Resumo: Politica de Segurança Cibernetica

ED&F MAN Capital Markets Distribuidora de Títulos e Valores Mobiliários Ltda.
("**ED&F MAN DTVM**" ou "**DTVM**")

Sumário

A Área de **Tecnologia** é responsável por toda e qualquer alteração, atualização e divulgação desta politica.

Versao	Autor	Revisado por	Data Aprovacao	Alteracoes
01	Tiago C. Sajben	Danilo Devecchi		Primeira publicao

1. Introdução

Este documento define a Política de Segurança Cibernética ("A Política") nos Departamentos da ED&F MAN DTVM ("A Empresa").

O objetivo da Política é comunicar ao reconhecimento da administração da Empresa que as informações são um ativo que precisa ser gerenciado e mantido de uma maneira que permita que a empresa funcione, ao mesmo tempo em que fornece controles adequadamente robustos para proteger a Empresa e suas afiliadas, parceiros e clientes.

A política visa garantir que exista:

- Confidencialidade adequada das informações, para impedir o acesso não autorizado ou a divulgação de informações que devem permanecer privadas para a ED&F MAN DTVM ou seus clientes.

- Integridade adequada dos ativos de informações para garantir que as informações sejam precisas e sejam modificadas ou apagadas somente por aqueles autorizados a fazê-lo.

- Disponibilidade adequada dos ativos de informação para apoiar as operações comerciais da ED&F MAN DTVM, seus parceiros e a prestação de serviços aos clientes.

2. Gerenciamento de Risco, Governança e Estrutura

A Política baseia-se no entendimento de que as ameaças à segurança cibernética são riscos que precisam ser tratados como parte do processo de gerenciamento de riscos da empresa. Os princípios e as melhores práticas de Gerenciamento de Riscos serão aplicados ao risco de segurança cibernética, assim como são aplicados aos riscos Estratégico, Financeiro, Operacional ou Jurídico.

O risco de segurança cibernética será avaliado com base na probabilidade e no impacto. Probabilidade é definida como a probabilidade de uma ameaça explorar uma vulnerabilidade de afetar adversamente um ativo Confidencialidade, Integridade ou Disponibilidade.

O impacto é definido como o custo - financeiro, reputacional ou não, se um ativo da Empresa for comprometido em: Confidencialidade, Integridade ou disponibilidade.

A Política será supervisionada por pessoal designado na Equipe de TI local e global da Empresa.

A equipe se reunirá conforme indicado abaixo para discutir os seguintes itens:

- Validade da versão atual da Política da Companhia (semestralmente).

- Atualizar itens de ação de correção pendentes para se alinhar aos requisitos atuais da política (semestralmente).

- Atualizar a política com base nos requisitos de melhores praticas de mercado ou do órgão regulador (anualmente).

- Avaliar o ambiente operacional em relação à Política, identifiquar lacunas e determinar um plano de implementação para remediar disparidades operacionais com a Política (anualmente).

a. Estrutura Funcional de Segurança Cibernetica

A estrutura do NIST permite que a DTVM se baseie em uma base de segurança cibernética reconhecida globalmente. A Estrutura Funcional do NIST emprega cinco filosofias funcionais simultâneas e contínuas, promovendo a comunicação da conscientização e transparência da segurança cibernética em toda a organização, do nível executivo ao nível de operações. Esses cinco pilares funcionais incluem o seguinte:

- Identificar (ID)
- Proteger (PR)
- Detectar (DE)
- Responder (RS)
- Recuperar (RC)

3. Identificar: Linha de base do ambiente

O foco desta seção é o desenvolvimento da compreensão estrutural para gerenciar os riscos de segurança cibernética em sistemas, ativos, dados e competências

a. Gerenciamento de ativos: inventário equipamento físico (*Hardware*)

A equipe de Tecnologia de Informacao da DTVM inventariará e manterá dispositivos e sistemas em uma base contínua, usando um banco de dados eletrônico.

b. Gerenciamento de ativos: inventário de sistemas (S*oftware*)

A equipe de TI da DTVM fará inventário e manutenção anual de plataformas de software de sistemas e aplicativos críticos dentro da organização.

c. Classificação de Recursos

Em conjunto com o inventário geral de ativos, particularmente no item b acima, uma classificação geral será aplicada a esses documentos para discernir o valor e a criticidade dos negócios.

d. **Funções e responsabilidades: Força de trabalho de TI**

Uma avaliação das funções e responsabilidades de segurança cibernética para a equipe de TI da DTVM e partes interessadas de terceiros será revisada e atualizada anualmente.

e. Política de Segurança Cibernética

A equipe revisará anualmente a Política para garantir a relevância e fornecer recomendações e definir os objetivos e metas de segurança cibernética do ano seguinte para melhoria contínua.

f. Funções e Responsabilidades: Comitê de Segurança Cibernética

Os membros da equipe do comitê de segurança cibernética da empresa são funcionários da empresa de grupos multifuncionais, como conformidade ou jurídico. Esses membros oferecem conselhos ou orientações com relação a interpretações legais que podem afetar a governança de segurança cibernética da empresa. Em conjunto com a revisão anual da Política, a Equipe também examinará a relevância dos Membros do Comitê de Cibersegurança, com considerações para incluir critérios como pessoas que abandonam o trabalho / junção, mudanças internas de emprego ou conflitos de recursos.

g. **Gerenciamento de Riscos**

A Equipe, em coordenação com a Equipe de Riscos e TI da DTVM, estabelecerá um processo de gerenciamento de riscos que destaca os riscos operacionais relacionados à segurança cibernética. O método no qual relatar e definir itens de ação priorizados para corrigir lacunas será revisado anualmente para garantir a relevância do processo

4. Protecao: Implantacao de Salvaguardas

Esta seção aborda o desenvolvimento e a implementação de soluções seguras e adequadas que garantem a entrega dos serviços críticos globais de Tecnologia da Informação da DTVM.

a. Controle de acesso:

- ambientes lógicos e físicos

b. Revisao de Redes

- Proteção

- Segregações lógicas

- Conectividade Física

c. Sensibilização e Formação

A DTVM garantirá que aqueles com privilégios elevados compreendam a responsabilidade de receber ou possuir privilégios elevados. Isso será conduzido por treinamento interno e direitos elevados serão aprovados pelos gerentes desse usuário.

d. Gerenciamento de Mudanças e Incidentes

A area de TI da DTVM apoiará a governança do gerenciamento de mudanças e incidentes.

e. Integração e manutenção de terceiros

Antes de prestar serviços à DTVM, os fornecedores terceirizados devem declarar ou fazer referência à governança anual de segurança cibernética do terceiro. Além disso, a Equipe revisará anualmente a lista de fornecedores terceirizados que têm acesso aos sistemas de produção usados em todo o inventário do sistema da DTVM.

f. Tecnologia de Proteção

A equipe analisará anualmente as soluções de segurança implementadas pela DTVM para garantir a resiliência dos sistemas e ativos de produção contra ataques cibernéticos.

5. Detectar: Implementação de Identificação de Atividade

Esta seção se concentra no desenvolvimento e implementação de ações apropriadas para reconhecer e aumentar a identificação de ameaças à segurança cibernética.

a. Anomalias e Eventos

b. Monitoracao Continua

c. Processo de Detecção

6. Responder: Itens de ação para violação

Esta seção se concentra no desenvolvimento e implementação das atividades da DTVM/ Empresa em torno de um incidente identificado de segurança cibernética.

a. Plano de Respostas

A equipe emitirá um PRSC (Plano de Resposta de Segurança Cibernética) que poderá incluir a participação da equipe de TI global da empresa, departamento de risco da DTVM, equipe de conformidade e executivos.

b. Comunicações

A empresa procurará empregar várias atividades de resposta que identifiquem ataques cibernéticos, preservem a integridade das informações e protejam a empresa.

Se um evento de segurança cibernética for detectado e as informações forem comprometidas, a comunicação da violação seguirá este procedimento de alto nível para garantir a legitimidade do evento:

- O número do ticket de gerenciamento de incidentes é emitido e os membros de TI validam e respondem ao evento

- O CTO é informado com relatórios detalhados de informações corroboradoras que isolam a área afetada

- O Departamento de Risco ficará ciente do incidente com um nível de ameaça designado

- Equipe de Conformidade e executivos são informados para avaliar a necessidade de comunicação voluntária

c. Análise

Se uma ameaça for identificada e confirmada, a Equipe de segurança cibernética da DTVM, em conjunto com a equipe de TI global da empresa, desempenhará um papel ativo para substanciar ainda mais a ameaça e seu impacto no ambiente de tecnologia da empresa, realizado da seguinte maneira:

- Seguir a prática padrão da empresa de gerenciamento de incidentes

- Examine o impacto do incidente

- Realizar investigação

- Categorizar incidentes com base no impacto do ambiente afetado

d. Remediação e Mitigação

Independentemente do nível de impacto, a Equipe fará o registro, avaliará e acompanhará a correção do incidente. Isso inclui a implementação de quaisquer processos, procedimentos ou recursos necessários para mitigar as vulnerabilidades identificadas. Dependendo dos recursos necessários versus o apetite do risco inerente identificado, a Equipe de segurança cibernética da DTVM pode documentar o risco potencial como um risco aceito.

e. Melhorias nas Acoes de Resposta

A Equipe revisará as atividades de resposta em toda a empresa, particularmente os grupos identificados na Seção 6.b. Esta revisão visa melhorar as ações tomadas durante uma ameaça à segurança cibernética, incorporando a identificação das lições aprendidas e atualizando as estratégias de resposta, quando aplicável.

7. Recuperar: Ação para Manter e Restaurar

Esta seção aborda o desenvolvimento e a implementação de atividades adequadas para manter as operações e restaurar os serviços prejudicados devido a um incidente identificado e confirmado.

a. Plano de Recuperação

Se o incidente de segurança cibernética estiver afetando diretamente um ambiente de produção (PROD), será avaliada o nivel de gravidade do ambiente de PROD afetado. O nivel de gravidade determinará as ações de recuperação necessárias:

- Alto: O PCN da empresa e / ou do sistema (quando disponível) são engajados para restaurar as operações de um sistema. As atividades serao coordenadas pelo Gestor de Crise da DTVM.

- Medio: os membros de TI da DTVM farão alterações isoladas no ambiente para reduzir a lacuna imediata.

- Baixo: Os membros de TI da DTVM implementarão uma alteração intra-semana no ambiente afetado após o fechamento dos negócios.

b. Melhorias na recuperação

A equipe revisará anualmente o plano de resposta à segurança cibernética da DTVM, revisando os incidentes de segurança cibernética do ano anterior, as tendências do setor e as diretrizes regulamentares. O planejamento de recuperação da empresa na seção 7. será atualizado e compartilhado entre os vários departamentos da DTVM.

c. Comunicação

A DTVM empregará um método de comunicação em que as atividades de restauração são coordenadas com partes internas e externas, incluindo fornecedores externos, quando aplicável. Se um alto nível de informação for comprometido, envolvendo informações confidenciais de funcionários ou clientes, será tomada uma decisão no nível executivo em relação ao canal e formato adequados de qualquer comunicação distribuída aos usuários impactados e / ou funcionários internos para garantir transparência e manutenção da reputação da DTVM.

8. Manutenção de política

A equipe se reunirá anualmente para discutir melhorias na política, bem como a preparação para segurança cibernética da DTVM.

Visando a melhoria contínua a equipe entregará um relatório, fornecendo uma descrição objetiva que será usada para descrever uma visao atual e uma visao alvo dos objetivos e controles de Segurança Cibernética da DTVM, com base na política descrita acima.

Os objetivos da avaliação são:

- Revelar lacunas nos objetivos de segurança cibernética da DTVM,
- Produzir uma lista para avaliar a prioridade da correção e
- Definir um roteiro para as iniciativas de segurança cibernética do ano seguinte.

9. Resumo e Melhoria Contínua

Após cada reunião anual, a equipe compilará um resumo representando o estado atual da da Seguranca Cibernetica da DTVM.

a. Resumo da Avaliação

Os resumos incluirão as exposições conhecidas à Seguranca Cibernetica da DTVM, representando o status de vulnerabilidades pendentes e os respectivos esforços de mitigação. O resumo também incluirá uma avaliação visual da estrutura de segurança cibernética adotada, os padrões da empresa e ferramentas ou processos corroboradores usados em toda a organização que apoiam os esforços.

b. Melhoria continua

Os esforços em torno das informações geradas na Seção 9.a permitirão à equipe de Segurança Cibernética da DTVM inventariar e priorizar os esforços de remediação de Segurança Cibernética e estabelecer metas para os projetos de mitigação do ano seguinte.