Política de BYOD - Uso de dispositivos móveis

Última atualização	28 de fevereiro de 2023

Esta política busca trazer instruções para o uso apropriado de dispositivos móveis no GRUPO G&E, no intuito de minimizar os riscos envolvidos em sua utilização e atender às legislações, em especial a Lei Geral de Proteção de Dados, normas e boas práticas recomendadas.

Esta política se aplica a todos os colaboradores do GRUPO G&E, quais sejam, funcionários, estagiários, menores aprendizes, prestadores de serviços ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações do GRUPO G&E. Todos esses colaboradores serão tratados nesta política como usuários.

DIRETRIZES DE USO DOS DISPOSITIVOS MÓVEIS

1.1.Usuários com dispositivos móveis corporativos

- **O equipamento está sujeito à monitoramento e inspeção física por parte da empresa;**
- **O equipamento está sendo colocado à disposição do usuário como beneficiário de uso temporário;**
- **Em caso de perda, deterioração, furto, extravio, quebra do equipamento, o usuário deverá avisar à empresa imediatamente.**

a) Devem ser estabelecidos procedimentos para concessão de dispositivos móveis, ainda que temporária, contemplando prazos de utilização e responsabilidade no uso;

a.1) Há termo para entrega de computadores e celulares;

b) O Grupo G&E dispõe de equipamentos móveis em quantidade limitada, de forma que a solicitação deve ser realizada após o desligamento do funcionário e indicando o responsável pelo uso do ativo;

c) Os dispositivos móveis corporativos devem ser concedidos pelo GRUPO G&E, em conformidade com as necessidades funcionais do trabalho;

d) Todos os notebooks disponibilizados pelo GRUPO G&E devem ser vinculados à rede com sistema operacional padrão, antivírus e softwares devidamente licenciados.

e) Os dispositivos móveis disponibilizados pelo GRUPO G&E só poderão ser utilizados única e exclusivamente pelos usuários que assumiram a responsabilidade pelo seu uso, conforme procedimento de concessão de dispositivos móveis;

f) Caso o colaborador ligado ao GRUPO G&E tenha dispositivo móvel sob sua responsabilidade e seja desligado ou remanejado, o gestor da área ou superior deve comunicar à área de T.I, para os procedimentos necessários;

g) Os usuários não possuem permissão para instalar aplicativos de fontes desconhecidas e aplicativos não autorizados ou alterar configurações de segurança nos dispositivos móveis, os aplicativos essenciais e permitidos para os celulares corporativos são; Aplicações nativas do celular, Whats App, Aplicativos fornecidos pelo Grupo G&E.

h) Os acessos dos usuários, bem como dos dispositivos às conexões de rede e recursos disponíveis devem ter mecanismos de concessão, alteração e cancelamento de acesso, conforme Política de Uso de Senhas.

i) Cabe ao usuário do equipamento à manutenção e guarda do mesmo, bem como responsabilidade pelo conteúdo armazenado;

j) Em relação aos aparelhos móveis a realização de backups é de responsabilidade do usuário e seguirá o disposto na Política de Segurança da Informação.

1.2. Visitantes com dispositivos móveis

a) Os dispositivos móveis não corporativos só poderão ter acesso à rede de visitantes;

b) Deve ser observado o procedimento para concessão e controle de acesso a visitantes que, durante a permanência em instalações do GRUPO G&E, necessitem conectar seus dispositivos móveis à internet;

c) A concessão de acesso à rede de visitantes deve estar associada à conscientização das regras internas de uso da rede.

1.3. Dispositivos móveis removíveis de armazenamento

a) É proibida a utilização de dispositivos móveis removíveis, como pen drive e HD externo, para armazenar ou copiar informações.

1.4. Proibições

Ficam expressamente proibido:

A. Material de natureza pornográfica, racista, que possa difamar ou caluniar não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede;

B. Tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta (também conhecido como "cracking"). Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes;
C. Tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques do tipo "negativa de acesso", provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "quebrar" (invadir) um servidor;

D. Usar de qualquer tipo de programa ou comando designado a interferir com a cessão de usuários. Exceto a TI para fins de suporte ou auditoria;

E. Softwares de comunicação instantânea, mensageiros, Messenger e afins, exceto a TI usando como ferramenta de trabalho.

F. Utilização de softwares de peer-to-peer (P2P), torrents, Kazaa, Morpheus e afins;

G. Utilização de serviços de streaming, tais como Youtube, Spotify, Netflix, Prime Vídeo e afins;

H. Adição ou remoção de qualquer dispositivo seja ele pen-drives, impressoras, ou outros dispositivos nas estações de trabalho sem prévia autorização;

I. Utilizar quaisquer recursos ou equipamentos da Empresa para fins diversos daqueles necessários ao desempenho da função contratada;

J. Acessar, copiar ou armazenar programas de computador ou qualquer outro material - músicas, fotos, vídeos, documentos - que violem a lei de direitos autorais (copyright);

K. Utilizar os recursos computacionais de propriedade da Empresa, colocado a disposição do colaborador em razão do exercício de sua função, para constranger, assediar, prejudicar, ou ameaçar a mesma ou a terceiros, sejam eles indivíduos ou organização;

L. Alterar os sistemas padrões sem autorização;

M. Divulgar quaisquer informações confidenciais para concorrentes e/ou qualquer pessoa não ligada às atividades da Empresa;

N. Efetuar qualquer tipo de acesso ou alteração não autorizada a dados dos recursos computacionais pertencentes à Empresa;

O. Criar Blogs e comunidades na internet, ou qualquer ambiente virtual semelhante, utilizando-se, sem autorização expressa, da logomarca da empresa;

P. Executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, leitura de dados de terceiros, a propagação de vírus de

computador, a destruição parcial ou total de arquivos ou indisponibilização de serviços;

Q. Instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da Empresa;

R. Usar recursos computacionais de natureza particular nas intermediações da empresa, tais como notebooks, etc.

1.5. Medidas de segurança e boas práticas

A. Evitar o uso de redes públicas;
B. Recomenda-se manter as conexões de comunicação, como bluetooth, desabilitadas e somente habilitar quando for necessário;
C. Ao trafegar com dispositivos móveis, sugere-se que estes sejam devidamente protegidos, guardados em locais seguros ou não expostos, como, por exemplo, na mala do carro;
D. Proteger o dispositivo com senha de acordo com a política de segurança da informação;
E. Atualizar software regularmente;
F. Instalar aplicativos que ofereçam medidas de segurança
G. Realizar cópias de segurança dos dados;
H. Não baixar aplicativos desconhecidos ou que não forneçam níveis adequados de segurança;
I. Não permitir que outras pessoas tenham acesso ao dispositivo;
J. Não compartilhar dados pessoais indevidamente;
K. Atualização automática dos aplicativos do telefone móvel;
L. Não permitir instalação de de aplicativos de fontes desconhecidas;
M. Não permitir o preenchimento automático dos códigos recebidos por SMS a partir das opções de desenvolvedor do Android, ou pelas configurações da conta Google;
N. Ativar o bloqueio instantâneo de tela, no botão liga/desliga;
O. Ative a autenticação de dois fatores para aplicativos ou sites que a suportam;
P. Desative as lojas de aplicativos de terceiros, que podem ser vetores para a propagação de malwares;
Q. Exclua periodicamente os aplicativos que não são usados ou não são mais necessários;
R. Limite as informações de identificação pessoal armazenadas em aplicativos;
S. Defina privilégios mínimos nos aplicativos instalados;
T. Permita que um aplicativo acesse sua localização apenas durante seu uso;

U. Apenas ative Bluetooth, NFC, Wi-Fi, ou GPS quando for necessário;
V. Use apenas carregadores e cabos confiáveis, evitando a utilização de carregadores do tipo USB públicos;
W. Habilite a função de localização de dispositivo perdido; e
X. Verifique a legitimidade de um e-mail antes de abrir um anexo ou clicar em links.

1.6. Responsabilidades e penalidades

Aquele que incorrer em descumprimento desta política poderá ser responsabilizado por perdas e danos, além de outras penalidades previstas contratualmente.