Name of the Employee / Nome do Funcionário(a):
Date / Data:
Area / Área:
Eu reconheço que li, entendi e aceitei a presente Política, que não foram feitas promessas ou declarações não mencionadas nesta Política para me induzir a assiná-la, e que assinei e contratei de maneira voluntária. _____ Assinatura

POLÍTICA

MONITORAMENTO DA SEGURANÇA DA INFORMAÇÃO

REVISÃO		PÁGINAS ALTERADAS	ÁREA RESPONSÁVEL	DESCRIÇÃO DA ALTERAÇÃO
Nº	DATA			
01	08/02/18	-	TI	Publicação
02	29/05/19	-	TI	Revisão

Esta Política será revisada a cada 24 (vinte e quatro) meses ou sempre que houver alguma alteração na diretriz descrita.

1. OBJETIVO

Esta política tem como objetivo definir o ambiente, diretrizes e as circunstâncias nas quais as atividades de Monitoramento de Sistemas de Rede, Sistemas de Dados e Comunicações serão realizadas.

2. ABRANGÊNCIA

Esta política abrange todas as empresas do Grupo StoneX, sediadas no Brasil e Paraguai.

3. LEGISLAÇÃO RELACIONADA

- Resolução Nº 4.658/18 do BACEN
- Política de Gestão de Incidentes de Segurança da Informação (POL-052)
- Cadeia de Valor de Serviços Relevantes (BCAM e DTVM)
- Política de Privacidade de Dados (POL-054)

4. DEFINIÇÕES

4.1. SIGLAS & TERMINOLOGIA

4.1.1. BACEN – Banco Central do Brasil

4.1.1.1. TI – Tecnologia da Informação, também conhecido, em inglês, como “IT”

4.2. ÁREAS ENVOLVIDAS NO PROCESSO

4.2.1. Área Responsável

4.2.1.1. Chefe de Global de TI

4.2.1.2. Gerente Global de Operações de TI

4.2.2. Áreas Suporte

4.2.2.1. Administradores do Sistema

4.2.2.2. Gerentes de Outros Departamentos

5. DISPOSIÇÕES

Esta política inclui computadores de propriedade da StoneX utilizados por funcionários em suas residências e que estão conectados à rede da StoneX, incluindo redes Wireless. Também se aplica a prestadores de serviço ou parceiros comerciais licenciados diretamente ligados a StoneX. Prestadores de serviço ou parceiros comerciais serão monitorados para o cumprimento dos termos da sua licença e a respeito das políticas de uso aceitável da StoneX.

5.1. DIRETRIZES

5.1.1. As pessoas autorizadas podem monitorar e analisar serviços de rede, sistemas, dados (incluindo sistemas de arquivos), aplicativos e instalações de comunicação de dados pertencentes à StoneX, ao cliente e às funções administrativas;

5.1.2. StoneX, tem o direito de examinar qualquer arquivo que esteja alocado em servidores ou estações de trabalho de propriedade da StoneX ou mesmo serviços de rede, instalações.

5.1.3. Os usuários devem ser informados de que a utilização dos serviços na StoneX, como comunicação de dados, serviços de infraestrutura, sistemas e aplicações podem ser monitorados por pessoas autorizadas conforme permitido pelas leis e legislação local e internacionais vigentes, e estabelecido na Política de Privacidade de Dados.

5.1.4. Serviços e Aplicações de Rede - Todos os sistemas em rede que fornecem serviços de rede ou aplicativos devem ser monitorados, quando relevantes (vide Cadeia de Valor de Serviços Relevantes), com relação a:

- Armazenamento de arquivo - utilização, tipos e tamanhos de arquivo;
- Violações de software licenciado;

- Estatísticas de rede, como por exemplo, erros e utilização média e máxima da largura de banda;
- Anomalias de log do sistema e de segurança;
- Tentativas de acesso bem-sucedidas - conta do usuário, data/hora, duração da sessão;
- Tentativas de acesso malsucedidas;
- Tráfego de rede.
- Registro e reporte de incidentes

5.1.5. Monitoramento Físico - Em locais que a empresa instalou câmeras de segurança, as gravações dessas áreas devem ser armazenadas por um período mínimo de três semanas, no entanto, se houver um reporte de incidente sobre investigação, as gravações serão mantidas durante o tempo necessário para ajudar a resolver o incidente. Demais medidas incluem:

- Proibição do acesso de terceiros ao armário de cada funcionário, sendo o acesso à documentos limitado apenas aos colaboradores autorizados para tal;
- As impressões enviadas são protegidas por senha e, impressões contendo assuntos restritos, devem ser prontamente retiradas das impressoras e o descarte destes documentos devem ser realizados através de trituradores;
- Manutenção constante do estoque de folhas dentro das impressoras, evitando o truncamento de impressões que podem ser recolhidas por pessoas não autorizadas;
- Laptops devem ser travados com cabos de bloqueio ou trancados em gaveta.

5.1.6. E-mail - Todos os e-mails de entrada processados pelo sistema central devem estar sujeitos ao seguinte:

- Medidas de prevenção de vírus;

- Medidas de prevenção de spams;
- O encaminhamento não autorizado de mensagens é proibido.

Os logs de correio eletrônico devem ser usados para acompanhar problemas relatados ao Chefe de Sistemas de Dados. Os logs são mantidos por por 7 anos. Os logs devem conter as seguintes informações:

- Registro de data e hora, endereço de e-mail do remetente e endereço de IP do sistema de correio eletrônico, endereço de e-mail do destinatário e endereço de IP do sistema de e-mail, id e tamanho da mensagem.
- Determinadas informações do protocolo SMTP, associadas aos diálogos SMTP inicial e final.

5.1.7. Acesso WEB - O controle de acesso a páginas Web deve ser realizado pelo aplicativo interno, tendo todo o trafego de páginas Webinspecionado através deste aplicativo.

5.1.8. Monitoramento de Rede - O tráfego de entrada da Internet está sujeito as seguintes restrições implementadas nos firewalls que conectam à rede da StoneX:

- Portas especificas IP, que estão associadas com os serviços que apresentam serias vulnerabilidades, são bloqueados;
- A lista atual de bloqueio de porta é derivada de conhecimentos locais, experiências e pelo conselho nacional CERT-BR;
- Alguns filtros são utilizados para bloquear endereços específicos seguindo as devidas solicitações;
- Os logs devem gravar determinados campos de IP e dados, ou seja, endereço IP de origem, endereço IP de destino, números das portas, volume e carimbo do tempo. Devido a considerações de espaço em disco, os arquivos de log são armazenados por um período máximo de 7 dias.

Os firewalls de fronteira da StoneX, Inc. mantém informações abrangentes sobre a rede, disponíveis para as seguintes finalidades:

- Investigações de falhas;
- Processamento de Incidentes;
- Perfil de tráfego;
- Alerta sobre atividades incomuns, como ataques DoS e tráfego potencialmente malicioso.

Os logs não registram o conteúdo dos dados do aplicativo; eles meramente registram alguns campos de IP e dados de volume, ou seja, endereço de IP de origem, endereço de IP de destino, números da porta, volume e registro de data e hora.

5.1.9. Monitoramento de Tráfego - O pessoal autorizado pode monitorar os seguintes aspectos da rede da StoneX, ou de segmentos específicos:

- Protocolos e aplicativos em uso;
- Origens e Destinos - padrões de tráfego;
- Métricas de desempenho;
- Bytes enviados e recebidos por roteador e interface de switch;
- Erros identificados por roteador e interface de switch;
- Condições de falha;
- Em circunstancias excepcionais, ou seja, para ajudar a investigar incidentes ou condições de falha, interações especificas entre endpoints podem ser monitorados e gravados para análise;
- Registros Estatísticos: são mantidos durante o tempo em que sejam considerados úteis, considerando o tempo que o incidente ou falha está ativa, depois serão destruídos.

5.1.10. Sistema de detecção de intrusão - Onde há sistema de detecção de intrusão (IDS) da StoneX, estes devem ser usados para identificar atividades maliciosas, incluindo computadores comprometidos localmente e derivar filtros adicionais de segurança para o roteador. Quando uma assinatura é reconhecida, um evento de log deverá prover detalhes da assinatura,os quais devem ser mantidos por curtos períodos.

5.1.11. Varredura Ativa – O pessoal autorizado poderá realizar varreduras ativas em segmentos de rede para identificar vulnerabilidades e/ou hosts comprometidos. O pessoal autorizado deve exercer a devida diligência ao realizar qualquer atividade de varredura, principalmente:

- Informar os administradores de redes e sistemas responsáveis pelo segmento da atividade de varredura planejada e fornecer o seguinte:

  (i) Cronograma, incluindo tempo e duração das varreduras;

  (ii) Sistemas que executam a varredura (endereços de IP);

  (iii) O objeto da varredura, ou seja, vulnerabilidades a serem testadas.

- Medidas razoáveis para garantir a continuidade da operação ou funcionalidade de qualquer sistema sendo inspecionado;

- Identificar sistemas vulneráveis para os administradores relevantes.

- Os registros de varreduras ativas serão mantidos para ajudar a identificar áreas nas quais ações associadas a outras políticas da StoneX, Inc. podem ser necessárias;

- Os usuários das instalações de acesso a WI-FI para convidados devem estar cientes de que a varredura ativa se aplicaria a qualquer sistema pessoal conectado a essas instalações. Qualquer usuário que considere essa condição inaceitável não deve conectar seu sistema aos recursos de acesso WI-FI para convidados.

5.1.12. Rede GuestNet - Usuários que utilizam a rede Guestnet, poderão passar por uma varredura da rede, mesmo utilizando computadores pessoais ou qualquer sistema ligado as instalações StoneX. Qualquer usuário que não concorde, não deve conectar seu sistema a rede StoneX GuestNet.

5.1.13. Conduta Ética - As pessoas autorizadas, incluindo administradores de rede e administradores de sistemas devem executar suas funções em conformidade com as diretrizes estabelecidas, em especial as pessoas autorizadas devem:

- Respeitar a privacidade dos outros;
- Não usar ou divulgar informações obtidas durante o monitoramento para fins diferentes daqueles para os quais o processo foi aprovado;
- Salvaguardar as informações recolhidas no processo de monitoramento;
- Destruir as informações recolhidas no processo de monitoramento quando ela não é mais necessária.

5.1.14. Caso seja identificado algum incidente de Segurança da Informação, devem ser seguidas as diretrizes impostas na Política de Gestão de Incidente (POL-052).

5.2. RESPONSABILIDADES

5.2.1. Chefe de Global de TI

- Autorizar os membros de sua equipe a executar procedimentos de monitoramento em rede, sistemas, aplicativos e comunicações de dados que estejam em conformidade com essa política e com todas as leis e regulamentações internacionais relevantes.
- O Chefe Global de TI é responsável pela gestão e implementação desta política, representado no Brasil pelo Diretor responsável pela função de TI.

5.2.2. Gerente Global de Operações de TI

- Autorizar os analistas de TI para executar procedimentos para monitorar a infraestrutura, comunicação, serviços e sistemas aplicativos, tais como: rede, sistemas, aplicações e dados que estejam em conformidade com a política e todas as leis e regulamentos locais e internacionais aplicáveis. Esta função também é representada, no Brasil, pelo Diretor responsável pela função de TI.

- Difundir a cultura de Segurança da Informação.

5.2.3. Administradores do Sistema

- Responsáveis pela realização das tarefas de monitoramento da segurança da informação referente aos sistemas sob sua responsabilidade. Esta função é representada, no Brasil, pelo profissional indicado pelo diretor que representa localmente o Chefe Global de TI.

5.2.4. Gerentes de outros departamentos

- Fortalecer, entre os membros de sua equipe, a cultura difundida pelo time de Seguraça da Informação.