QUESTOR **Política de Segurança da Informação**		
ÁREAS RESPONSÁVEIS Setor de T.I e DPO	**APROVADO POR** DPO e Direção	**DATA DA ÚLTIMA ATUALIZAÇÃO** 21/07/2023
VERSÃO 02	**CLASSIFICAÇÃO** Uso Interno	**CÓDIGO** Questor_PolíticaSegurançadaInformação

Resumo

Esta Política estabelece diretrizes a serem observadas pelos Colaboradores, Terceiros e partes interessadas da Questor Sistemas S.A., com o objetivo de preservar a confidencialidade, integridade e disponibilidade das informações da Companhia.

Índice

1- Introdução

A política de segurança é um conjunto formal de regras a serem seguidas pelos desfrutadores dos recursos de uma organização (colaboradores e prestadores de serviço), para a proteção dos ativos de informação e a prevenção de responsabilidade para todos os usuários. Devem, portanto, ser cumpridas e aplicadas em todas as áreas da organização, levando em consideração duas filosofias por trás de qualquer política de segurança: a proibitiva (tudo que não é expressamente permitido é proibido) e a permissiva (tudo que não proibido é permitido). Contudo, a filosofia proibitiva é a orientação adotada nesta Política de Segurança.

A presente política define que todas as informações coletadas e processadas são consideradas sigilosas e restritas. Portanto, nenhuma informação deve ser utilizada para outra finalidade. Deste modo, compreende-se que as ferramentas internas são exclusivamente para fins de trabalho.

As informações de todos os clientes Questor são sigilosas e restritas ao uso e aplicadas às necessidades do trabalho. Neste caso, os dados dos clientes recebem a classificação de restrição e sigilosidade não sendo possível encontrá-las senão pelo próprio interessado, os dados são tratados de acordo com tal classificação.

Entenda-se "organização" ou "instituição" como: Questor Sistemas S/A.

2- Objetivo

A presente Política de Segurança da Informação tem o objetivo de definir normas e procedimentos específicos relacionados à segurança da informação, bem como discorre a respeito da implementação de controles e processos para seu atendimento.

Assim, este documento foi elaborado a fim de garantir a segurança e acesso à informação, organizar e controlar o uso de equipamentos e software e formalizar as ações e procedimentos.

3- Responsabilidades

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores, de modo que a orientação sobre os procedimentos de segurança, bem como o uso correto dos ativos ocorra a fim de reduzir possíveis riscos. Desta forma, estes devem assinar um termo de responsabilidade *disponibilizado pelo RH*, visto que lhes foram repassadas as informações pertinentes e obrigatórias.

Portanto, a política de segurança deve ser seguida por meio dos procedimentos de

segurança definidos e repassados na integração, tendo subsídio no Manual do Colaborador, sendo estes obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

Em caso de Incidentes de Segurança que afetem Dados Pessoais, os Colaboradores devem seguir as orientações do Plano de Resposta a Incidentes com Dados Pessoais, que deverá ser implementada e continuamente aprimorada com o objetivo de estabelecer orientações estruturadas para remediar referidos incidentes e assegurar (i) o menor impacto aos Dados Pessoais e Titulares envolvidos no Incidente de Segurança; (ii) a notificação rápida aos Titulares de Dados Pessoais e à Autoridade Nacional e/ou ao Controlador, quando aplicável; e (iii) uma robusta resposta interna e externa ao Incidente de Segurança.

O não cumprimento das Normas de Segurança da Informação acarretará violação às regras internas da instituição.

4- Área de Tecnologia da Informação

A Área de Tecnologia da Informação tem a responsabilidade de configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requisitos de segurança estabelecidos.

De mesmo modo, possui a incumbência de administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a organização.

Quando ocorrer movimentação interna dos ativos de TI, a Área tem de garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Não obstante, são responsáveis por planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

OBS: Os administradores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade.

Por fim, compete ao Setor de Tecnologia da Informação, monitorar o ambiente de TI,

gerando indicadores e históricos de uso da capacidade instalada da rede e dos equipamentos; tempo de resposta no acesso à internet e aos sistemas críticos da organização; períodos de indisponibilidade no acesso à internet e aos sistemas críticos da organização; incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante) e atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados,).

5- Segurança da Informação

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada, pertence à referida instituição.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

A instituição, por meio da Área de TI, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas, bem como possui autorização para efetuar auditorias nas máquinas dos colaboradores, sem qualquer tipo de aviso prévio, de modo periódico ou sob demanda.

Cabe a Área de TI montar um Plano de Continuidade de Negócio, visando assegurar a continuidade do negócio durante e após qualquer incidente crítico que resulte em interrupção de sua capacidade operacional normal, garantindo cópias de segurança (backup) de arquivos e dados, bem como o acesso dos colaboradores a este backup, se necessário, mas não se restringindo a estes.

Não obstante, o plano de continuidade de negócios deve ser documentado, testado e revisado periodicamente ou sob demanda, de forma que seus serviços essenciais sejam devidamente identificados, contemplando os mecanismos de Segurança da Informação estabelecidos nos ambientes de produção.

OBS: A restauração de um backup (completa ou parcial) deve ser solicitada à Área de TI por meio formal (e-mail) e após a conclusão da tarefa, a mesma deve ser registrada formalmente pela Área de TI.

As informações devem ser armazenadas preferencialmente eletronicamente, caso tenham sido impressas, devem ser digitalizadas e armazenadas no drive de rede, nas pastas específicas.

Os recursos de informação (documentos, equipamentos, mídias...), quando forem descartados, devem ser tratados de maneira a não permitir a recuperação das informações por terceiros.

6- Mecanismos de Segurança

Referente aos Mecanismos de Segurança, foram adimplidos controles para limitar ou bloquear, de forma parcial ou integral, o acesso indevido, sendo eles:

Controles físicos: são barreiras que limitam o contato ou acesso direto à informação ou a infraestrutura (que garante a existência da informação) que a suporta. Existem mecanismos de segurança que apoiam os controles físicos: Portas / trancas / paredes / blindagem / guardas / etc.

Controles lógicos: são barreiras que impedem ou limitam o acesso à informação, que esta em ambiente controlado, geralmente eletrônico, e que, de outro modo, resultaria em um ambiente vulnerável e desprotegido. Ex: Senhas / firewalls / antivírus / etc…

7- Ameaças à Segurança

As ameaças à segurança da informação são relacionadas diretamente à perda de uma de suas 3 características principais, quais sejam:

Perda de Confidencialidade: ocorre quando há uma quebra de sigilo de uma determinada informação (ex: a senha de um usuário ou administrador de sistema) permitindo que sejam expostas informações restritas; e, essas seriam acessíveis apenas por um determinado grupo de usuários.

Perda de Integridade: aconteceria quando uma determinada informação fica exposta a manuseio por uma pessoa não autorizada, essa, por sua vez efetua alterações que não foram aprovadas e não estão sob o controle do proprietário (corporativo ou privado) da informação.

Perda de Disponibilidade: acontece quando a informação deixa de estar acessível por quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, que aconteceu com a queda de um servidor ou de uma aplicação crítica de negócio, que apresentou uma falha devido a um erro causado por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção.

8- Monitoramento do Ambiente

O Setor de TI tem como dever, implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – Se necessário a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

Não obstante, possui o encargo de tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de solicitação do gerente (ou superior); Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade (ex.: atualização de softwares, limpeza de disco, etc...);Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações (ex.: antivírus).

9- Computadores e Recursos tecnológicos

Os equipamentos disponíveis aos colaboradores são de propriedade da organização, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

As informações (em formato físico ou lógico) e os ambientes tecnológicos utilizados pelos usuários são de **exclusiva propriedade da Questor, não podendo ser interpretados como de uso pessoal**.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Área de TI. As gerências que necessitarem fazer testes deverão solicitá-los previamente à Área de TI, ficando responsáveis pelas ações realizadas.

O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a Área de TI para obter as instruções devidas.

Arquivos pessoais e/ou não pertinentes ao negócio da organização (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem a necessidade de comunicação prévia.

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão

ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Cada colaborador tem acesso somente à pasta de rede relacionada à sua área de trabalho. O acesso às demais pastas (de outras áreas) será fornecido pela Área de TI mediante solicitação formal do gestor da área solicitante.

Acrescentamos algumas situações em que é **PROIBIDO** o uso de computadores e recursos tecnológicos da organização:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem a expressa autorização do proprietário.
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional

10- Dispositivos Móveis

A organização deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que alguns colaboradores usem equipamentos portáteis.

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Área, como: notebooks, smartphones.

Desta forma, a presente norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

Lembrando que todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel (**se possível**).

Não obstante, o suporte técnico aos dispositivos móveis de propriedade da organização e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Assim, não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da Área de TI.

Portanto, deve-se buscar orientação junto a Área de TI quando forem executadas atualizações de versões do sistema operacional.

Ainda assim, o colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da Área de TI. Destarte, a reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: em sua residência, hotéis, fornecedores e clientes.

Lembrando que é responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela organização notificar imediatamente seu gestor direto e a Área de TI. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

10.1- Do Acesso Remoto, Computadores e Dispositivos Móveis Particulares

Todos os colaboradores deverão, quando utilizarem a conexão VPN, manter as boas práticas de uso, considerando que em tal modalidade de conexão todo o tráfego de dados é roteado por um túnel virtual criptografado.

Além disso, deverão, da mesma forma, manter as boas práticas quando utilizarem os instrumentos tecnológicos particulares para fins de trabalho. Isto inclui qualquer tipo de dispositivo que acesse aplicativos ou sistemas cujo a identificação será vinculada à Companhia.

Não obstante, os computadores particulares trazidos às dependências internas da Questor Sistemas S/A para fins de uso, tanto particular, como para o desempenho da função, deverão, obrigatoriamente, ser conduzidos ao Setor de T.I para análise e revisão da

máquina.

11- DataCenter

O Datacenter deve manter-se fechado por meio de chave, no caso da Questor Sistemas S/A por porta com biometria digital, com ambiente apropriado para o funcionamento (ex.: ar-condicionado em constante funcionamento, extintor de incêndio acessível, etc...).

O acesso ao Datacenter somente deverá ser feito por pessoas previamente autorizadas, visando a não interrupção dos serviços: Servidor de arquivos, Acesso à rede interna, Acesso à internet e Telefonia.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado.

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.

Lembrando que não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

Não obstante, a entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com a liberação dos colaboradores previamente autorizados.

12- Uso do Correio Eletrônico

O uso do correio eletrônico é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a organização e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a organização vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e

afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando a organização estiver sujeita a algum tipo de investigação.

Produzir, transmitir ou divulgar mensagem que:

- Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da organização;
- Vise obter acesso não autorizado a outro computador, servidor ou rede;
- Vise burlar qualquer sistema de segurança;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Contenha anexo(s) superior(es) a 20 MB para envio (interno e internet) e 20 MB para recebimento (internet)
- Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Contenha perseguição baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- Tenha fins políticos (propaganda política);

Dica: *Desconfie de e-mails de fontes desconhecidas ou inesperadas, normalmente são e-mails falsos enviados com a intenção de prejudicar ou obter algum tipo de vantagem do destinatário (ex.: dados pessoais ou bancários). Ao receber um e-mail suspeito contate imediatamente a Área de TI informando o fato para receber as devidas instruções. Em hipótese alguma abra o e-mail, mas caso tenha acontecido, não clique em links ou imagens ou execute o download de arquivos.*

OBS: Ao enviar e-mails para contatos fora da instituição, obrigatoriamente deverá constar a seguinte mensagem: O conteúdo desta mensagem é confidencial e destinado exclusivamente aos destinatários. Caso a receba por engano, favor destruí-la e notificar o remetente de imediato. O correio eletrônico não configura meio seguro para transmissão de dados e o remetente NÃO se responsabiliza por eventual erro, atraso, extravio, interceptação ou infecção por vírus. Cabe ao destinatário solicitar a versão física sempre que necessário.

Nos casos em que a mensagem acima não constar no corpo do e-mail, é fundamental solicitar o auxílio da Área de T.I.

13- Uso rede sem Fio

O uso da rede sem fio (Wi-Fi), também é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. Desta forma, a utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a organização e também não cause impacto no tráfego da rede sem fio.

Não obstante, para utilizar a rede sem fio o colaborador, visitante ou prestador de serviço deverá solicitar a senha de acesso à Área de TI.

14- Acesso à Internet

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a organização, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

15- Download de Arquivos

Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades da organização e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela Área de TI.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado que for baixado (instalado) será excluído pela Área de TI.

- Arquivos da organização, proibição de cópia para equipamentos particulares ou com terceiros estranhos à instituição.

OBS: O acesso a softwares peer-to-peer (eMule, Kazaa, BitTorrent e afins) não serão permitidos.

16- Usuário e Senha

Os dispositivos de identificação e senhas protegem a identidade do colaborador (usuário), evitando e prevenindo que uma pessoa se faça passar por outra perante a organização e/ou terceiros.

Não poderá existir login ou senha de uso compartilhado por mais de um colaborador. Portanto, é proibido o compartilhamento para funções de administração de sistemas, pois os acessos são de uso pessoal e intransferível.

A Área de TI responde pela criação da identidade lógica dos colaboradores na instituição (sistemas, redes de computadores).

Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas na Política de Senhas.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é de 90 (NOVENTA) dias.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca para o seu gestor, líder ou comparecer formalmente junto ao setor de TI e Infraestrutura.

17- Documentos de Referência

Série ISO 27000.

Código de Conduta da Questor Sistemas S/A

Manual de Relacionamento com o colaborador

Política de Senhas Questor Sistemas S/A

18- Revisões e Aprovações:

Data	Versão	Descrição	Autor

22.06.2021	1.0	Criação da Política	Setor de TI
21.07.2023	2.0	Atualização da Política	Setor de TI e Setor de Proteção de Dados