Normas e Procedimentos da Requestia

1. INTRODUÇÃO

Esta norma é um documento interno, aplicável a todos os colaboradores, estagiários, consultores, prestadores de serviços, parceiros e sócios (referidos neste documento como apenas "Colaboradores") que venham acessar ou utilizar equipamentos e ter acesso às informações da Requestia e demais ativos tangíveis ou intangíveis da empresa.

Esta norma está alinhada às seguintes políticas:

1. Política de Segurança da Informação da Requestia
2. Política de Privacidade de Dados para Aplicações, Sites e Portais da Requestia
3. Política de Privacidade de Dados para a Plataforma Requestia

As politicas estão disponíveis no endereço **http://requestia.com/docs**

2. PROPRIEDADE INTELECTUAL

Qualquer informação e propriedade intelectual pertencentes a Requestia, ou por ela disponibilizadas, não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas, inferidas ou desenvolvidas pelo próprio colaborador em seu ambiente de trabalho, em acordo ao que está estabelecido nos contratos de trabalho.

Produtos

Para todos aqueles que possuem contato com as informações sobre os produtos desenvolvidos pela Requestia, fica claro que é expressamente proibido divulgar informações sobre futuras atualizações ou versões dos produtos antes do anuncio público oficial feito pela equipe de marketing da Requestia;

Código Fonte

Todos que possuem acesso a qualquer código fonte da empresa, deverão seguir as regras de uso e armazenamento destas informações:

i. Somente é permitido o armazenamento destas informações nos servidores de desenvolvimento, portanto, é proibido qualquer outro tipo de armazenamento;
ii. O código fonte é categorizado como informação confidencial, ou seja, é expressamente proibido divulgar para qualquer outra pessoa que não esteja autorizada a acessar tal informação.

3. CÓPIAS DE SEGURANÇA (BACKUP)

As cópias de segurança da Requestia contemplam arquivos (dados e informações), sistemas digitais, de máquinas virtuais e bancos de dados, código fonte, armazenados e/ou hospedados nos servidores da Requestia, não sendo contemplados dispositivos móveis, notebooks ou desktops;

O planejamento das cópias de segurança deve levar em consideração a importância do dado e relacionar a abrangência (ex: completa ou incremental), a frequência (ex: diária, semanal, mensal, semestral, anual), o período de retenção, versionamento e local de armazenamento;

O procedimento deve considerar que as cópias sejam efetuadas e testadas regularmente, de maneira que os dados copiados estejam em condições de uso quando houver necessidade de recuperá-los;

O procedimento deve definir e disponibilizar requisitos técnicos e operacionais adequados na geração e restauração de cópias de segurança, assim como, para testes de análise e validação;

As cópias de segurança devem ser armazenadas em localidade remota, distante do local principal o suficiente, para o caso de desastre ou impedimento, não comprometa o acesso para a recuperação quando for necessário.

4. ACESSOS ÀS REDES

Todo usuário tem uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal.

A distribuição das senhas aos usuários, inicial ou de recuperação, devem ser feitas de forma segura, ou seja, não devem ser anotadas em agendas, post-its, cadernos, folhas, entre outros.

O acesso a rede de computadores, sistemas e outros recursos de tecnologia da Requestia, é concedido mediante apresentação de uma identificação, geralmente um nome de usuário e senha. Esse método é utilizado para controlar os direitos de acesso as informações, como também identificar cada colaborador e uso dos recursos.

A troca de senha bloqueada só deverá ser liberada por solicitação do próprio usuário, preferencialmente usando um mecanismo de autosserviço. As senhas devem ser alteradas em qualquer caso de suspeita do comprometimento de seu sigilo.

Ao criar uma senha, o usuário deverá seguir a criticidade:

i. No mínimo 10 caracteres;
ii. Pelo menos um caractere especial (! @ # $ % & * _ - + =?. ,);
iii. Um número e uma letra maiúscula;
iv. Não serem idênticas às últimas 5 (cinco) utilizadas.

O usuário deverá evitar colocar na senha dados óbvios, como por exemplo nome da empresa, mãe, pai, cônjuge, data de aniversários, nome de animais de estimação, cidade em que vive, entre outros. Poderá usar para criação da senha palavras ou frases de músicas, poemas, textos, citações entre outros, por exemplo, usando a Música Pais e Filhos da Legião Urbana:

> "**E**státuas **e C**ofres **e p**aredes **p**intadas **N**inguém **s**abe **o que a**conteceu"

A senha poderá ser: *EeCeP-pNsOqu3A*

Rede Corporativa

À Rede Corporativa só deverão se conectar Colaboradores e dispositivos para uso profissional. Senha de rede Wi-Fi da Rede Corporativa deverá atender aos seguintes critérios:

i. A senha da rede corporativa deverá ser trocada a cada 90 dias;
ii. Possuir no mínimo 14 caracteres;
iii. Pelo menos um número;
iv. Uma letra maiúscula;
v. Pelo menos um caractere especial (! @ # $ % & * _ - + =?. ,).

Rede Convidados

Nesta rede poderão se conectar convidados, clientes, fornecedores, colaborador e demais relacionados ao negócio. É apenas nesta rede que deverão ser conectados celulares ou equipamentos pessoais. A senha da rede convidados deverá atender aos mesmos critérios de complexidade da Rede Corporativa.

Acesso via VPN

Os recursos de VPN serão utilizados para acessos externos. A VPN só deve ser acessada em período comercial durante atividades em outros locais, salvo em casos especiais em que esteja alinhado com seu superior imediato.

O uso dos recursos da VPN deverá ser utilizado para fins estritamente profissionais, de forma a cumprir as normas e procedimentos de segurança descrito nesta Norma e na Política de

Segurança da Informação da Requestia, ficando sob responsabilidade do colaborador a utilização adequada dos recursos de VPN.

Autenticação Multi-Fator

Sempre que possível, deve-se usar autenticação multi-fator para acessar as aplicações corporativas como e-mail e a própria plataforma Requestia Service Management usada para atendimento aos clientes da Requestia.

5. EMAIL CORPORATIVO

Todo Colaborador da Requestia recebe um endereço de e-mail. O serviço de e-mail corporativo tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções institucionais.

O Colaborador não deve manter qualquer expectativa de privacidade sobre as mensagens criadas, armazenadas, enviadas ou recebidas através do sistema de e-mail corporativo

6. MONITORAMENTO DE USO

TODOS OS COLABORADORES SÃO CIENTES DE QUE OS RECURSOS ELETRÔNICOS SÃO DE PROPRIEDADE E LICENCIADOS À **REQUESTIA**, E, PORTANTO, A RASTREABILIDADE E MONITORAMENTO DE INFORMAÇÕES NÃO CONFIGURA LESÃO, INVASÃO DE PRIVACIDADE OU QUALQUER CONSTRANGIMENTO PASSÍVEL DE DANOS MORAIS.

7. TRATAMENTO DOS DADOS

Armazenamento e Transferência

Não é permitido realizar o upload (transmitir arquivos) ou compartilhamento de informação confidencial da Requestia ou de seus clientes para serviços e aplicativos de comunicação instantânea, de armazenamento na nuvem ou repositórios digitais, a exemplo, mas não se limitando a Whatsapp, Facebook Messenger, Telegram, WeTransfer, Google Drive, OneDrive, Dropbox, iCloud, Box, Slideshare, Trello, e Scribd.

É proibida a utilização de dispositivos móveis removíveis, como pen drive e HD Externo, para armazenar ou copiar informações classificadas como confidencial e/ou interna, conforme descrito na Política de Segurança da Informação da Requestia.

Para toda informação classificada como confidencial e/ou interna fica proibido o uso de ferramentas online para conversão de formatos (eg. PDF para Word, PDF para Excel, XML para JSON) ou validador de códigos e/ou textos (eg. validador de XML, formatação de JSON). Nestes casos, todos deverão optar por processar e manipular os dados com ferramentas instaladas localmente.

Diretório Temporário de Rede

O diretório temporário de rede da Requestia é uma área comum entre todos da empresa, destinada exclusivamente para transferências entre os usuários de arquivos que não sejam considerados confidenciais. Não use diretórios temporários para armazenamento de documentos classificados como Confidencial.

Descarte Adequado

Quando necessário fazer o descarte de mídias, documentos, entre outros, todos deverão seguir as regras abaixo:

Os documentos deverão ser triturados na fragmentadora de papel;

Não é permitido em lixo comum de documentos confidenciais, como crachás, notas fiscais, currículos, planilhas, entre outros;

Ao descartar objetos como HD, Pen Drive, CDs, DVDs, computadores, notebooks, celulares, entre outras mídias, toda informação contida deverá ser totalmente removida pelo responsável, de preferencia usando métodos como: desmagnetização, destruição física, sobrescrever.

8. DADOS DE TERCEIROS

Os Colaboradores da Requestia usualmente têm acesso a dados de terceiros, clientes, fornecedores ou parceiros, durante a configuração da aplicação ou para a execução de suas atividades de suporte a aplicação.

A manutenção destes dados nos computadores, sejam eles notebooks ou servidores, da Requestia após a execução de tais serviços é expressamente proibida. Devendo tais dados serem descartados assim que não forem mais necessários.

9. AMBIENTES DE TERCEIROS

Nenhum acesso à ambiente de terceiros será feito sem a expressa autorização do seu proprietário ou responsável. Sempre que possível o Colaborador da Requestia deverá fazê-lo mediante o uso de gravação de sessões, usando o recurso de gestão de acesso privilegiado (PAM) disponível no Requestia Service Management (a partir de Março de 2021). O Colaborador deverá informar ao responsável pelo ambiente que estarão disponíveis:

i. a facilidade de acompanhamento remoto das sessões
ii. o acesso as gravações das sessões gravadas

10. HOME OFFICE OU TELETRABALHO

O colaborador que estiver trabalhando em um regime de home-office, teletrabalho ou qualquer outra forma de trabalho remoto (referenciado neste documento como Trabalho Remoto), deverá seguir as seguintes regras:

a) Deverá cuidar que o lugar elegido para o Trabalho Remoto tenha privacidade no que refere a confidencialidade e segurança das informações da Requestia, assim como baixo ruído ambiental;
b) Não é autorizado realizar o Trabalho Remoto em restaurantes, cafeterias, parques, ou qualquer outro lugar público;
c) Não é autorizado realizar a conexão para o Trabalho Remoto através de redes de internet não confiáveis, como redes WiFi públicas, sejam elas de lojas, shoppings ou mesmo uma rede compartilhada com vizinhos.
d) Os colaboradores que praticarem o Trabalho Remoto deverão portar os devidos equipamentos: notebook corporativo com aceso a internet e VPN proporcionado pela companhia, seguindo os critérios vigentes estabelecidos pela área de Suporte e Segurança da Informação;
e) Às práticas de Mesa Limpa e Tela Limpa descritas neste documento também se aplicam ao Trabalho Remoto, bem como todas as demais boas práticas de trabalho descritas nas Políticas de Segurança e Privacidade da Requestia.
f) Deverá retornar ao local de trabalho quando houver impossibilidade de realizar seus afazeres remotamente devido a imprevistos relacionados a falta de energia elétrica, conexão à internet, entre outros.

11. MESA LIMPA E TELA LIMPA

A prática de mesa limpa e tela limpa são destinadas a todos os colaboradores com o objetivo de manter as informações da empresa seguras, evitando exposições desnecessárias e o comprometimento de documentos classificados como internos e confidenciais.

São práticas de **Mesa Limpa**:

a) Não escreva em agendas, post-its, cadernos, folhas, entre outros, quaisquer informações caracterizadas como confidenciais ou internas. Por exemplo: senhas, logins, dados de clientes, fornecedores ou colaboradores, etc.;
b) Ao terminar uma reunião, não deixe informações sensíveis descritas nos quadros brancos ou flip-chart;
c) Não deixe recados nas mesas de outras pessoas através de post-its ou papeis;
d) Não deixe papeis impressos nas impressoras, ao imprimir, pegue imediatamente.

São práticas de **Tela Limpa**:

a) Não deixe a tela do computador desbloqueada evitando assim o acesso não autorizado;
b) Não salve informações categorizadas como confidenciais ou internas no armazenamento local do computador ou área de trabalho, opte por salvar no diretório de rede;
c) Ao final do expediente, ou no caso de ausência prolongada do local de trabalho, guardar os documentos, trancar as gavetas, armários e desligar computador;
d) Os arquivos contidos na "lixeira" do computador deverão ser excluídos periodicamente.

12. CRIPTOGRAFIA DOS DADOS LOCAIS E UNIDADES EXTERNAS

Os dados armazenados em notebooks e desktops devem estar em unidades logicas separadas dos sistemas operacionais e aplicações. Nas unidades logicas onde são armazenados os dados e qualquer unidade externa que contenha informações confidenciais devem estar protegidas por criptografia de dispositivo (Bitlocker).

13. ENGENHARIA SOCIAL

A Engenharia Social se trata da exploração de confiança das pessoas para roubo de informações pessoais ou de empresas. Este tipo de golpe é dado principalmente devido à falta de conscientização do usuário com relação à Segurança da Informação para a obtenção de informações sigilosas e importantes. Ela pode ser feita diretamente, ou seja, pelo contato direto entre o engenheiro social e a vítima através de telefonemas, e-mails, mensagens de texto, mensagens via WhatsApp e até mesmo pessoalmente.

São boas práticas de prevenção a Engenharia Social

a) Nunca considere que uma mensagem é confiável com base na confiança depositada em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada. Portanto, ligue para confirmar com o remetente daquela informação se realmente o assunto tratado é verídico.
b) Para manter as informações da empresa seguras, é vedada qualquer tipo de troca de informações relacionadas à empresa fora do ambiente de trabalho, principalmente com pessoas desconhecidas ou não relacionadas com o processo organizacional.

14. PHISHING

Phishing é um tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário ou organização através da utilização combinada de meios técnicos e engenharia social. O Phishing ocorre principalmente através de envio de e-mails com links, aplicativos e sites que são projetados especificamente para roubar dados e informações.

Boas práticas de prevenção a Phishing

a) Todos os colaboradores, consultores, temporários, parceiros e sócios devem ficar atentos as mensagens recebidas em nome de alguma instituição, que tentem induzi-los a fornecer informações, instalar/executar programas ou clicar em links;

b) Não deve considerar que uma mensagem é confiável com base na confiança depositada em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada;
c) Todos devem ser cuidadosos ao acessar links, executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: .bat, .exe, .msi, .vbs, .ps1, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela equipe de Segurança da Informação da Requestia.
d) É recomendado com que todos excluam os e-mails ou arquivos recebidos que sejam suspeitos e reportem aos supervisores e a equipe de Segurança da Informação.
e) Não é permitido acessar via rede e nem instalar aplicativos de Internet/Home Banking pessoais nos equipamentos da empresa

15. HISTÓRICO DE VERSÕES DESTE DOCUMENTO

Versão 1 de 01 de Dezembro de 2020: Versão inicial do documento (*sob revisão*)