MANUAL DE SEGURANÇA CIBERNÉTICA *(COMPLIANCE* E GESTÃO DE RISCO*)*

Versão	Atualizada em	Responsável:
1	Janeiro/2019	Frederico Bernardo Mesnik
2	Agosto/2019	Frederico Bernardo Mesnik
3	Abril/2021	Frederico Bernardo Mesnik
4	Junho/2021	Arthur Meier Mesnik
5	Janeiro/2022	Arthur Meier Mesnik

1. INTRODUÇÃO E OBJETIVO

O presente Manual de Segurança Cibernética tem como objetivo estabelecer práticas da TRÍGONO CAPITAL LTDA. ("Trígono") aderentes ao Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros e ao Código ANBIMA de Melhores Práticas para Distribuição de Produtos de Investimento e suas respectivas diretrizes e deliberações.

Esse Manual de Segurança Cibernética foi elaborado seguindo o Guia de Cibersegurança ANBIMA para atender especificamente às atividades desempenhadas pela Trígono, de acordo com natureza, complexidade e riscos a elas inerentes, observada a obrigação de revisão e atualização periódica.

A Trígono contrata a empresa FWSTORE Comércio eletrônico de informática (Witec) para o fornecimento de sua infraestrutura de tecnologia da informação.

2. SEGURANÇA CIBERNÉTICA

2.1. Avaliação de Riscos

Os principais riscos identificados pela Trígono como ameaças cibernéticas são:

i. Acesso indevido a pastas, documentos internos, restritos e/ou sigilosos;
ii. Acesso indevido a informações de clientes e/ou potenciais clientes;
iii. Acesso indevido a propriedade intelectual, metodologias e planos de negócios;
iv. Acesso indevido a lista de usuários e quebra de senhas de sistemas;
v. Manipulação e/ou adulteração de informações;
vi. Sabotagem com a finalidade de corromper e/ou tornar indisponível totalmente ou parcialmente o ambiente de tecnologia.

2.2. Recursos Relevantes

i. Armazenamento de arquivos em nuvem (*File Server* Office 365 Business Standard);
ii. Versionamento e retenção de arquivos (histórico de versões de arquivos em nuvem);
iii. Antivirus – BitDefender;
iv. Firewall Watchgard;
v. Switches de distribuição e Wireless;
vi. Controles de Acesso;
vii. Nobreaks;
viii. PABX IP 3CX;
ix. Um servidor físico na plataforma Windows Server 2019;
x. Estações de trabalho na plataforma Windows 10 Pro;
xi. Suite Microsoft 365 para sistema de e-mail, colaboração e aplicações de área de trabalho;
xii. Links de Internet;
    1. LINK MUNDIVOX – Dedicado – IP Estático
    2. LINK HOSTFIBER Dedicado – IP Estático
    3. LINK VIVO – IP Dinâmico

2.3. Ações de Prevenção e Proteção

i. O Firewall Watchguard está devidamente funcional e com os sistemas de proteção de borda ativos;
ii. Servidores e estações de trabalho atualizados com as últimas versões do fabricante;
iii. Versionamento de arquivos (armazenamento com número definido em em 500 versões);
iv. Retenção de Dados – Sistema Dropsuite que recupera arquivos excluídos;
v. Equipamentos com antivírus Bitdefender ativo, integrado com o software RMM de gerenciamento/alerta/automação utilizado nos servidores e estações de trabalho;
vi. Criptografia de discos – Bitlocker;
vii. Sistema operacional dos servidores com acesso restrito ao administrador e sem navegação;

viii. Usuários sem acesso administrativo no equipamento, evitando assim instalação de software indesejado;
ix. Dados salvos diretamente na nuvem do Office 365, onde é aplicada a rotina de retenção e versionamento;
x. Sistema de rede wireless acessado através de software específico para gerenciamento/monitoramento;
xi. Rede sem fio com criptografia;
xii. Pacote Microsoft Office 365 configurado e ativo com as melhores práticas para a ferramenta, protegendo o ambiente de ameaças cibernéticas;
xiii. Duplo fator de autenticação (MFA) para acesso ao ambiente em nuvem Office 365.

2.4. Monitoramento e Testes

i. Monitoramento do ambiente tecnológico permanente;
ii. No caso de falha em um link de internet, o link de redundância é ativado automaticamente;
iii. Trimestralmente é verificado se há novo firmware para o firewall, com avaliação das correções e o impacto na sua atualização;
iv. Itens monitorados pelo software RMM:
   - Atualizações do sistema operacional;
   - Atualização/alerta do antivírus;
   - Condições técnicas do equipamento com dispositivo de alerta para Witec;
   - Atualização de *software* de terceiros.
v. Integração do antivírus com o console de gestão da Witec, onde é monitorado diariamente situações de ataques e/ou infecção;
vi. Envio de e-mail de alerta para Witec pela plataforma do Microsoft Office 365 em caso de anormalidade.

2.5. Plano de Resposta

Está descrito no Plano de Continuidade de Negócios, contido no Manual de Controles Internos da Trígono.

2.6. Reciclagem e Revisão

i. A Witec é notificada quando há necessidade de inserir no ambiente tecnológico um novo dispositivo. Nesse caso é avaliado o impacto e adotadas as ações necessárias para uma instalação segura;

ii. As ações de prevenção a falhas são constantes devido ao monitoramento online;

iii. As atualizações de software são previamente analisadas para uma instalação segura;

iv. A Witec está atualizada e sempre em contato com fabricantes para monitorar as vulnerabilidades dos produtos utilizados pela Trigono.

2.7. Responsável dentro da Trígono

Felipe Mendes Batista
fbatista@trigonocapital.com
11 4780-0180

3. Atualização

A Trígono deve atualizar o presente manual em prazo não superior a doze meses, ou quando houver alteração na Regulação referente a segurança cibernética.

*****