ANEXO

1. FERRAMENTAS DE PROTEÇÃO, VARREDURAS, PATCHES, BACKUP E ETIQUETAGEM DE E-MAILS

A Cy Capital deverá manter mecanismos de proteção destinados a evitar e detectar conexões não autorizadas, incursões maliciosas e demais eventos que possam comprometer seus ativos cibernéticos, inclusive por meio da utilização de firewall, softwares de proteção contra malware e antivírus atualizados.

Serão conduzidas varreduras periódicas para detectar e limpar programas que venham a obter acesso a dispositivos da rede da Cy Capital, cabendo ao Diretor de Compliance e PLD supervisionar tais rotinas e definir, conforme necessário, os parâmetros aplicáveis à sua execução.

A Cy Capital deverá manter plano de manutenção destinado a resguardar seus dispositivos e softwares contra vulnerabilidades, inclusive com a aplicação regular de correções, atualizações de segurança e patches nos sistemas utilizados.

A Cy Capital manterá e testará regularmente medidas de backup consideradas apropriadas pelo Diretor de Compliance e PLD, observadas as premissas operacionais previstas na política principal e a necessidade de armazenamento em ambiente seguro e monitorado.

Caso a Cy Capital utilize sistema de análise e etiquetagem de e-mails, as mensagens eletrônicas poderão ser analisadas com base em critérios de segurança da informação, inclusive para identificação de phishing, malware, conteúdo não autorizado ou outras ameaças cibernéticas, podendo ser classificadas conforme sua criticidade e relevância. Os Colaboradores deverão observar as etiquetas, alertas e orientações de segurança aplicáveis e comunicar imediatamente ao Diretor de Compliance e PLD qualquer e-mail suspeito ou potencialmente comprometedor.

2. MONITORAMENTO E TESTES

O Diretor de Compliance e PLD, ou pessoa por ele incumbida, poderá adotar medidas de monitoramento dos sistemas, comunicações e ferramentas de trabalho da Cy Capital com o objetivo de detectar acessos não autorizados, violações potenciais, uso indevido dos recursos tecnológicos e descumprimento das diretrizes internas de segurança da informação.

Sem prejuízo dos testes periódicos previstos na política principal, a Cy Capital realizará, em base no mínimo semestral e por amostragem, verificações relacionadas ao uso de e-mails, internet, aplicativos, ligações telefônicas corporativas, bem como às informações de acesso ao espaço físico do escritório, desktops, pastas e sistemas, conforme aplicável.

O Diretor de Compliance e PLD poderá adotar medidas adicionais de monitoramento e supervisão sempre que julgar oportuno e necessário para avaliar o cumprimento e a eficácia dos controles de segurança da informação e cibersegurança da Cy Capital.

3. PLANO DE IDENTIFICAÇÃO E RESPOSTA A INCIDENTES

Qualquer suspeita de infecção, acesso não autorizado, comprometimento da rede ou dos dispositivos da Cy Capital, bem como qualquer vazamento efetivo ou potencial de informações, deverá ser prontamente comunicada ao Diretor de Compliance e PLD.

Uma vez reportado o incidente, caberá ao Diretor de Compliance e PLD coordenar a avaliação do evento, inclusive para:

I. avaliar o tipo de incidente ocorrido, as informações acessadas e a extensão da respectiva perda;
II. identificar quais sistemas, se houver, deverão ser desconectados, desabilitados ou submetidos a medidas de contenção;
III. definir os papéis e responsabilidades dos envolvidos no tratamento do incidente;
IV. avaliar a necessidade de recuperação e/ou restauração dos serviços afetados;
V. avaliar a necessidade de notificação das partes internas e externas cabíveis, conforme a natureza do incidente;
VI. avaliar a necessidade de divulgação ao mercado, reguladores, clientes, investidores ou demais terceiros, quando aplicável; e
VII. definir, após a condução da investigação e a avaliação das circunstâncias do caso, a responsabilidade pelas perdas eventualmente decorrentes do incidente.

Os incidentes deverão ser registrados internamente, com a descrição do evento, das providências adotadas e das medidas corretivas e preventivas definidas para evitar recorrência.