POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A **RF Fábrica de Software** reconhece a importância de identificar e proteger os ativos de informação da organização, evitando destruição, divulgação indevida, modificação indevida ou uso não autorizado de quaisquer informações relacionadas aos seus clientes, funcionários e prestadores de serviço.

A **RF Fábrica de Software** está, portanto, comprometida em desenvolver, implementar, manter e melhorar continuamente o Sistema de Gestão de Segurança da Informação (SGSI), a fim de garantir a confidencialidade, disponibilidade e integridade das informações. Em caso de descumprimento da Política de Segurança da Informação, a **RF Fábrica de Software** tomará as medidas adequadas para corrigir.

Para alcançar esse objetivo a **RF Fábrica de Software**:

- Estabelece objetivos anuais em relação à Segurança da Informação;
- Garante a identificação e o cumprimento dos requisitos do negócio, obrigações contratuais, legais e regulamentares de segurança;
- Desenvolve um processo de análise de risco e, de acordo com seus resultados, implementa as ações adequadas para enfrentar riscos considerados inaceitáveis com base em critérios estabelecidos no processo de Identificação e Avaliação de Riscos.

Nosso Objetivo

Estabelecer as responsabilidades, melhores práticas, recomendações e políticas de uso aceitável e permitido aos recursos de TI por meio de diretrizes e normas, resguardando a segurança das informações da instituição. Preservar a segurança das informações da **RF Fábrica de Software, parceiros, fornecedores, colaboradores e clientes**, garantindo a sua confidencialidade, integridade e disponibilidade.

A Importância da Segurança da Informação

A Política de Segurança da Informação é um conjunto de regras e diretrizes estabelecido por uma empresa para proteger suas informações confidenciais e sensíveis. Ela define como essas informações devem ser coletadas, armazenadas, processadas e compartilhadas de maneira segura, minimizando o risco de vazamentos ou outros tipos de ameaças à segurança.

A Política de Segurança da Informação abrange uma ampla gama de questões, desde a segurança da rede da empresa até a gestão de senhas e a criptografia de dados. Ela também inclui regras para o uso de dispositivos móveis, acesso a sistemas remotos e a privacidade de informações pessoais de clientes e funcionários.

Além disso, a Política de Segurança da Informação estabelece as responsabilidades de cada departamento e funcionário da empresa em relação à segurança de dados, incluindo a forma como eles devem lidar com possíveis violações de segurança. É importante que todos os funcionários da empresa entendam e sigam estas regras para garantir a segurança de informações sensíveis.

Em resumo, a Política de Segurança da Informação é fundamental para garantir a integridade e confidencialidade das informações da empresa, protegendo-as contra ameaças externas e internas. Ela ajuda a criar um ambiente de trabalho seguro e confiável para todos os envolvidos e contribui para a construção de uma reputação positiva da empresa.

Acesso Seguro:

Para acessar nossos sites, os clientes devem usar senhas fortes e únicas.
É recomendável que as senhas tenham no mínimo 12 caracteres, incluindo letras, números e símbolos.
A autenticação de dois fatores (2FA) deve ser habilitada para reforçar a segurança.

Manutenção da Segurança:
Os clientes devem evitar compartilhar suas senhas com terceiros e mantê-las em segurança.
É importante que as senhas sejam alteradas regularmente.

Caso suspeite de comprometimento da conta, o cliente deve entrar em contato imediatamente com o suporte para tomar as medidas necessárias.

Uso de dispositivos não confiáveis:
É recomendável que os clientes não acessem nossos sites em dispositivos públicos ou compartilhados, como computadores em bibliotecas ou internet em cafés e estabelecimentos similares.

Se precisar acessar nossos sites em um dispositivo não confiável, é importante desconectar da sua conta antes de sair.

Atualização de Software:
É importante que os clientes mantenham seus dispositivos atualizados com as últimas atualizações de segurança e correções de bugs.

Conclusão:
A segurança de seus dados é de suma importância para nós. Seguindo estas regras, os clientes podem ter a certeza de que suas informações estão seguras ao acessarem nossos sites. Qualquer dúvida ou preocupação, não hesite em entrar em contato com o nosso suporte.

FÁBRICA DE SOFTWARE®

Política de Segurança de Acesso Externo

A segurança de nossos sites é de extrema importância para nós. Para garantir que nossos clientes acessem nossos sites de forma segura, estabelecemos as seguintes regras de segurança:

1. Acesso ao site somente através de conexão segura (HTTPS);
2. Uso de senhas fortes e únicas para cada conta de usuário;
3. Verificação de autenticidade de usuários através de dois fatores;
4. Monitoramento constante do tráfego de rede para detectar atividades suspeitas;
5. Atualização constante de todos os softwares usados em nossos sites, incluindo correções de segurança;
6. Realização diária de backup dos dados em nossos sites;
7. Limitação do acesso a dados sensíveis a somente funcionários autorizados;
8. Treinamento periódico para funcionários sobre práticas de segurança de dados;
9. Utilização de soluções de segurança de última geração, incluindo firewalls e software antivírus;
10. Impressão de log de acesso aos sites para auditoria.

Recomendações para os Clientes:

1. Evite compartilhar sua senha com terceiros;
2. Atualize frequentemente sua senha;
3. Não acesse nossos sites em computadores públicos ou compartilhados;
4. Mantenha seu computador protegido com um software antivírus atualizado;
5. Não clique em links suspeitos enviados por e-mail ou em páginas da web;
6. Informe-nos imediatamente sobre qualquer atividade suspeita em sua conta.

Ao seguir estas regras e recomendações, nós garantimos a segurança de nossos sites e a privacidade de nossos clientes. Caso haja qualquer violação de segurança, tomaremos medidas imediatas para corrigir a situação e informaremos nossos clientes sobre qualquer ação tomada.

Esperamos que esta política ajude a garantir a segurança de nossos sites e a confiança de nossos clientes em nosso serviço. Qualquer dúvida ou preocupação entre em contato conosco.

A seguir estão algumas regras de segurança para acesso remoto VPN:

Autenticação de usuário forte: é importante que os usuários usem senhas seguras e únicas para se conectar à VPN. A autenticação de dois fatores (2FA) também pode ser usada para reforçar a segurança.

Atualização de software: mantenha seu dispositivo de acesso remoto e software VPN atualizados com as últimas correções de segurança.

Conexão segura: sempre use uma conexão segura, como uma conexão Wi-Fi privada, ao se conectar à VPN. Evite usar conexões públicas ou compartilhadas, pois essas conexões podem ser inseguras.

Criptografia de dados: certifique-se de que a VPN use criptografia de dados forte para proteger as informações transmitidas entre seu dispositivo e a rede da empresa.
Logs de auditoria: mantenha registros detalhados das conexões VPN, incluindo informações sobre o usuário, o dispositivo e o horário de acesso. Isso pode ajudar a identificar possíveis violações de segurança.
Configuração segura: configure a VPN de acordo com as melhores práticas de segurança, incluindo a definição de regras de firewall restritivas.
Treinamento de funcionários: forneça treinamento aos funcionários sobre a importância da segurança de dados e as regras para o acesso remoto à VPN.

Essas regras devem ser seguidas rigorosamente para garantir a segurança do acesso remoto à VPN e proteger as informações confidenciais da empresa.

Normas Gerais aos Colaboradores da RF Fábrica de Software

Responsabilidades dos Usuários de Computador

1. Todo usuário de computador é responsável pelos atos e acessos realizados com sua identificação de acesso no ambiente informatizado;
2. Manter sigilo sobre as informações consideradas confidenciais da **RF Fábrica de Software**;
3. Manter arquivos importantes à Instituição armazenados no servidor de arquivos, a fim de que sejam inclusos na rotina de cópia de segurança (backup);
4. Remover, da rede e das estações de trabalho e notebooks, os arquivos temporários não mais necessários ou arquivos que se refiram a assuntos alheios aos interesses da Instituição;
5. Conhecer e cumprir as determinações da Política de Segurança da Informação da **RF Fábrica de Software**;
6. Comunicar à área de TI qualquer ocorrência que, direta ou indiretamente, afete a Segurança da Informação da **RF Fábrica de Software.**

Proteção de Propriedade Intelectual

1. Todo material produzido por colaboradores da **RF Fábrica de Software** que esteja relacionado ao negócio da Instituição é de propriedade desta;
2. É vedado o armazenamento ou uso de músicas, vídeos e arquivos pessoais nos ativos da **RF Fábrica de Software**;
3. É vedada a instalação ou uso de softwares não homologados para uso nos ativos de TI da **RF Fábrica de Software;**
4. Registro de Acesso e Monitoramento;
5. Toda conexão do usuário (ex: rede, internet, sistemas, correio, estação de trabalho, telefone corporativo, etc.) pode ser monitorada e registrada visando garantir o cumprimento desta Política.

FÁBRICA DE SOFTWARE®

ANEXO I – Orientação aos Colaboradores

PSI V.1 – Manual Política de Segurança de Informação (Sistemas de Informação)

Autoria/Programador: Heber Lencina
Criado em: 15 de dezembro 2021

O que é Segurança da Informação?

Devido ao constante aumento da dependência dos negócios por redes e sistemas interconectados, a informação está cada vez mais exposta a um número crescente e uma grande variedade de ameaças. A informação pode existir em muitas formas: impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, a informação deve ser tratada de forma adequada levando-se em consideração os aspectos da segurança da informação e o valor que possui para a **RF Fábrica de Software**.

A Segurança da Informação é a proteção da informação contra vários tipos de ameaças para garantir a continuidade das operações, minimizar riscos ao qual a instituição está exposta, evitar danos inesperados e garantir o retorno sobre os investimentos realizados na instituição.
A segurança da informação é caracterizada pela preservação de:
a) Confidencialidade: Garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
b) Integridade: Garantia de que a informação não será modificada ou destruída por pessoas não autorizadas ou de forma inadequada que modifique ou inutilize a informação;
c) Disponibilidade: Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

A Segurança da Informação é melhorada a partir da implementação de um conjunto de controles adequados; incluindo políticas, processos, procedimentos, estruturas organizacionais e tecnologia. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e constantemente melhorados, para garantir que os objetivos do negócio e de segurança específicos da instituição sejam atendidos.

As regras descritas neste documento definem a forma como os ativos de T.I (Tecnologia de informação) da empresa devem ser utilizados por seus usuários autorizados.

- Senhas e acessos
- Navegadores
- Serviço de e-mail
- Conexão WI-FI
- Rede interna
- Pen-drives e hardware externo
- Classificação da informação
- Redes sociais
- Serviços mensageiros
- Compartilhamento de arquivos
- LGPD
- Downloads
- Ligações

Senhas e Acessos

Todas as senhas geradas para serviços como sites ou acessos a servidores, devem ser geradas após confirmação com o responsável e ela será cadastrada em sistema centralizado de gestão de senhas. O mesmo serve para o e-mail utilizado caso seja um serviço de terceiro que esteja sendo realizado o cadastro.

Senhas de uso pessoal são de responsabilidade do usuário, porém, quando elas conferem acesso aos ativos da empresa, o usuário deve seguir as boas práticas ao criar a senha e sendo elas de padrão forte. E nunca compartilhar com pessoas não autorizadas ou enviar por meios inseguros ou anotar em locais públicos.

Uma senha sempre é classificada como nível restrito “A” ou seja, nunca deve ser compartilhada com pessoa não autorizada ou repassada por meios inseguros ou informada em ligação. Nunca anotar em local inseguro! E nunca utilizar um padrão fraco como ex: “abc, 123, carro123” datas etc.

Obs: A melhor prática é que as senhas sejam geradas pelo responsável sempre que forem para serviços de terceiros. Ou criar três tipos de senhas para classificação A, B, C: A = restrito, B = Uso interno, C = público (ou irrestrito). Então, sempre que necessário, utiliza-se uma das três conforme classificação do nível de acesso que ela protegerá.

Obs: A melhor prática seria as senhas de classificação “A” restrita serem trocadas periodicamente. (90 dias) no máximo.

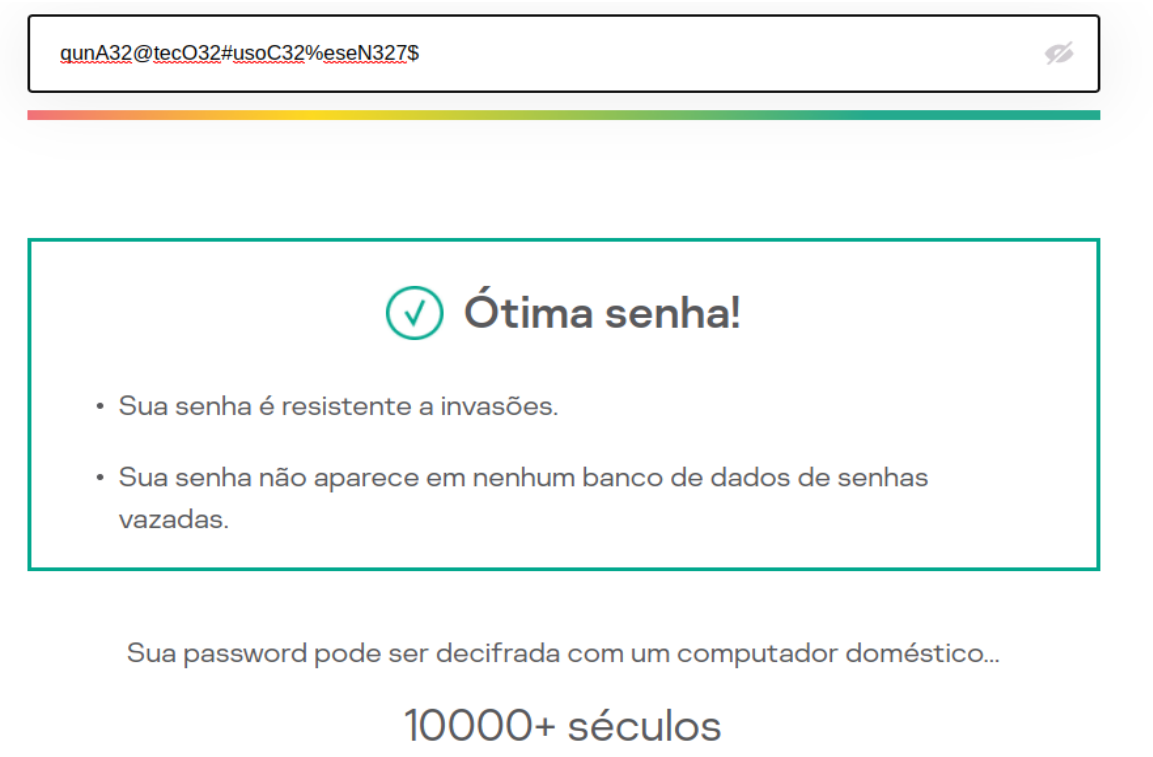
Dica: Como criar um padrão bom de senha, que possa ser lembrado com facilidade. Primeiro escolher uma frase como exemplo: - "Quem não tem colírio usa óculos escuro" então, definir um padrão como exemplo: Pegar as primeiras duas letras de cada palavra "qunatecousocesen" e logo, acrescentar uma regra exemplo: A cada quatro letras adicionar a soma de dia e mês de nascimento exemplo: 28 + 4 = 32 e usar letra maiúscula a cada quatro letras com um caractere especial, nesta sequência @ # $ % & no final de cada número ficando:

qunA32@tecO32#usoC32%eseN327$

Quando precisar lembrar-se da senha, basta lembrar-se da frase e aplicar o padrão. Criando-se três frases para os três tipos de classificação. Toda vez que for criar uma conta em um site, por exemplo, você pensa, este site é inseguro? Utilizar a frase da classificação "C". Este site é restrito? Utilizar a primeira frase classificação "A". Esta prática ajudaria a sempre serem utilizadas as mesmas senhas, e a nunca esquecê-las. Além de que a senha "geneticamente" não seria um tipo de senha fácil de gerar com softwares "geradores de senhas".

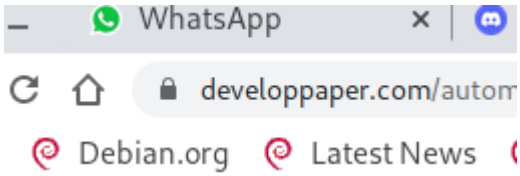
A seguir um exemplo desta senha testada.
Após aplicar esta dica na frase utilizada como exemplo e testar a força da senha em um site que possui inúmeros dicionários de senhas "vazadas", o resultado foi este:

(site kapersky - https://password.kaspersky.com/pt/)

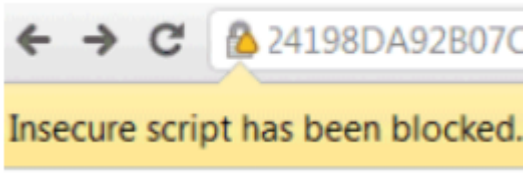


Navegadores

Utilizar navegadores instalados nos computadores e evitar instalar extensões desnecessárias. Sempre verificar se os links a serem abertos são seguros do tipo HTTPS (evitar HTTP). Todo site seguro utiliza “ssl” exemplo:



O site acima está seguro com criptografia!



O site acima está com cadeado quebrado e inseguro!

Não acessar, sites suspeitos, pornográficos ou de pirataria.

Obs: Não baixar “pirataria” (Software ilegal ou sem licença)
Nunca instalar “crack” (ativadores de software)

Procurar manter o navegador sempre atualizado.

Caso haja algum comportamento estranho ou anormal, instalar uma nova versão.

Serviços de E-Mails

Não enviar senhas acessos por e-mail sem autorização.

Cuidado ao abrir e-mail com link evitar clicar no link, sem antes inspecionar.

Se houver dúvidas da origem do e-mail, clicar com botão direito em cima “show original” ou “inspecionar código” e abrirá uma caixa ou semelhante com os dados reais, verificar pelo endereço de origem se realmente é a fonte:

Return-Path: <full-1@gmail.com>
Received: from zimbra.pop3provider.com.br (LHLO zimbra.pop3provider.com.br)
(167.114.21.240) by zimbra.pop3provider.com.br with LMTP; Wed, 15 Dec 2021
10:33:58 -0200 (BRST)
Received: from localhost (localhost [127.0.0.1])
by zimbra.pop3provider.com.br (Postfix) with ESMTP id 4D78521E8A7A
for <full-2@elejaonline.com>; Wed, 15 Dec 2021 10:33:58 -0200 (-02)
X-Virus-Scanned: amavisd-new at zimbra.pop3provider.com.br
X-Spam-Flag: NO
X-Spam-Score: -2.598
X-Spam-Level:
X-Spam-Status: No, score=-2.598 required=6.6 tests=[BAYES_00=-1.9,
DKIM_SIGNED=0.1, DKIM_VALID=-0.1, DKIM_VALID_AU=-0.1,
DMARC_PASS_NONE=-0.6, FREEMAIL_FROM=0.001,
HTML_IMAGE_ONLY_*32=0.001*,
HTML_MESSAGE=0.001, RCVD_IN_MSPIKE_H2=-0.001, SPF_PASS=-0.001,
URIBL_BLOCKED=0.001] autolearn=ham autolearn_force=no
Authentication-Results: zimbra.pop3provider.com.br (amavisd-new);
dkim=pass (2048-bit key) header.d=gmail.com
Received: from zimbra.pop3provider.com.br ([127.0.0.1])
by localhost (zimbra.pop3provider.com.br [127.0.0.1]) (amavisd-new, port 10024)
with ESMTP id csDCW-qdvtdZ for <full-2@elejaonline.com>;
Wed, 15 Dec 2021 10:33:57 -0200 (-02)
Received: from mail-lf1-f43.google.com (mail-lf1-f43.google.com [209.85.167.43])
by zimbra.pop3provider.com.br (Postfix) with ESMTPS id 5A87121E2A60
for <heber.lencina@elejaonline.com>; Wed, 15 Dec 2021 10:33:57 -0200 (-02)
Received: by mail-lf1-f43.google.com with SMTP id k37so42944815lfv.3

Existem fraudes que copiam o domínio, por exemplo:
O domínio real é “www.meusite.com” o falso seria algo como “www.meusite44.com”
Percebe-se alteração no nome do domínio. Um usuário desatento teria aberto o link.

Cuidar quando baixar anexos (geralmente vírus e softwares maliciosos são executáveis ou links para outro endereço que baixa o programa) exemplos de extensões conhecidas de vírus:

CMD – é a abreviação para command (comando, em inglês). Neste sentido, trata-se de uma “ordem” para um programa ou componente de um sistema executar uma tarefa específica.

BAT – este é um arquivo de texto com uma sequência de comandos, escritos linha por linha. É um conjunto de instruções utilizado para executar várias instruções de uma só vez.

SCR – extensão para proteções de tela.

EXE – arquivos executáveis que não precisam de nenhum software para ativá-los, eles são autoexecutáveis.

VBS – sigla para Visual Basic Script (script para Visual Basic). É uma linguagem que acessa elementos de ambientes que utilizam a linguagem.

WS – sigla para Web Service. Trata-se de uma interface que pode ser acessada pela internet e executada em um sistema remoto.

Obs: Nunca utilize e-mail corporativo, para se inscrever em sites de uso pessoal ou sites que demonstram atividade de “spam”. (Sem autorização)

Importante!

Nunca envie dados pessoais, próprios ou de terceiros (clientes) por e-mail ou "WhatsApp" sem autorização! (risco de multas de acordo com a LGPD).

A- Cuidados com o login.

Erro 1: usar apenas uma conta de e-mail.

Muitas pessoas pensam no e-mail como seu endereço de casa: um endereço, um e-mail. A verdade é que o e-mail deve ser como o molho de chaves: cada uma tem sua função. Uma boa dica para o usuário é ter no mínimo três contas: uma somente para o trabalho, uma pessoal e outra para uso genérico e comportamento "perigoso". Isso quer dizer que todas as listas de discussão vão para esta última conta, assim como este endereço é o que você vai usar para posts em blogs e formulários online. Esta conta genérica deve ser substituída a cada seis meses, mais ou menos, já que a esta altura vai estar entupida de spam.

Erro 2: guardar contas carregadas de spam por muito tempo.

É um fato certo que contas de e-mail vão começar a acumular spam depois de algum tempo. Quando acontecer, jogue fora e recomece do zero. Filtrar muito spam dá trabalho demais e desperdiça tempo precioso.

Erro 3: não fechar o navegador depois de deslogar.

Quando você usa seu e-mail a partir de um local público, você precisa não só deslogar da sua conta, mas também fechar a janela do navegador. Alguns serviços de e-mail apresentam o seu usuário mesmo depois de deslogar.

Erro 4: esquecer de apagar cache, histórico e senhas do navegador.

Depois de utilizar um terminal público, é importante que você se lembre de apagar o cache, o histórico e as senhas do navegador. A maioria dos navegadores mantém por padrão um histórico de todas as páginas visitadas, além de senhas e dados pessoais.

Erro 5: utilizar contas de e-mail inseguras para enviar dados importantes.

Grandes empresas gastam grandes somas de dinheiro para certificar-se de que suas redes e contas de e-mail estejam seguras. Nunca utilize e-mail pessoal ou seu computador de casa para enviar dados importantes, que devem ser passados por uma rede protegida.

Erro 6: esquecer que existe o telefone.

O e-mail nunca vai ser à prova de falhas. Portanto, se você não precisa de um registro por escrito ou está falando para o outro lado do mundo, talvez um telefonema seja a forma mais segura de passar informação.

B - Cuidados na hora de enviar mensagens.

Erro 7: não utilizar a opção Cópia Carbono Oculta (CCO).

Quando você coloca o endereço de alguém no campo CCO nenhum dos outros destinatários verá que esta mensagem também foi enviada para ela. Utilizando esta opção, você estará protegendo os endereços das pessoas de spammers.

Erro 8: utilizar sempre o "responder para todos".

Ao utilizar o campo "responder para todos", sua mensagem pode acabar parando na caixa postal de muita gente que nada tem a ver com o assunto. Por exemplo, uma amiga lhe manda um e-mail confidencial sobre suas brigas com o namorado. Em vez de responder este e-mail, você por engano aperta no "responder a todos" do e-mail anterior que ela havia mandado para 23 pessoas e você está encrencado.

Erro 9: repassar e-mail.

Repassar e-mail é uma forma rápida de repassar informações. Mas ao repassar uma mensagem, todos os e-mails para os quais a mensagem inicial foi enviada estarão no corpo da mensagem atual. Se a mensagem cair na mão de um spammer, o estrago está feito. Faça backups e mantenha registros.

Erro 10: deixar de fazer backup de seus e-mails.

E-mails não são apenas para conversar, mas também para fazer contratos e gerenciar transações financeiras, além de decisões profissionais. É importante sempre fazer cópias das suas caixas de e-mail, para o caso de acontecer qualquer problema inexplicável no seu programa e ele perder todos os seus dados. O Gmail, programa de e-mail do Google, por exemplo, perdeu os dados de alguns usuários em dezembro de 2006 por causa de uma pane.

Erro 11: acesso móvel: apagar mensagens online.

O acesso móvel ao e-mail, através do celular e Blackberry, revolucionou a forma de pensar. As mensagens não estão mais atreladas ao PC. Mas tem que se ter cuidado ao ler as mensagens, pois depois de baixar o e-mail para o Blackberry, ele foi excluído do servidor e não pode mais ser baixado em casa ou no trabalho. Caso queira baixar as mensagens posteriormente em um computador, certifique-se de que o seu dispositivo móvel esteja configurado para não apagar as mensagens online.

Erro 12: pensar que um e-mail apagado sumiu para sempre.

Não é só apagar o e-mail da caixa de entrada do destinatário e da caixa de saída do remetente para fazê-lo sumir. Algumas mensagens ficam armazenadas em arquivos de backup nos servidores por diversos anos e podem ser reparadas por profissionais. Então, ao escrever um e-mail, sempre pense que ele será um documento permanente.

C - Saiba evitar e-mails fraudulentos

Erro 13: acreditar que você ganhou na loteria e outras "novidades".

Spammers utilizam uma grande variedade de títulos para convencer as pessoas a abrirem o e-mail cheio de vírus e outros elementos maléficos. Então preste atenção: você não ganhou na loteria, não é herdeiro de um rei nigeriano, não precisa confirmar dados do imposto de renda e nem descobrir quanto está devendo no sistema financeiro - pelo menos não via e-mail não-solicitado. Preste atenção a esses e outros golpes online.

Erro 14: não reconhecer ataques phishing no conteúdo do e-mail.

A melhor forma de se manter livre de ataques de phishing é identificar o golpe na leitura do e-mail. Neste tipo de golpe, o usuário é enganado para entregar seus dados aos criminosos. Tenha cuidado e preste atenção nos detalhes. Um logo distorcido, mensagens requisitando dados imediatos ou ameaçando processar o usuário, e-mails vindos de domínios diferentes do da empresa, são todos indícios de um e-mail de phishing.

Erro 15: enviar dados pessoais e financeiros por e-mail.

Bancos e lojas têm, praticamente sem exceção, uma conexão segura onde é possível colocar dados pessoais e financeiros. Isto é feito porque é sabido que o grau de segurança do e-mail é muito baixo. Portanto, nunca envie qualquer tipo de informação sigilosa por e-mail - e fique seguro de que seu banco não vai lhe pedir para fazer isso. Na dúvida, consulte o banco via telefone ou o site da instituição.

Erro 16: parar de assinar boletins que você nunca assinou.

Uma técnica comum usada por spammers é a de criar boletins de notícias falsos, que trazem um link para se cancelar o envio. Os usuários que desejam se descadastrar (sendo que, na verdade, nunca se cadastraram para receber a mensagem) clicam no link e passam, a partir daí, a receber toneladas de spam. Se você não se lembra de ter assinado um boletim, simplesmente classifique-o como spam. É uma solução melhor do que se arriscar a ter um cavalo-de-tróia (programa que cria uma porta aberta para hackers no PC) instalado na sua máquina.

D - Evite softwares perigosos

Erro 17: confiar em e-mails assinados por amigos.

A maioria dos usuários tem muito cuidado ao ver e-mails de quem não conhece. Mas quando um amigo envia o e-mail, toda a preocupação é esquecida. Mas a verdade é que a possibilidade desta mensagem assinada pelo amigo conter vírus é a mesma do que de qualquer outra. Pessoas que têm programas maléficos (malware) instalados em sua máquina enviam e-mails com vírus sem nem saber disso. Portanto, é muito importante manter um programa de antivírus atualizado em seu computador - e não confiar nem em e-mails assinados por alguém que você conhece.

Erro 18: apagar spam ao invés de classificá-lo como tal.

Classificar um e-mail como spam faz com que o programa de e-mail passe a reconhecer aquele tipo de mensagem como "lixo". Simplesmente apagar a mensagem não faz com que o remetente seja barrado, e você continuaria vítima dos seus ataques.

Erro 19: desabilitar o filtro de spam.

Usuários novos normalmente não têm muito spam e por isso não dão valor ao filtro de spam. Como o filtro não é perfeito, o inconveniente de ter que olhar na caixa de spam por mensagens classificadas erroneamente faz com que muitos desativem a opção por completo. Entretanto, quanto mais antiga a conta, mais spam ela receberá, e sem um filtro, a conta ficará muito difícil de ser administrada e mais complicado será treinar o filtro. Quanto mais cedo o filtro for treinado, maior será a vida útil da conta.

Erro 20: deixar de passar antivírus em todos os arquivos anexos.

Nove em cada dez vírus que infectam computadores vêm por e-mail. Por isso, é importante sempre passar antivírus em todos os e-mails que chegam em sua caixa. Muitos provedores, como o Terra, mantêm serviços de antivírus pela web, onde todas as mensagens são verificadas automaticamente, aumentando a segurança.

E - Mantenha os hackers longe

Erro 21: compartilhar dados com outros.

Todos já o fizeram. Precisamos de um dado urgente do e-mail, telefonamos e pedimos para alguém logar na conta dando usuário e senha. Claro que se confia nesta pessoa, mas mesmo assim, a conta não é mais tão segura quanto antes. O problema é que talvez seu amigo não utilize as mesmas medidas de segurança que você. Ele pode utilizar uma rede insegura ou até ter vírus em seu computador.

Erro 22: usar senhas fáceis de adivinhar.

Hackers utilizam programas que pegam nomes comuns e compilam possibilidades de usuário. Quando alguém recebe spam, o hacker recebe uma mensagem dizendo que aquele e-mail é válido. A partir daí ele roda um programa com um dicionário que vai tentando palavras comuns da língua. Por isso uma boa senha é a que tem no mínimo oito caracteres e intercala maiúsculas, minúsculas e números, sem sentido algum.

Erro 23: deixar de encriptar (codificar) e-mails importantes.

Não importa quantas medidas você tome para estar seguro online, você deve sempre assumir que alguém pode estar acessando seus dados. Desta forma é importante encriptar (codificar) suas mensagens mais importantes para evitar que leiam seus e-mails. Programas de encriptação, como o PGP, estão disponíveis na web.

Erro 24: utilizar uma rede sem fio sem encriptação.

Um dos pontos mais vulneráveis no caminho do e-mail é a distância entre o laptop e o ponto de acesso sem fio. Por isso é importante manter uma encriptação com padrão WPA2. O processo é simples e rápido, mesmo para o usuário mais novato.

Erro 25: deixar de utilizar assinaturas digitais.

A lei agora reconhece o e-mail como uma importante forma de comunicação. Uma forma de combater a falsificação de e-mail é através de uma assinatura digital ao redigir uma mensagem importante. Uma assinatura ajuda a provar de quem e de onde o e-mail vem e que a mensagem não foi alterada no meio do caminho.

Conexão WI-FI

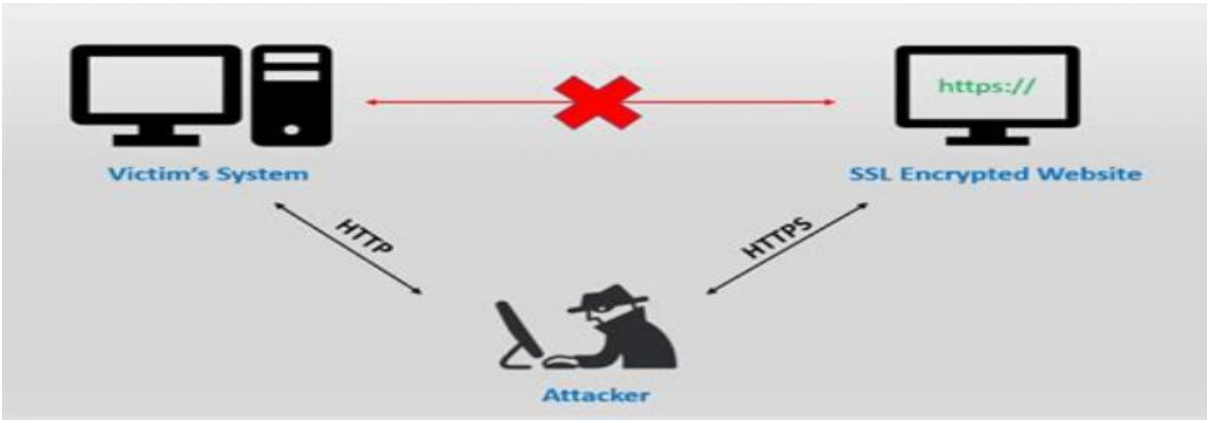
Obs: Cuidado quando instalar Apps que compartilham conexões, pois existem alguns que podem coletar dados de acesso da rede e compartilhar com outros usuários.

A senha do Wi-fi nunca deve ser compartilhada com terceiros sem autorização!

Nunca utilize o Wi-fi para downloads sem autorização!

IMPORTANTE!

Se um invasor conseguir conectar no Wi-fi, será possível realizar ataques do tipo “Man in the middle” (homem no meio). Este tipo de ataque permite que o invasor consiga escutar o tráfego da rede e capturar pacotes, como também fazer um ataque do tipo “sequestro de SSL”. Neste tipo de ataque, ele irá “floodar” (clonar) uma máquina da rede e todo tráfego dela será redirecionado para ele e então ele irá enviar para o site original e será o intermediador da conexão. Exemplo: você irá logar no Facebook, mas o cadeado aparecerá como “quebrado”, se você prosseguir, na realidade estará conectado no computador do atacante.



Rede Interna

A Rede Interna deve estar separada da rede do WI-FI que deve ser isolada. Um invasor pode ter acesso a rede interna (local) ao conectar em um sinal Wi-Fi as chances de invasão de um roteador são altas. Levando em consideração a LGPD existem ativos internos com dados de clientes que poderiam ser facilmente copiados e distribuídos.

Pen-drives e Hardware Externo

IMPORTANTE! Nunca conectar Pen Drives em qualquer computador sem autorização e sem antes verificar presença de vírus.

A conexão de um simples Pen Drive pode instalar um software de conexão remota a um computador!

Não conectar dispositivos externos sem autorização!

Não abrir os computadores da empresa em hipótese alguma sem prévia autorização!

Nunca copiar dados dos computadores para dispositivo externo ou em nuvem sem autorização!

Não dar golpes com as mãos ou outra coisa nas mesas, ou próximo da CPU! Isto pode causar danos ao HD (disco rígido) que está com seus discos a uma alta velocidade, qualquer vibração brusca pode causar ranhuras entre as superfícies dos seus discos.

Classificação da informação

Toda informação dentro de uma empresa possui um nível de acesso. Separados em basicamente três níveis: I, II, III ou A, B, C.

A ou I) Restrito! Para acesso apenas autorizado ou direto.
B ou II) Uso interno! Dentro da empresa, permitido ou não.
C ou III) Público, não há riscos em vazamento.

Quanto à manipulação de dados, eles devem ser classificados pelos respectivos usuários (responsáveis) antes de serem distribuídos.

IMPORTANTE! Contando com o risco da aplicação de multas "pesadas" devido à LGPD (Lei Geral de Proteção de Dados), quando forem identificadas informações de titulares (clientes, pessoas físicas ou semelhantes) **NUNCA DUPLICAR, ENVIAR OU GUARDAR EM LOCAL INSEGURO** sem confirmar antes com o responsável pela gestão destes dados (no caso o DPO - Encarregado Pelo Tratamento de Dados Pessoais). Utilizar o bom senso e se você for o responsável pelo dado tenha controle.

Redes Sociais

As redes sociais devem ser utilizadas para questões de trabalho (salvo, emergências de comunicação!). Exceto quando a empresa específica der liberdade de uso.

OBS: Cuidado com comentários em redes sociais ou posts quando pode haver relação da sua imagem privada com a imagem pública da empresa. Às vezes uma pequena informação pode favorecer a concorrência ou comprometer a imagem da empresa.

Serviços Mensageiros

Quando utilizar WhatsApp ou qualquer tipo de site ou app de mensagens, cuide para não compartilhar informações da empresa com terceiros!

O WhatsApp possui segurança em dois fatores, isso deve ser sempre ativado! (Ou não receberá acesso ao Wi-Fi da empresa). Em caso de roubo, perda ou clonagem evitará que a pessoa não autorizada tenha acessos aos dados do aplicativo. Onde existem informações confidenciais da empresa.

Obs.: Não enviar arquivos com dados sensíveis da empresa ou de terceiros por meio de mensageiros. Exceto quando necessário e se possui autorização para tal.

Compartilhamento de Arquivos

Todo código criado por desenvolvedores da empresa, é produto e objeto intelectual da empresa. Nunca deve ser copiado para mídias, nuvem pessoal ou distribuído ou demonstrado em sites como GitHub, etc.

A empresa deve possuir GIT para controle de versões e também para poder compartilhar software de forma controlada entre os desenvolvedores.

Obs.: não enviar código por site de terceiros ou outros meios (exceto quando autorizado).

LGPD

Lei Geral de Proteção de Dados. Devido a esta lei, todos os dados que pertencem à pessoa física ou jurídica devem ser controlados o acesso, compartilhamento, cópias, distribuição, uso etc. Sendo assim, sempre que qualquer dado que seja sensível for utilizado deve ser levado em consideração a classificação quanto aos níveis de acesso e, também, a autorização de quem irá receber estes dados ou a forma como serão utilizados.

O monitoramento dos dados deve ser levado em consideração em todas as situações. Existe dentro da empresa uma pessoa designada como DPO (Data Protection Officer ou Encarregado de Dados) para controlar a forma como estes dados são armazenados, utilizados e distribuídos. Este responsável deve desenvolver essas políticas e classificar estas informações. Pois, um auditor do governo, pode realizar uma visita à empresa e solicitar tanto a política de tratamentos de dados por escrito, assim como, as evidências de que ela está sendo aplicada. Neste sentido, a colaboração de todos é imprescindível para o cumprimento da adequação à LGPD.

Downloads

IMPORTANTE! Nunca faça download sem autorização!

Cuidado ao baixar de links enviados por e-mails!

Todo arquivo baixado em sistemas Windows deve ser verificado com software antivírus!

Ligações Telefônicas

Os sistemas telefônicos da empresa devem ser utilizados para comunicação de trabalho. Exceto emergências (para outros casos deve ser solicitada autorização).

Obs: Cuidado! Ao repassar informações de nível sigiloso, restrito, uso interno, terceiros ou de clientes via ligação, pois 95% dos ataques “invasores” são do tipo de “engenharia social” (enganar usuários autorizados de ativos computacionais) e, geralmente, grande parte destes ataques são realizados por ligações diretas a funcionários.

Sanções:

A não observância dos preceitos do Regulamento Interno de Segurança da Informação da **RF Fábrica de Software**, suas Normas e Procedimentos, implicará na avaliação pelo Comitê de Segurança da Informação e possível aplicação de sanções administrativas, cíveis e penais previstas pelo Código Penal (Decreto-Lei N°2.848/40, com as alterações da Lei N° 9.983/00 e no Decreto N°2.910/98), no Novo Código Civil (Lei 10.406 de 10/01/2002).

Em caso de dúvidas sempre consultar um responsável.