Prevenção em primeiro lugar:

O ciclo de vida do colaborador

e as funções da administração de TI em cada etapa

Digital Security
Progress. Protected.

Em uma organização, a jornada de cada colaborador é composta por diferentes etapas, da integração ao trabalho cotidiano até o eventual desligamento, e cada uma delas apresenta demandas de TI específicas. Assim, desde a recepção de novos membros, passando pelo suporte aos colaboradores atuais, até o gerenciamento das saídas, a equipe de TI desempenha um papel fundamental na garantia da operação segura e contínua da organização.

A construção de um processo ou plano de ação bem definido para o ciclo de vida dos colaboradores é, além de uma questão de eficiência, uma medida preventiva importante. Ao alinhar os processos de TI com as boas práticas, as organizações podem reduzir riscos relacionados à segurança de dados, controle de acessos e compliance.
Desenvolvemos uma checklist para orientar profissionais de TI nas diferentes fases da trajetória dos colaboradores, capacitando-os a cumprir suas responsabilidades e proteger o ambiente digital da organização.

Como usar a checklist?

A checklist de integração e desligamento atua como uma ferramenta para garantir a segurança e eficiência da infraestrutura digital.
Seu uso auxilia no planejamento e execução de todas as etapas necessárias para cada fase do ciclo do colaborador na empresa.

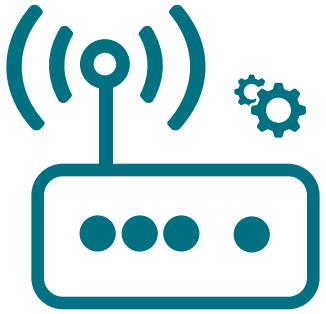
Integração

Digital Security
Progress. Protected.

1. Preparação de dispositivos para novos colaboradores:

- Atribua os ativos de hardware, realizando a identificação adequada.
- Reúna todos os acessórios necessários, como monitores, estações de acoplamento, teclados e mouses.
- Faça a preparação dos referidos dispositivos para os novos colaboradores, que pode incluir:
  - ☐ Instalar e disponibilizar todo o hardware e software necessários
  - ☐ Configurar contas de e-mail e permissões de acesso
  - ☐ Definir medidas de segurança e perfis de usuário
  - ☐ Personalizar o dispositivo de acordo com a função e requisitos do usuário

2. Acompanhamento no primeiro dia:



- Auxilie os novos colaboradores com o primeiro login no local de trabalho.
- Preste a ajuda necessária na configuração de senhas.
- Realize uma verificação do dispositivo com o usuário, garantindo o funcionamento correto de todos os recursos.
- Forneça um guia básico de instruções, abrangendo segurança, configuração do Wi-Fi e outros pontos essenciais.
- Garanta que o novo colaborador assine o protocolo de entrega do equipamento.

3. Regulamentos e diretrizes:

- Compartilhe uma lista dos aplicativos e softwares utilizados pelos colaboradores e suas diretrizes.
- Apresente aos colaboradores as variadas políticas da empresa, incluindo, por exemplo:
  - ☐ Política de TI/cibersegurança
  - ☐ Política de proteção de dados (GDPR)
  - ☐ Política de trabalho remoto
  - ☐ Política de mídias sociais
  - ☐ Política BYOD (traga o seu próprio dispositivo)

Política BYOD (traga o seu próprio dispositivo)

O modelo BYOD (traga seu próprio dispositivo) tem se tornado cada vez mais comum, trazendo a necessidade de instruir os colaboradores sobre o uso seguro dos seus dispositivos pessoais para atividades profissionais, evitando colocar em risco a segurança da empresa. Confira alguns aspectos que a política BYOD deve abordar:

- ☐ **Quem é elegível para participar do programa BYOD**
- ☐ **Lista de dispositivos, sistemas operacionais e plataformas permitidos e compatíveis com a política**
- ☐ **Requisitos de senha**
- ☐ **Requisitos de criptografia de dados**
- ☐ **Explicação do processo de limpeza remota**
- ☐ **Limitações de acesso e uso de dados**
- ☐ **Informações sobre o nível de suporte de TI oferecido para dispositivos pessoais**
- ☐ **Especificações sobre monitoramento e auditoria**
- ☐ **Responsabilidades dos colaboradores em termos de segurança e compliance**
- ☐ **O que fazer em caso de perda ou roubo de um dispositivo**
- ☐ **O que fazer no término do vínculo empregatício**

Durante o vínculo empregatício

Digital Security
Progress. Protected.

1. Educação em cibersegurança:

- Estabeleça uma instrução contínua dos colaboradores no tema das ciberameaças e boas práticas em segurança.

Como criar uma cultura de conscientização em cibersegurança, evitando a fadiga com o tema?

- ☐ Coopere com o departamento de RH para tornar a educação interativa e utilitária.
- ☐ Implemente sessões de formação mais curtas e frequentes, que costumam ter maior eficácia em relação a um único evento anual de treinamento.
- ☐ Compartilhe histórias da vida real e exemplos de suas experiências para tornar o conteúdo relevante e próximo da realidade dos colaboradores.
- ☐ Utilize formatos divertidos, como jogos, quizzes e simulações, para envolver os colaboradores.
- ☐ Assustar as pessoas não aumenta a sua conscientização em cibersegurança. Ao adotar essa abordagem, é possível que os colaboradores tenham receio em relatar erros ou ciberameaças potenciais.
- ☐ Mantenha a abertura para perguntas e reforce a sua disponibilidade para auxiliar quando necessário.

2. Princípio do privilégio mínimo:

- Garanta que o princípio do privilégio mínimo seja seguido.
- Reavalie e ajuste regularmente as permissões de acesso conforme o princípio.
- Desabilite o compartilhamento de arquivos e o encaminhamento de e-mails para endereços externos, prevenindo o vazamentos de dados.

3. Manutenção de dispositivos:

- Realize verificações periódicas, garantindo a instalação das mais recentes atualizações de segurança e software nos dispositivos dos colaboradores. Aplicável aos dispositivos fornecidos pela empresa e aos dispositivos pessoais utilizados para o trabalho.

4. Regras para trabalho remoto:

- Desaconselhe o uso de dispositivos pessoais para tarefas de trabalho, exceto no caso de adoção do sistema BYOD na sua empresa.
- Incentive o uso de uma rede privada virtual (VPN) para conexões seguras.
- Promova o uso de criptografia para dados sensíveis.
- Reforce a importância de senhas fortes para redes Wi-Fi, evitando acessos não autorizados.
- Garanta que a proteção de endpoint esteja ativa e atualizada em todos os dispositivos remotos.

Desligamento

Digital Security
Progress. Protected.

1. Gerenciamento de conta e acesso:

- Revogue as permissões de todos os aplicativos e serviços aos quais o colaborador desligado tinha acesso.
- Redefina as senhas de todos os dispositivos da empresa utilizados pelo colaborador.

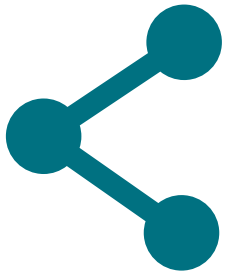
2. Acesso físico e hardware:

- Revogue o acesso ao prédio, incluindo crachás e chaves.
- Colete e recupere todos os dispositivos da empresa fornecidos ao colaborador, como laptops, smartphones e outros equipamentos.

3. Monitoramento e proteção de dados:

- Mantenha comunicação regular com o colaborador desligado, a fim de observar seu comportamento durante o processo de desligamento
- Realize uma revisão final das ferramentas de monitoramento e registro, verificando qualquer atividade incomum ou não autorizada associada às contas e sistemas do colaborador em desligamento.
- Considere a implementação de uma solução de prevenção contra perda de dados (DLP) para identificar acessos não autorizados a dispositivos ou dados durante ou após o desligamento.

4. Procedimentos do último dia:



- Garanta que a conclusão da entrega do hardware.
- Bloqueie as contas do colaborador, evitando acesso posterior.
- Execute uma limpeza segura dos dispositivos do colaborador para a remoção dos dados da empresa.

Sobre a ESET

Defesa proativa. O nosso foco é restringir a superfície de ataque.

Antecipe-se contra ciberameaças conhecidas e emergentes com nossa abordagem preventiva, impulsionada por inteligência artificial e expertise humana.

Experimente a melhor proteção da categoria com a nossa inteligência contra ciberameaças global, compilada e examinada por mais de 30 anos, que impulsiona nossa extensa rede de P&D, liderada por pesquisadores aclamados no setor. A ESET garante a proteção do seu negócio para você aproveitar todo o potencial da tecnologia.

SAIBA MAIS

ESET®
Digital Security
Progress. Protected.