações de trabalho, incluindo equipamentos portáteis e stand alone, devem utilizar proteção de tela com senha. A estação será bloqueada após 5 minutos de inatividade;
- O colaborador não está autorizado a desativar a ferramenta de antivírus de seu equipamento e em caso de suspeita de vírus, deve entrar em contato imediatamente com a Infraestrutura;
- Não é permitida a gravação de informações do OMNISBLUE nas estações de trabalho ou o compartilhamento de arquivos locais da estação com outras máquinas da rede. Os usuários devem proteger os dados do OMNISBLUE de perda, armazenando-os num servidor de arquivos de forma que serão adequadamente criadas cópias de segurança para esses dados. Todo e qualquer compartilhamento deverá ocorrer nos servidores de arquivos disponibilizados pelo Departamento de Infraestrutura;
- Não é permitido o uso de dispositivos para gravação de dados (ex. pen drives, gravadores CD, etc) a menos que estejam explicitamente autorizados pela Segurança da Informação;
- Constitui falta grave alterar, transferir, remover quaisquer equipamentos de propriedade do OMNISBLUE sem a autorização da Área de Infraestrutura;
- Não é permitida a inclusão ou exclusão de qualquer hardware ou software nas estações de trabalho do OMNISBLUE. Todas as inclusões ou exclusões devem ser efetuadas através da área de tecnologia responsável pelas instalações.

12. Confidencialidade das informações

- Todos os usuários de recursos de computação do OMNISBLUE devem conhecer e aderir às regras para manuseio de dados corporativos descritas na Política de Classificação da Informação;
- Todas as informações e ativos associados aos recursos de processamento da informação devem ter um gestor responsável por tomar as medidas necessárias para protegê-los;
- As informações devem ser armazenadas, transmitidas e divulgadas de acordo com as regras estabelecidas para o nível de classificação das mesmas. O mesmo se aplica à proteção das informações impressas;
- Deve-se limitar a quantidade de armazenamento e tempo de retenção das informações de portadores de unidades de armazenamento externa (CD, pendrives, etc.) para o mínimo requerido pelo negócio ou por propósitos legais ou regulatórios;
- Cuidados especiais devem ser tomados na interpretação da classificação dos documentos recebidos de outras organizações, as quais podem ter diferentes definições para a mesma classificação. Informações recebidas de terceiros não devem ser divulgadas antes da assinatura de um documento de liberação;
- Durante a sua ausência do local de trabalho, mantenha documentos, mídias digitais (CD, disquetes, etc.) em local seguro. Não os deixe disponíveis em cima da mesa ou em local desprotegido.

13. Comunicação de Incidentes de Segurança

É responsabilidade dos usuários relatar prontamente qualquer comportamento ou circunstância suspeita que ameace a integridade dos ativos da empresa ou recursos de processamento de informação. Caso perceba alguma anormalidade, atividade fraudulenta ou evento que configure em um incidente de segurança, siga as orientações a seguir:

- Evite tomar ações arbitrárias como remover arquivos desconhecidos ou reinicializar o sistema. Nenhuma tentativa de correção do problema deve ser feita pelo usuário, a menos que sob direta orientação do OMNISBLUE ou área de TI responsável;
- Tome nota de todas as mensagens ou sequências de eventos que originaram o incidente;
- Na ocorrência de um vírus não removível pela vacina instalada, os usuários de desktops ou notebooks devem desligar o equipamento para evitar a propagação dos danos e entrar em contato imediatamente com o OMNISBLUE.

14. Recomendações e boas práticas

- Busque sempre a orientação da Área de Infraestrutura para implementação de novos aplicativos ou questões relativas aos sistemas de informação da Empresa;
- Procure armazenar arquivos críticos em servidores de arquivos disponibilizados pelo Departamento de Infraestrutura. Não faça cópias de segurança em CDs ou Disquetes. Em caso de dúvida com relação a procedimentos de armazenamento e backup, contate a área de Infraestrutura;
- Deve-se verificar a existência de códigos maliciosos nos arquivos armazenados em mídias, bem como nos arquivos transmitidos através de redes antes do uso dos mesmos;
- Somente mídias e produtos previamente autorizados e de origem confiável devem ser utilizados;
- Deve-se travar a estação, finalizar sessão, remover token de autenticação quando o usuário sai do local de trabalho;
- Evite vazamento de informações restritas à empresa. Caso receba uma chamada telefônica por engano, não forneça informações como, estrutura organizacional interna, sua localização, atribuições ou área onde trabalha. Fale apenas o necessário para finalizar a ligação gentilmente;
- Não abandone documentos na impressora, evite divulgar informações de propriedade do OMNISBLUE a pessoas não autorizadas;
- Se vir um estranho que não esteja usando crachá de identificação, ou que apresente comportamento suspeito, entre em contato com a equipe de segurança local imediatamente;
- Proteja os equipamentos do OMNISBLUE e tenha atenção redobrada caso o seu equipamento seja um notebook. Procure deixá-lo em lugar seguro na empresa após o término do expediente. Não o utilize para fins pessoais e siga as recomendações da área de Infraestrutura. Cadeados são disponibilizados e devem ser utilizados inclusive no ambiente do OMNISBLUE.
- Utilize sempre senhas fortes, contendo além de letras e números algum caractere especial como por exemplo @ ou _ e se possível utilize letras maiúsculas e minúsculas.

15. Glossário

- **Administrador de Redes\Segurança** – Funcionário com privilégios especiais, responsável por efetuar administração de usuários.
- **Antivírus** - Programa ou software especificamente desenvolvido para detectar, anular e eliminar de um computador, vírus e outros tipos de códigos maliciosos.
- **Autenticação / Login** - Processo de validação de credenciais para conexão com a rede, sistema ou aplicação.

- **Backup** - Cópia de segurança de arquivos, mídias, papéis, ou qualquer outra fonte de informação.
- **Classificação da informação** – Processo através do qual o Proprietário da Informação atribui um grau de sigilo às informações.
- **Códigos Maliciosos** - Código malicioso de computador é um programa – uma parte de um código executável – com capacidade de auto-replicação podendo destruir arquivos, formatar a unidade de disco rígido ou causar outros danos.
- **Colaborador** – Qualquer pessoa que trabalhe ou preste serviços para o OMNISBLUE;
- **Comunicação eletrônica** - é todo o meio eletrônico utilizado para o envio e recebimento de dados, esteja ele restrito ou não ao perímetro corporativo do OMNISBLUE. As comunicações eletrônicas incluem, mas não se limitam a: Correio Eletrônico, Correio de Voz, videoconferência, bips, fax, acesso a Internet (seja web ou qualquer outro tipo de protocolo) e Intranet.
- **Conta de Usuário** – ID de usuário, “User ID”, nome que o usuário utiliza para acessar a rede, sistema ou aplicação.
- **Contas Genéricas** – Contas de usuário que não são relacionadas à uma determinada pessoa.
- **Criptografia** - Métodos de proteção de informações pelos quais apenas os detentores de um determinado segredo denominado "chave", têm acesso a elas. Informações criptografadas, mesmo quando capturadas em trânsito pela rede, não podem ser lidas por quem não conhece a chave necessária.
- **Desktop** – Computador de mesa;
- **Software de Domínio Público** - Um software é denominado de domínio público se seus direitos de cópia tiverem sido abdicados.
- **Download** – Ato de transferir cópias de um arquivo ou programa de um site ou de uma página da Web do servidor para um computador. O mesmo que baixar.
- **Equipamentos stand alone** – Computadores desconectados da rede.
- **Freeware** - Freeware é um software com direitos autorais, mas o detentor dos direitos permite e encoraja os usuários a melhorar o produto. No entanto, o software resultante pode somente ser distribuído gratuitamente.
- **Gestor da Informação** – Responsável pelo departamento e/ou processo de negócio onde a informação foi gerada ou o primeiro receptor / manipulador da informação.
- **Gestor de sistema** – Responsável pelo departamento e/ou processo de negócio que seja o principal usuário das informações manipuladas pelo sistema.
- **Grau de Sigilo** – Gradação atribuída a ativos de informação considerados sigilosos em decorrência da sua natureza ou conteúdo.
- **Informação** - Recursos de informação são definidos como qualquer dado criado, coletado, comunicado, usado ou observado por qualquer usuário de informação durante o seu período empregatício ou relacionamento com a OMNISBLUE.
- **ID de Usuário** – Mesmo que userID, “conta de usuário”, nome que o usuário utiliza para acessar a rede, sistema ou aplicação.
- **Log** – Arquivo de registro de ações efetuadas em sistemas de informação, utilizado para investigação de fraudes ou atividades suspeitas.
- **Notebook / laptop** – Computador portátil;
- **PDA / Pocket PC** - Personal Digital Assistant, é um computador de dimensões reduzidas, com possibilidade de interconexão com computadores pessoais e redes sem fio (wireless). Ex: Palmtop;
- **Portas USB (Universal Serial Bus)** – Portas utilizadas para conexão de qualquer dispositivo que possua a mesma interface, por exemplo, um "pen drive", dispositivo móvel que permite armazenar até centenas de MBs em dados de qualquer tipo.
- **Privilégios Especiais** – Direitos de acessos que dão capacidade ao usuário de efetuar administração de contas usuários e alterar parâmetros no sistema.
- **SAS** - Solicitação de Acesso a Sistemas - Formulário disponibilizado pela área de Segurança da Informação para submeter solicitações de acesso aos sistemas do OMNISBLUE.
- **Smartphone** - É uma mistura de Telefone Celular com PDA que possui aplicações de gerenciamento de informações pessoais e funções de multimídia;
- **Shareware** - Software distribuído livremente por um determinado período para fins de avaliação (ex: Winzip), permitindo ao usuário utilizá-lo antes de concordar em comprá-lo.
- **Sigilo** - Segredo de conhecimento restrito a pessoas credenciadas, proteção contra revelação não-autorizada.
- **SPAM** - Mensagem eletrônica não solicitada (geralmente para fins publicitários).
- **Upload** - Ação de enviar dados do seu computador para outro computador remoto (contrário de download).
- **Usuários Privilegiados** – Usuários com privilégios administrativos.

- **VPN (Virtual Private Network)** – Conexão entre dois pontos utilizando infraestrutura de rede pública.
- **Wireless** – Mesmo que rede sem fio, permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.