Política de Segurança da Informação.

Tel: (11) 3158-1047
https://fcamara.com.br/

Sumário

1. Definições Gerais

A segurança da informação tem sido um dos assuntos mais falados nos últimos tempos, desde o surgimento da internet e com o advento de ataques maliciosos. Dessa forma, essa política tem o objetivo de transparecer de forma clara e objetiva como funciona a estrutura organizacional do Grupo FCamara, bem como, a sua preocupação quanto a segurança da organização.

Permanentemente, empenhamos todas as nossas ações e os nossos esforços para prover total segurança e proteção aos dados em que o Grupo FCamara é receptor, primando pela confidencialidade, integridade, disponibilidade, autenticidade, bem como legalidade dos processos que amparam a operacionalização e gestão.

Neste sentido, todas as informações e dados coletados em nosso ambiente são manuseados e armazenados de modo responsável e íntegro, em total observância a legislação vigente e demais regulamentações aplicáveis, por este motivo, não admitimos a não coparticipação nos modelos estabelecidos pela organização.

As informações que concernem ao Grupo FCamara devem ser utilizadas e armazenadas de acordo com as necessidades da empresa, com procedimentos documentados, autorização da equipe competente e, se necessário, autorização da Diretoria. Sendo certo que devem ser utilizados apenas recursos autorizados para garantir o compartilhamento seguro das informações.

Ademais, essa política abrange os direcionamentos quanto a e-mails; acessos; senhas; usuários; utilização de equipamentos; armazenamento; e o descarte de informações, contando com sanções em caso de não cumprimento das diretrizes abaixo elencadas.

2. Diretrizes e Definições Específicas

O fluxo de recebimento de informações **externas** deverão obedecer os passos abaixo, seguindo à ordem:

2.1. Do recebimento de Informação Externa

Antes de iniciar o tratamento de qualquer informação externa recebida, é necessário atentar-se ao revelador da informação, se de fato àquela informação pertence a pessoa que deveria e/ou poderia repassá-la, nas diretrizes comunicadas.

- Como observar se a área externa tem poderes para tanto?

Necessário identificar o domínio do e-mail, o padrão de palavras utilizadas no corpo da mensagem, verificar se a pessoa a qual se comunica faz parte da organização pretendida, dentre outros quesitos a serem utilizados pelo bom senso crítico.

Caso a informação de fato tenha sido repassada por pessoa autorizada, seguirá aos trâmites normais.

2.2. Do repasse da Informação Externa

É necessário observar junto ao Departamento Jurídico se determinada Organização já possui um NDA ('*Non Disclosure Agreement*') assinado com o Grupo FCamara.

Tal medida se faz necessária, em razão de prevenir o vazamento de informações confidenciais de Outra Empresa, evitando possível passivo ao Grupo.

Além do exposto, um NDA assinado evita a possibilidade de utilização de informações de clientes, parceiros e/ou fornecedores, em momento anterior da tomada de decisão. Como por exemplo, a utilização de informações sem permissão, inviabilizando o projeto requisitado.

2.3. Após a assinatura do NDA

Mesmo assinando o documento em comento, faz-se necessária a concentração de informações sigilosas apenas às pessoas que de fato necessitem daquela informação para as funções previamente estabelecidas.

É necessário lembrar que a informação confidencial estará em posse de ambas as Empresas em questão, contudo, em caso de má índole; má expertise; despreparo; imperícia; e/ou neglicência de algum colaborador do Grupo, este responderá isoladamente pelos danos ocasionados.

Ao fazer parte da organização (sendo por contrato de trabalho; em condição de associado; de prestador de serviços; parceiro; ou que de qualquer forma colabore em conjunto ao Grupo FCamara), declara permanentemente medir esforços para seguir essa Política com total abrangência, sendo que o descumprimento das normas estabelecidas implicará a aplicação das sanções pertinentes.

O fluxo de informações internas, bem como, o que fizer referência a dados pessoais, serão tratados em Política de Privacidade de Dados, que complementará esta política.

3. Política de e-mails

Essa política pretende que arquivos maliciosos não sejam compartilhados, bem como, que não sejam vazadas informações confidenciais sem rótulo ou a pessoas indevidas e para que seja disseminada a informação de que qualquer e-mail que saia da caixa corporativa da organização é de propriedade intelectual desta.

A organização estrutural de e-mails corporativos do Grupo FCamara possui os seguintes domínios @fcamara.com.br, @fcamara.com, @fcnuvem.com.br ou @omnik.com.br, precedido de nome e sobrenome do colaborador. Desconfie de e-mails com domínios diferentes dos acima apontados.

Se você é colaborador, para solicitar a criação de e-mails, deverá seguir o fluxo de requisição à infraestrutura interna[1], em conformidade com esta política cabendo ao colaborador atribuir assinatura eletrônica nos moldes da empresa, com seu nome, cargo, unidade de negócio e demais ícones do Grupo FCamara.

É certo que a liberação de acesso aos domínios do Grupo FCamara tem critério exclusivo para a prestação dos serviços contratados, dessa forma a empresa poderá monitorar o e-mail corporativo de seu domínio, sem que haja a notificação prévia para tanto.

O colaborador tem ciência de que não haverá restrição de acesso ao e-mail corporativo pela empresa e que o monitoramento não acarretará violação de privacidade sobre as mensagens criadas, armazenadas, enviadas ou recebidas através do sistema de e-mail corporativo.

Ainda, para evitarmos as práticas de *pishing*, bem como, possíveis ataques *malwares*, recomendamos que **não** sejam abertos anexos com extensões como: .bat, .exe, .src, lnk e .com se não tiver absoluta certeza de que solicitou esse e-mail e de que conhece o remetente. Para combater qualquer conduta neste sentido, entre em contato com a Infraestrutura Interna do Grupo.

[1] https://suporte.ti.fcamara.com.br/support/home

Ao enviar um anexo via e-mail certifique-se de rotular o título e corpo do e-mail com a informação de: confidencial (apenas aqueles destinatários podem visualizar a informação), pública (qualquer pessoa pode visualizar a informação) ou privada (as demais pessoas daquela organização podem visualizar a informação). Caso o e-mail não seja rotulado com as informações necessárias será enviado em caráter confidencial.

Desconfie de todos os assuntos estranhos, de língua estrangeira, de destinatário suspeito ou de arquivo não solicitado. Ao receber um e-mail com essas características com constância, abra um chamado junto à infraestrutura@fcamara.com.br para que seja melhor investigado.

Não reenvie e-mails do tipo: corrente, aviso de vírus, avisos da *Microsoft*, crianças desaparecidas ou doentes, premiação espontânea ou por sorteio, etc.

Ainda, resta claro a proibição de envio de mensagens de baixo calão, xingamentos, ameaças, ou ainda, conteúdos sexistas e/ou racistas, que de alguma forma, ofendam alguém.

Abaixo as melhores práticas que devem ser praticadas:

- Não utilize e-mail da empresa para assuntos pessoais;
- Evite anexos muito grandes, prefira convite à links de repositório interno, com prazo para expiração;
- Compartilhar mensagens ou anexo pertencente a outro colaborador, sem obter a permissão desta pessoa;
- Não envie arquivos acima de 20MB;
- Não utilizar o e-mail corporativo para cadastro em sites de compra;
- Exclua e-mails que estão na quarentena ou no *spam*, com recorrência mínima de 60 (sessenta) dias de intervalo.

4. Política de acessos e senhas

Em detrimento da minimização de dados, devido aos conceitos de *privacy by design* e *privacy by default*, o Grupo FCamara tem realizado os seus devidos esforços para minimizar ao máximo o acesso aos dados em posse e/ou propriedade da organização. Para isso, os níveis de acesso devem obedecer ao cargo do colaborador envolvido, bem como à sua unidade de negócio.

Para fins de acesso, essa política leva em consideração os sistemas internos, como é o caso do Financial e do FCteam; sistemas Terceiros: SharePoint, Teams, Outlook, Tangerino, Be Compliance, Senior, etc; e ainda, sistemas internos de clientes/parceiros/fornecedores, sendo de exclusiva responsabilidade do colaborador manter à sua visualização restrita às suas competências, bem como, arcar com os danos a que vier dar causa mediante acesso não autorizado; acesso prolongado; facilitação dos meios aplicáveis; etc. Para tanto, será devida a denunciação da lide, bem como, ação de regresso.

Todas as pessoas com acesso à informação de propriedade e/ou posse do Grupo FCamara deverão possuir usuário e log único, capaz de identificá-lo ou torná-lo identificável. Exceções a essa regra devem ser aprovadas pela Diretoria, via e-mail, em cópia para a infraestrutura@fcamara.com.br.

A utilização de login único permite com que o Grupo tenha maior controle sobre os acessos, bem como, consiga registrar eventos de entrada em sistema, detectar tentativas de acesso não autorizado, emitir relatórios gerenciais de acesso, etc.

A visualização do colaborador em questão deve ser compatível à função exercida, bem como, deve ir ao encontro ao bom senso em caso de acesso além do necessário, restando a responsabilidade ao colaborador, conforme supramencionado.

Para todos os sistemas utilizados pela Empresa deverão ser disponibilizados e criados acessos únicos e segmentados ao Usuário necessário, sendo expressamente proibido o seu compartilhamento, bem como, a reciclagem de senha por tempo superior a 90 (noventa) dias.

A senha é a forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade da pessoa, evitando que outra pessoa se faça passar por ela.

Para a criação de senhas seguras, será necessário o critério mínimo de 10 (dez) caracteres, sendo ao menos: 1 (um) de letra maiúscula e 1 (um) minúscula, 1 (um) número, 1 (um) caractere especial, sendo vedada a utilização das últimas 5 (cinco) senhas, bem como: data de aniversário, próprio nome, senhas de diversos locais.

As senhas já utilizadas anteriormente não poderão ser recicladas, ainda, caso algum sistema forneça uma senha inicial para acesso ela deverá ser trocada dentro de 24 (vinte e quatro) horas após o primeiro acesso do usuário.

Em caso de erro por 5 (cinco) vezes consecutivas no momento da inserção da senha, o sistema será bloqueado e o usuário deverá abrir chamado junto à infraestrutura@fcamara.com.br.

Para a finalização de cadastros de acesso, deverá ser considerada a dupla autenticação de fatores, para maior segurança junto ao Grupo FCamara, podendo alguns sistemas solicitarem de forma obrigatória a 2FA (*two factors authentication)* [2].

[2] Dupla autenticação de fatores: sistema de segurança utilizado para a verificação em duas etapas diferentes ao mesmo usuário.

5. Política de armazenamento e descarte de informações

As informações e dados coletados pelos colaboradores deverão ser armazenadas em repositório recomendado pelo Grupo FCamara, atualmente sendo o Sharepoint[3].

As informações salvas deverão obedecer aos critérios de pastas compartilhadas com as unidades de negócio da Empresa, observando o acesso permitido para tanto. É vedada a criação de links compartilháveis em pastas de acesso restrito às demais unidades de negócio ou aos usuários externos.

Os documentos da Empresa serão armazenados em observância aos padrões de segurança e confiabilidade internos do Grupo FCamara, através de medidas técnicas e administrativas adequeadas à privacidade e proteção de dados pessoais.

No momento em que esta política foi escrita, utilizamos de tecnologia centralizada da microsoft, como: o microsoft Teams, o microsoft 365, o outlook, bem como, o SharePoint.

Adicionalmente, é importante a ciência dos Usuários de que:

I. Apenas as pessoas autorizadas e vinculadas ao desenvolvimento das nossas atividades, com base nas finalidades previstas nesta Política, terão acesso ao local (físico ou lógico) de armazenamento;
II. Todos os nossos colaboradores, fornecedores, clientes e parceiros deverão se empenhar com a privacidade e a proteção dos dados pessoais, comprometendo-se, sob as penas da lei, a observar os padrões descritos nessa Política e na legislação aplicável.

Adotamos todas as medidas necessárias com foco na proteção dos dados pessoais, entretanto, **é importante destacar que todo o processo de transmissão de informações é passível de ser alvo de acessos não**

[3] Dispositivo de nuvem disponibilizado pela Microsoft (parceira do Grupo FCamara)

autorizados, através de vírus, invasões externas não identificadas, ou, ainda, por falhas técnicas. **Nenhum sistema é considerado totalmente seguro e o Grupo Fcamara não pode garantir integralmente que todas as informações que trafegam internamente não sejam alvo de acessos não autorizados perpetrados por meio de métodos desenvolvidos para obter informações de forma indevida, como por exemplo, um ataque ransomware.**

Na remota e eventual hipótese da ocorrência de tal cenário, envidaremos todos os nossos esforços para colocar em prática os nossos planos de ação, em total observância e conformidade com as disposições legais e normativas aplicáveis.

O Grupo FCamara poderá reter informações dos Titulares de dados pelo período compatível com a finalidade para as quais aquelas informações foram coletadas, conforme dispõe a Política de Proteção de Dados da organização.

Ainda, para se prevenir de eventuais litígios quanto ao processamento, ou para o exercício da ampla defesa, como por exemplo, obrigações jurídicas e regulamentares de auditoria, contabilidade e a termos de retenção estatutária.

Por esse motivo, nós incentivamos a todos a tomarem as medidas apropriadas para se protegerem, como por exemplo, mas não se limitando, à: manter como confidenciais todos os nomes de usuário e senhas criados; utilizar do conceito de “mesa limpa”; não manter usuários/senhas em papéis próximos ao equipamento; manter os antivírus atualizados; bem como, o *backup* e o armazenamento em nuvem; ainda, a contratar os devidos seguros cibernéticos.

6. Política de utilização de equipamentos e redes

Como regra interna do Grupo FCamara, **não** é permitido o uso de notebook pessoal para a prática das atividades contratadas.

A partir do momento da recepção do seu equipamento, por meio de comodato, para a prestação dos serviços contratados o colaborador deverá, nesta ordem:

1. Ter a certeza de que o notebook está sem avarias, sendo o silêncio no recebimento entendido como aceite tácito das condições, bem como, possível responsabilização pelos danos não apurados previamente;
2. Alterar a senha padrão para acesso ao Windows, levando em consideração os mesmos critérios comentados acima, para a criação de senhas nos demais sistemas;
3. Configurar periféricos recebidos, para as devidas interações;
4. Seguir as demais diretrizes intituladas em Termo próprio, de Recebimento de Equipamentos[4].

Bem como, **evitar**:

1. Comidas e bebidas próximas ao equipamento fornecido;
2. Excessivo transporte do equipamento;
3. Quedas;
4. Superaquecimento;
5. Utilizar o equipamento em cima de superfícies não adequadas.
6. Acessar sites duvidosos de fins não profissionais;
7. Baixar softwares ou cópias;

Vale ressaltar que o usuário é responsável direto pela conservação, guarda e utilização dos equipamentos mantidos à sua posse e/ou disposição.

[4] https://camara1.sharepoint.com/:w:/r/sites/PortalFCamara/Modelos%20contratuais/Colaboradores/FC.Termo.de.Entrega.Equipamentos.FC.2022.docx?d=wdd393417a08a49149997729c521db4dc&csf=1&web=1&e=HwnwqA

Caso o cliente final solicite ao operador a utilização de máquina dele, será de responsabilidade do colaborador avisar a governança aplicável, para que não seja caracterizado como descumprimento contratual.

O Usuário deverá garantir que, qualquer uso de redes externas, sejam seguras através de Firewalls, Antispam, Antivírus, Antiproxy, afim de que evite todo e qualquer risco operacional.

Se você for vítima de roubo ou furto, entre em contato em até 24 (vinte e quatro horas) do acontecimento com a nossa Infraestrutura Interna, com o viés de bloquear os acessos indevidos à rede.

No momento do retorno do equipamento à Empresa, seja por fim de contrato, realocação, descanso remunerado, dentre outros motivos, deverá o colaborador assinar o termo de entrega de equipamento.

No momento da entrega, Infraestrutura de TI Interna do Grupo FCamara será responsável pela averiguação técnica do equipamento, podendo o colaborador em questão ter retido de sua própria contraprestação pecuniária o valor necessário para que a Empresa arque com os danos apurados.

Quanto ao uso da internet, o colaborador apenas poderá acessar sites e conteúdos pertinentes à sua área e função, sendo proibido qualquer conteúdo que denigra a imagem do Grupo, como: pornografia, pedofIlia, racismo, jogos, etc.

Quanto à utilização de redes sem fio, o colaborador deverá observar a conexão segura e privada. Qualquer modem ou wi-fi deverá acessado apenas mediante senha devendo ser avaliado como uma rede segura de acesso, preferencialmente as redes disponibilizadas pelo Grupo FCamara, mas, em hipótese alguma, via redes abertas (sem fio e sem senha).

7. Política de acesso físico às instalações do Grupo

Todos os integrantes e visitantes do Grupo deverão portar crachá identificado na portaria do condomínio, bem como, registrar fotografia e biometria no momento do ingresso.

O datacenter próprio do Grupo, bem como, o local de configuração de computadores, apenas será acessado por pessoa autorizada da organização, via de regra, que faça parte do Departamento de Infraestrutura de TI interno.

Todos os controles, nas áreas comuns do condomínio, são realizados por meio de câmeras de vídeo e seguranças devidamente identificados. Sendo necessário informar que as câmeras são estritas aos ambientes comuns, não sendo aplicável aos refeitórios, salas de reunião, banheiros e ambientes internos compartilhados. Dessa forma, **não** nos responsabilizamos por itens deixados sob a mesa; acessos facilitados; fiscalização interna; etc.

As informações confidenciais são mantidas em locais restritos, por meio de chave de acesso, sendo pertinente apenas ao Departamento Pessoal e ao Jurídico, quando aplicável, também ao Departamento de Infraestrutura.

8. Política de Transferência Internacional de Dados

A transferência internacional de dados deverá ser regulamentada pela ANPD, Autoridade Nacional de Proteção de Dados, no sentindo de estipular os países que sejam de fato seguros para tanto, bem como, dispor das normas específicas de cada País.

Entretanto, os colaboradores do Grupo apenas poderão transferir dados internacionalmente quando obtiver a autorização expressa para tanto. Ainda, deverão obedecer os seguintes requisitos:

- ✓ O Receptor deverá cumprir os princípios da Lei Geral de Proteção de Dados ou de legislação própria, quando equiparada ou superior à LGPD;
- ✓ O Receptor deverá conter selos e certificações adequadas;
- ✓ O Receptor deverá ter termo e/ou contrato assinado com o Grupo com as devidas responsabilidades estipuladas; e
- ✓ Quando necessário, deverá ser previamente aprovado pela ANPD.

O termo acima mencionado deverá conter:

i) a devida transparência ao Titular de Dados, explicando seus direitos, como o dado será utilizado e o motivo;
ii) a estrutura de como atender o Titular de Dados;
iii) quais medidas serão tomadas em caso de alteração acidental, divulgação, acesso não autorizado, etc;
iv) cláusula de responsabilidade integral do Receptor, em razão de deter de infraestrutura adequada para tanto;
v) os procedimentos a serem adotados após a vigência do contrato;
vi) a responsabilidade do Receptor por obter o consentimento específico e destacado dos Titulares aplicáveis.

O Grupo FCamara poderá transferir dados internacionalmente, tendo em vista o armazenamento via datacenter das mais conhecidas plataformas de serviços de computação em nuvem, como: Google, AWS, Microsoft, etc.

Ainda, o Grupo FCamara está expandindo e pretende estender-se aos demais países, logo, as informações concentradas em sua sede poderão ser acessadas e/ou transferidas aos demais países em que se localize, obedecendo as normativas que lhe forem impostas.

Ademais, a transferência internacional de dados poderá ocorrer para cumprimento de obrigação legal ou regulatória; proteção à vida; incolumidade física do Titular de Dados, nos termos da LGPD, para tanto, o Encarregado de dados deverá ser notificado para tomar a ação necessária.

Todos os registros de tratamento de dados, bem como, tratativas com o Encarregado de dados deverão ocorrer por meio da caixa de e-mail **lgpd@fcamara.com.br**. Cada responsável por determinada área de negócios, deverá informar ao Encarregado do Tratamento de Dados sobre qualquer alteração nos seus processos de tratamento de dados, bem como, mas não se limitando a novos (as): projetos; procedimentos; ideais; implementações.

Qualquer procedimento que fuja deste padrão, deverá ser expressamente autorizado pelo Comitê Interno de Privacidade de Dados do Grupo FCamara.

9. Sanções

Levando em consideração que o Usuário é o responsável pelo conteúdo das mensagens enviadas sob a sua identificação, bem como, pelo uso de login/senha de caráter pessoal, possibilitando a troca de senhas com a periodicidade necessária de 90 (noventa) dias, a Empresa agirá conforme abaixo estipulado.

A medida em que o Grupo achar necessário, havendo evidências de que esta política esteja sendo descumprida, a empresa terá o direito de tomar as medidas cabíveis, como a rescisão contratual em conjunto com medida cautelar ou tutela antecipada, inclusive com pedido de aplicação de multa diária para o cumprimento da obrigação. Bem como, apuração dos danos em processo judicial ou administrativo, servindo os devidos pareceres técnicos para tanto.

O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade), logo, os usuários e senhas devem ser de uso individual e não deverão ser compartilhados em nenhuma hipótese.

A infração às redações e normas aqui estabelecidas fazem parte integrante ao contrato de prestação de serviços (ou contrato de trabalho, quando se tratar de empregado). Dessa forma, o não cumprimento das diretrizes apresentadas poderão levar à imposição de multa e demais infrações, previstas contratualmente e/ou, quando se tratar de empregado, regerá-se pelas normas da CLT.

10. Plano de conscientização

O Grupo FCamara tem como objetivo principal levar a conscientização a todos os seus colaboradores, para que a segurança seja compreendida por todos.

A meta inicial é de que ocorram ao menos 2 treinamentos por ano, com relação à matéria de segurança da informação e suas ramificações, que incluem:

- Vídeos;
- Materiais didáticos para leitura;
- Avaliações em formato teste para melhor compreensão

Além do exposto acima, o Grupo detém de treinamentos obrigatórios para seus colaboradores e fornecedores/parceiros que necessitem de acesso ao parque tecnológico da Empresa, que podem ser acessados via: https://fcamara.becompliance.com/lgpd/index.html.

O treinamento oferecido é gratuito e conta com 2 (dois) cursos obrigatórios, 4 (quatro) cursos opcionais.

Para conscientização global interna, é de caráter obrigatório a conclusão dos cursos básicos sobre a Lei Geral de Proteção de Dados fornecidos pelo parceiro oficial Be Compliance.

Ainda, enviamos semanalmente *news* internas, via e-mail corporativo; e-books; políticas via Portal Oficial do Grupo FCamara, divulgando novidades e conteúdos, que incluem segurança da informação e LGPD.

Os materiais estarão sempre a disposição de todos os colaboradores, inclusive, em caso de interesse em demais cursos deverão ser requisitados via lgpd@fcamara.com.br.

11. Atualizações e Segurança

Essa política possui uma periodicidade de revisão, no mínimo a cada 12 (doze) meses, conforme eventual necessidade, para fins de adequação e conformidade legal dos seus termos com a realidade do Grupo FCamara.

Todas as alterações serão consideradas válidas, eficazes e vinculantes, e dependendo do tipo de alteração, poderemos avisar através de divulgação em nossos Sites, Aplicativos ou por email, cabendo sempre ao usuário interessado verificar a versão atualizada dessa Política em nossos canais.

Todos os procedimentos internos são fiscalizados pela Diretoria, bem como, pelas áreas relativas e necessárias, como: Departamento Jurídico, Sistemas Internos, Infraestrutura.

Abaixo as demais definições de alguns termos utilizados neste documento:

Empresa e/ou Grupo: Grupo FCamara;
Firewall: Dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança;
Software: Sequência de instruções escritas para serem interpretadas por um computador com o objetivo de executar tarefas específicas. Também pode ser definido como os programas que comandam o funcionamento de um computador;
Log único: Acesso único.

12. Contato e Foro de Eleição/Legislação

O Grupo FCamara se coloca a disposição para resposta de quaisquer dúvidas às presentes políticas, por meio do endereço de e-mail lgpd@fcamara.com.br.

Esta Política será regida, interpretada e executada de acordo com as Leis da República Federativa do Brasil, especialmente a Lei nº 13.709/2018, independentemente das Leis de outros estados ou Países, sendo competente o Foro Central da Comarca de São Paulo Capital para dirimir qualquer dúvida decorrente deste documento.

[Última atualização: 21 de fevereiro de 2022 – São Paulo/SP].