Política de Segurança Cibernética

Versão v0.1

13 de outubro de 2022

Sumário

1. Introdução

A informação é um importante ativo na execução das atividades corporativas. Isso faz com que ela se torne alvo constante de ameaças internas e externas. Esta crescente ameaça é um dos principais fatores de risco não financeiros ao negócio. Portanto, a proteção dos dados é um componente essencial ao Grupo Virgo.

A segurança cibernética visa implementar métodos, procedimentos, orientações e ferramentas, buscando aumentar o nível de proteção de tais dados, que são tão essenciais como parte de nosso fluxo operacional, além de um forte diferencial competitivo.

2. Objetivo

A presente Política de Segurança Cibernética ("Política") tem por objetivo a manutenção e segurança das informações sigilosas compartilhadas com os sócios, empregados, diretores, colaboradores e funcionários ("Colaboradores") do Grupo Virgo.

3. Abrangência

Esta Política tem abrangência ampla e contempla toda a coleta e/ou tratamento de informações obtidas através dos diversos canais do Grupo Virgo, bem como dados compartilhados por parceiros, clientes, fornecedores e prestadores de serviços.

4. Documentação e regulamentação relacionada:

Esta política se baseia nos seguintes documentos:

- Ética e valores dispostos no Código de Ética e Conduta do Grupo Virgo
- Código ANBIMA para Ofertas Públicas
- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados)
- Resolução CVM nº 60, de 23 de dezembro de 2021

5. Sigilo e conduta

Nenhuma informação confidencial ou sigilosa deve, em qualquer hipótese, ser compartilhada fora do Grupo Virgo.

É vedada, seja em âmbito pessoal ou profissional, qualquer divulgação que não esteja de acordo com as normas legais ou ainda com a presente Política.

É obrigação de todos os Colaboradores manter o sigilo das informações a que teve acesso em decorrência das atividades desenvolvidas no Grupo Virgo, tendo ciência de sua natureza privilegiada e confidencial, de forma a não as divulgar a terceiros sem consentimento prévio do Diretor de Compliance ou ainda se o terceiro tiver dever de confidencialidade perante o Grupo Virgo.

As proibições estabelecidas nesta Política permanecerão aplicáveis, inclusive, após o término do vínculo do Colaborador com o Grupo Virgo até que a Informação Confidencial venha a conhecimento do público em geral de qualquer outra forma que não através da divulgação do Colaborador.

São consideradas informações confidenciais ("Informações Confidenciais"), independente dos meios que as contenham ou pelos quais foram obtidas, seja em Hard Drives, Pen-drives, e-mails e ainda escritas, verbais ou apresentadas de modo tangível ou intangível, quaisquer informações do Grupo Virgo, seus clientes, sócios, parceiros e incluindo ainda, mas não se limitando a:

- know-how, técnicas, modelos, protótipos, códigos, programas de fórmulas, amostras;
- informações protegidas por sigilo bancário, de natureza operacional, financeira, administrativa, comerciais, contábil, a exemplo dos resultados financeiros antes da sua publicação, jurídica, processos;
- projetos, conceitos de produto, especificações, amostras de ideia;
- clientes, definições, informações mercadológicas, invenções e ideias, outras informações técnicas e demais documentos e informações;
- transações realizadas que tenham sido divulgadas ao público em geral;
- quaisquer informações obtidas junto aos Colaboradores do Grupo Virgo, ou ainda de seus representantes, clientes, fornecedores, prestadores de serviços, consultores ou assessores.

A divulgação de informações protegidas por sigilo bancário, como por exemplo a posição de investidores, será limitada a pessoas que tenham real necessidade de conhecê-las, vedada a sua divulgação, exceto quando necessário para fins regulatórios ou em razão de obrigação legal.

5.1. EXCEÇÕES

A divulgação de Informações Confidenciais sobre quaisquer clientes, ex-clientes, parceiros e ex-parceiros só poderá ser feita mediante a autorização do Diretor de Compliance, com a finalidadede instruir sobre a sua correta divulgação.

Qualquer Colaborador que acredite que qualquer Informação Confidencial foi obtida ou divulgada de forma a contrariar as disposições desta Política deverá notificar o Diretor de Compliance.

O Colaborador não deverá utilizar ou divulgar posteriormente a informação, a menos que, e até ser notificado pelo Diretor de Compliance.

5.2. DIVULGAÇÃO MEDIANTE AUTORIZAÇÃO DO TITULAR DA INFORMAÇÃO

Informações Confidenciais podem ser divulgadas a terceiros desde que mediante o consentimento do titular da informação, ou de acordo com as instruções a serem fornecidas diretamente pelo titular da informação, de forma expressa.

5.3. DIVULGAÇÃO PARA OUTROS COLABORADORES

As Informações Confidenciais poderão ser divulgadas pelos Colaboradores a outros Colaboradores que necessitem ter acesso a tais Informações Confidenciais em razão das atividades exercidas no Grupo Virgo.

5.4. Divulgação para terceiros

As Informações Confidenciais poderão ser divulgadas a parceiros ou prestadores de serviços autorizados, apenas e exclusivamente quando for essencial para a execução da atividade, desde que o parceiro ou prestador de serviço tiver dever de confidencialidade perante o Grupo Virgo.

Quaisquer intermediários financeiros, agente, parceiro ou prestador de serviço terá a obrigação de cumprir as normas de confidencialidade referente às Informações Confidenciais fornecidas pelo Grupo Virgo, utilizando-a única e exclusivamente à execução da atividade acordada.

5.5. Divulgação por determinação legal ou regulatória

Informações Confidenciais também poderão ser divulgadas para o cumprimento de leis, ordens judiciais ou ainda de obrigações regulatórias, sendo que, neste caso, o Grupo Virgo deverá divulgar apenas a informação a que for obrigada por força de lei, ordem judicial ou obrigação regulatória.

6. Segurança cibernética e proteção de dados

6.1. Objetivos de segurança cibernética e proteção de dados

6.1.1. Confidencialidade

Garantir o acesso aos documentos estritamente a quem os necessita, sempre respeitando a política do menor acesso.

6.1.2. Integridade

Garantir a exatidão e preservação dos documentos sem alterações indevidas (acidentais ou não).

6.1.3. Disponibilidade

Os dados devem estar acessíveis aos Colaboradores sempre que necessários, podendo consultá-los a qualquer momento.

6.2. Identificação de usuários para redes e computadores

A identificação de usuário (“Identificação de Usuário”) para o acesso de recursos de informática do Grupo Virgo é privilégio concedido a todos os Colaboradores, sendo seu acesso segregado de acordo com as atividades exercidas no Grupo Virgo.

Cada indivíduo autorizado a acessar os sistemas do Grupo Virgo receberá uma Identificação de Usuário, que não deverá ser compartilhada com nenhuma outra pessoa, seja Colaborador ou não, que será imediatamente desativada mediante notificação do encerramento do vínculo do indivíduo com o Grupo Virgo.

São utilizadas senhas, combinadas com Identificações de Usuário, para autenticação de pessoas autorizadas e conferir-lhes acesso aos recursos de informática do Grupo Virgo.

Cada Identificação de Usuário está vinculada a uma senha única e individual, que não deverá ser compartilhada com qualquer outra pessoa, seja Colaborador ou não.

Cada Identificação de Usuário está vinculada a um segundo fator de autenticação, dentre as opções de ligação telefônica, SMS ou aplicativo autenticador, servindo como uma camada extra de proteção ao acesso indevido da conta. Este cadastro deve estar vinculado a um item de posse do colaborador, e não deverá ser compartilhado com qualquer outra pessoa, seja Colaborador ou não.

6.3. TELAS LIMPAS

As estações de trabalho devem ser fisicamente seguras e as sessões abertas devem ser bloqueadas quando deixadas sem supervisão.

As senhas jamais devem ser armazenadas em um sistema de computação, aparelho, ou por escrito de forma desprotegida.

Para evitar o acesso indevido por outros Colaboradores ou terceiros, todos os Colaboradores devem fechar os programas após sua utilização e efetuar o log-off de seus computadores quando ausentar-se por um período prolongado.

6.4. PROTEÇÃO ANTIVÍRUS/ANTIMALWARE

Os servidores do Grupo Virgo são dotados de um sistema automático de antivírus/firewall que atualiza as definições de vírus bem como as definições de segurança do firewall em todos os postos; todos os equipamentos fazem a verificação automática constante contra ameaças.

6.5. RESTRIÇÃO AO USO DE RECURSOS INFORMÁTICOS

Os equipamentos e recursos tecnológicos, seja de *hardware* ou *software*, providos pelo Grupo Virgo têm finalidade exclusiva de conduzir os negócios relativos às atividades desempenhadas pelo Colaborador no Grupo Virgo.

Nenhum hardware ou software (incluindo hardwares e softwares pessoais) não autorizado deverá ser usado, carregado, instalado e/ou ativado em nenhuma estação de trabalho, computador ou sistema de produção ou estágios sem análise e aprovação prévias.

Vai de encontro à esta Política que Colaboradores abusem de quaisquer equipamentos de informática, suprimentos ou instalações para uso pessoal, sendo vedado aos Colaboradores remover qualquer tipo de informações das instalações do Grupo Virgo, a menos que necessário para conduzir as suas atividades desempenhadas no Grupo Virgo.

6.6. AVALIAÇÃO DA POLÍTICA DE USO DA REDE

Com a finalidade de assegurar o cumprimento dos procedimentos mencionados, o Grupo Virgo se reserva o direito de:

- Empregar softwares e sistemas capazes de monitorar e registrar todos os usos do e-mail corporativo e da Internet através da rede de estações de trabalho do Grupo Virgo;
- Inspecionar qualquer arquivo armazenado na rede, no hard drive do computador ou em áreas privadas da rede a fim de assegurar o cumprimento rigoroso desta Política; e
- Manter um conjunto de softwares e hardwares instalados para proteger a rede interna e a integridade de dados e programas.

6.7. Realização de testes periódicos de segurança para sistemas de informação

O Grupo Virgo realiza análise e testes periódicos que têm como objetivo a identificação de eventuais vulnerabilidades técnicas e procedimentais que, por acaso venham a apresentar risco às informações e seus sistemas críticos de negócios.

6.8. Backup

Todos os dados e documentos estão protegidos por vários tipos de cópias de segurança, que devem ser executadas da forma mais automática possível, mitigando erros operacionais. Os dados periodicamente precisam ser testados, a fim de evitar problemas durante uma necessidade de recuperação futura. O ciclo de dados destes backups também precisará ser revisado periodicamente, visando a eventual eliminação de dados obsoletos.

As proteções são divididas em:

- Lixeiras:
  Permitem a rápida recuperação de deleção acidental de documentos
- Versionamento:
  Guarda múltiplas versões de cada documento, visando a recuperação de versões anteriores por sobrescrita acidental
- Arquivo morto:
  Local especial para guarda de longa duração de documentos para atendimento regulatório, com maior nível de restrição de acesso
- Backup externo:
  Gera cópias externas aos produtos onde os dados são gerados, sendo uma camada extra de proteção contra o sequestro de dados (“Ransomware”) ou vandalismo em massa dos repositórios de documentos

6.9. VPN

O Grupo Virgo fornece uma VPN de acesso exclusivo aos Colaboradores, visando o acesso a rede restrita da empresa fora do ambiente físico do escritório. Seu acesso é pessoal e atrelado a sua Identificação de Usuário. O acesso a VPN não deve ser compartilhado com ninguém, seja Colaborador ou não.

6.10. Gerência de ponto de extremidade

Os laptops do Grupo Virgo possuem aplicativo de gerência de ponto de extremidade (“MDM”), visando aplicar e manter as proteções descritas neste documento. Os seguintes benefícios estão atrelados ao uso do MDM:

- Criptografia completa do disco rígido
- Ativação e atualização constante do antivírus/antimalware/firewall nativo
- Atualizações de segurança do sistema operacional
- Bloqueio de tela automático em caso de inatividade
- Configurações automáticas dos navegadores nativos
- Coleta estatística de uso de software

7. Tratamento de incidentes de segurança cibernética

Os incidentes ou suspeitas identificadas pelos Colaboradores devem ser comunicados através ao time de Segurança Cibernética ou Infraestrutura Tech. Todos os incidentes confirmados devem ser comunicados ao Diretor de Compliance, a fim de informar todos os interessados de maneira adequada e aderente as obrigações regulatórias.

Todos os casos confirmados devem ser registrados em um diário de incidentes, tornando o processo catalogável e consultável no futuro.

Em caso de interrupção de serviços com impacto significativo e/ou risco grave, um Plano de Recuperação de Desastre deverá ser apresentado assim que possível.

8. Violação

Nos casos em que houver violação desta Política, sanções disciplinares e/ou legais poderão ser adotadas, sem prévio aviso, de acordo com o caso. Isso independe de ter auferido ou não qualquer benefício ao infrator através da violação.

O infrator poderá ser notificado e a ocorrência do incidente poderá ser comunicada a seus gestores e diretoria.

9. Vigência

Esta política entra em vigência na data de sua aprovação.

10. Versões

ALTERAÇÕES	
Data da Publicação	**Alterações**
13/10/2022	Publicação Inicial