Título:	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - GRUPO SIFRA

Esta Política de Segurança de Informação ("Política") compreende os princípios e as medidas técnicas e administrativas adotadas para a garantia da segurança da infraestrutura de informação do GRUPO SIFRA (o "GRUPO"), grupo empresarial composto por SIFRA S.A., SIGS PAY SOLUÇÕES EM MEIOS DE PAGAMENTO LTDA., SIGSTECH SOLUÇÕES EM TECNOLOGIA LTDA., OSHER INVESTIMENTOS E PARTICIPAÇÕES LTDA., SIFRA SERVIÇOS DE CRÉDITO LTDA., OPINIÃO ASSESSORIA E CONSULTORIA LTDA., OPS DESENVOLVIMENTO DE NEGÓCIOS LTDA. e SIFRA SELL SERVICOS DE CREDITOS LTDA. Esta Política impõe o gerenciamento da segurança de informação pelo GRUPO e estabelece uma estrutura de responsabilidade focada na implementação e manutenção de boas práticas de segurança.

1. ESCOPO

O escopo desta Política abrange as diretrizes de segurança de informação aplicáveis a todos os ativos de informação, sejam eles lógicos ou físicos, de propriedade ou sob responsabilidade direta ou indireta do GRUPO. Isso inclui os ativos de informação sob posse ou controle de seus empregados, gestores, parceiros, fornecedores e prestadores de serviços, além de outras pessoas que se relacionem com o GRUPO sempre que aplicável a responsabilidade do GRUPO.

2. APLICAÇÃO

A Política aplica-se a todos os colaboradores, diretores, parceiros, fornecedores e prestadores de serviços que utilizem redes, sistemas, equipamentos e ativos de informação do GRUPO.

Regras e políticas de segurança adicionais poderão ser adotadas por empresas ou áreas específicas do GRUPO para atender a requisitos regulatórios (e.g. Bacen, ANPD) ou convencionais (e.g. PCI-DSS), desde que não conflitem com esta Política.

3. DEFINIÇÕES

Ativos de informação: ativos físicos (e.g. hardware, documentos, mídias) ou lógicos (e.g. informações, dados) do GRUPO ou utilizados para finalidades corporativas do GRUPO que contenham, acessem, processem ou realizem qualquer tratamento de qualquer tipo de informação, além da própria informação quando aplicável;

Colaboradores: empregados, gerentes, diretores, parceiros, fornecedores e prestadores de serviços do GRUPO.
Custodiantes da informação: colaboradores com acesso autorizado às informações e sua consequente custódia.

Dados pessoais: informação relacionada a uma pessoa natural identificada ou que possa ser identificada mediante esforços razoáveis, ou ainda que possa ser individualizada por meio do tratamento dado a essas informações, mesmo sem que o indivíduo seja identificado.

Informação: conjunto de dados que podem ser interpretados em meio impresso, eletrônico ou escrito, podendo estar armazenada ou ser transmitida por meios eletrônicos ou tradicionais, sendo considerada um ativo que tem valor para o GRUPO e que necessita ser adequadamente protegida.

Proprietários da informação: colaboradores em cargos de gestão responsáveis pelas informações, a quem

compete autorizar acesso delegar sua custódia para colaboradores de que sejam superiores diretos, mas sem isenção de responsabilidade.

4. OBJETIVOS

Esta Política tem como objetivo geral estabelecer as diretrizes de segurança de informação do GRUPO em nível de infraestrutura de tecnologia de informação de forma uniforme entre as empresas do grupo.

São objetivos específicos desta Política:

- Garantir o cumprimento da legislação, regulamentos e diretrizes de boas práticas aplicáveis;

- Cumprir os requisitos de confidencialidade, integridade e disponibilidade de informações;

- Estabelecer controles para proteger as redes, sistemas e ativos de informação do GRUPO contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração ou divulgação de informações;

- Em especial, estabelecer controles para proteger dados pessoais sob responsabilidade do GRUPO contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração ou comunicação, ou qualquer forma de tratamento inadequado ou ilícito;

- Orientar colaboradores do GRUPO a manter a responsabilidade e conhecimento sobre segurança da informação, a fim de minimizar o risco de incidentes de segurança.

- Assegurar a continuidade dos negócios do GRUPO, mesmo na ocorrência de incidentes de segurança da informação, garantindo a disponibilidade e confiabilidade da infraestrutura de tecnologia da informação.

5. PRINCÍPIOS

As medidas e práticas relacionadas à garantia da segurança de informação visam os seguintes princípios:

- **Confidencialidade:** somente pessoas autorizadas devem ter acesso à informação, conforme necessário e suficiente para as atividades e atribuições de cada colaborador, diretor, parceiro, fornecedor e prestador de serviços do GRUPO.

- **Disponibilidade:** as pessoas autorizadas terão acesso à informação sempre que necessário e os recursos para execução de suas atividades estarão sempre disponíveis de forma precisa e tempestiva.

- **Integridade:** a informação será mantida íntegra, com garantia de veracidade, transparência, completude e atualização, de modo que sejam corretas e confiáveis, sem a ocorrência de alterações não autorizadas.

- **Proteção de dados pessoais:** adesão aos princípios da LGPD - Lei de Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e respeito aos direitos à privacidade e proteção de dados pessoais de todos os indivíduos cujas informações sejam tratadas pelo GRUPO.

6. DIRETRIZES DE SEGURANÇA DE INFORMAÇÃO

6.1. Definição de papéis

O Departamento de Infraestrutura do GRUPO avaliará os riscos de segurança de informação e adotará medidas e controles técnicos e administrativos para garantir a confidencialidade, a disponibilidade e a integridade das informações do GRUPO, bem como a proteção de dados pessoais na infraestrutura de informação do GRUPO, segundo as diretrizes desta Política.

Os proprietários da informação serão responsáveis pela supervisão e dos atos dos custodiantes e pela classificação das informações, sendo corresponsáveis pela sua segurança junto aos respectivos custodiantes.

Os custodiantes da informação que devam acessar ou manipular a informação diretamente por conta de suas tarefas ou atribuições no GRUPO serão responsáveis diretos pela sua segurança.

Todos os colaboradores deverão obedecer a esta Política e responderão pela sua violação por culpa (e.g. ato

descuidado ou imprudente) ou dolo (ato com intenção de violá- la).

6.2. Normas gerais de conduta

Informações de propriedade do GRUPO não devem ser divulgadas em redes sociais ou qualquer outro tipo de sistema externo, nem compartilhada com terceiros sem os devidos mecanismos de segurança, tais como criptografia, autenticação e controle de acesso, bem como a assinatura de termo de confidencialidade ou contrato contendo cláusula de confidencialidade.

Na eventual necessidade de terceiros terem acesso a informações que contenham dados pessoais, quaisquer que sejam suas classificações, deve-se proceder com a assinatura de um acordo específico para o compartilhamento ou a operação dos dados.

Os colaboradores devem reduzir a quantidade de cópias de documentos e arquivos com informações do GRUPO ao mínimo necessário.

Os colaboradores devem garantir que os destinatários dos seus e-mails e comunicações sejam apenas aqueles indivíduos que devam ter acesso às informações do GRUPO veiculadas e usar com extremo cuidado recursos como "encaminhar", "responder a todos" e "autocompletar". Esta regra vale para anexos e informações no corpo de e-mail, incluindo campo de assunto e histórico da mensagem. Caso uma mensagem seja enviada para um destinatário indevido, o colaborador deve utilizar imediatamente o recurso "recall", ou outro que permita apagar ou substituir a mensagem que ainda não tenha sido entregue ao destinatário e comunicar o incidente de segurança.

Os colaboradores devem ter o máximo cuidado ao discutir informações do GRUPO em público ou áreas com possível circulação de pessoas ou gravação de som ambiente.

Os colaboradores devem tomar cuidado ao usar seus equipamentos em local público e sempre verificar se uma pessoa não autorizada pode visualizar a tela do seu dispositivo ou ouvir suas conversas acerca de assuntos do GRUPO.

Os colaboradores nunca devem deixar um equipamento de tecnologia da informação sem supervisão ou desbloqueado em local público.

Qualquer ocorrência de incidentes de segurança como roubo ou extravio de documentos, equipamentos, mídias ou informações do GRUPO devem ser imediatamente reportados ao Departamento de Infraestrutura, bem como ao Encarregado pelo Tratamento de Dados Pessoais caso o colaborador suspeite que há dados pessoais envolvidos. O colaborador deve comunicar a ocorrência do fato mesmo se envolver equipamento que não seja de propriedade do GRUPO caso este contenha alguma informação de propriedade do GRUPO.

Todo acesso a ativos de informação, equipamentos, sistemas e servidores do GRUPO será protegido com senhas fortes, compostas por pelo menos 10 (dez) caracteres alfanuméricos letras em caixa alta e caixa baixa e com sinais especiais, que não sejam repetidos.
Obrigatoriamente a cada 45 (quarenta e cinco) dias, as senhas devem ser alteradas, sem repetir as 25 senhas anteriores. Avisos de expiração de senha serão disparados faltando 15 dias para o vencimento. As regras de senhas serão inseridas nas configurações dos ativos de informação, equipamentos, sistemas e servidores e garantidas por meios técnicos adequados. No caso de ativos de informação de maior criticidade, será adotado duplo fator de autenticação.

7. CLASSIFICAÇÃO DE ATIVOS

7.1. Quanto à confidencialidade

Todos os ativos de informação sob responsabilidade do GRUPO serão classificados pelo respectivo proprietário dentre as seguintes categorias, listadas da mais restritiva para a menos restritiva, e informados ao Departamento de Infraestrutura:

- **Confidenciais:** possuem informações que devem ser mantidas em sigilo pois, se divulgadas indevidamente, poderão trazer perdas e danos graves ao GRUPO ou pôr em risco a continuidade de seus negócios;

- **Restritos:** possuem informações cuja divulgação deve ser restrita às pessoas autorizadas do GRUPO pois, se divulgadas indevidamente mesmo dentro da organização, poderão trazer consequências adversas para o GRUPO;

- **Internas:** possuem informações que não devem ser divulgadas ao público, pois tratam de assuntos internos e

se destinam a circulação interna ao GRUPO;

- **Públicos:** possuem informações que podem ser divulgadas ao público sem restrições.

Até que sejam reclassificados pelo proprietário, todos os ativos de informação serão considerados restritos, com circulação autorizada apenas aos subordinados ao proprietário, membros do respectivo departamento.

Ativos de informação restritos, confidenciais ou internos serão eliminados ao fim de sua utilização, de forma segura e irrecuperável, sendo aplicável a sobrescrição completa de arquivos e informações no caso de ativos lógicos e a destruição completa por trituração ou incineração no caso de ativos físicos.

Nenhum documento será reaproveitado para "rascunho" e nenhum dispositivo ou mídia será reaproveitada sem formatação e sobrescrição completa de seu conteúdo.

Ativos de informação contendo informações classificadas do GRUPO não devem ser deixados sem supervisão em cima de mesas ou com acesso desbloqueado, devendo ser trancados ou bloqueados com senha quando estiverem sem uso. Serão configurados bloqueios automáticos de sistemas e dispositivos no caso de inatividade prolongada para evitar essa situação.

7.2. Quanto à criticidade

Todos os ativos de informação sob responsabilidade do GRUPO serão classificados pelo Departamento de Infraestrutura entre **alta, média e baixa** conforme a necessidade de sua disponibilidade para a manutenção dos negócios do GRUPO segundo avaliação de risco de segurança de informação.

7.3. Dados pessoais

Dados pessoais serão sempre classificados como informações confidenciais ou restritas, ressalvada, pela sua natureza e finalidade, sua destinação à divulgação particular (e.g. informações cadastrais de clientes) ou pública (e.g. imagens de modelos em publicidade).

Nenhum ativo de tecnologia da informação contendo dados pessoais sensíveis será classificado em categoria abaixo de confidencial sem passar por uma avaliação de impacto à proteção de dados conduzida junto ao Encarregado pelo Tratamento de Dados Pessoais. Igualmente, nenhum ativo de tecnologia da informação contendo Dados Pessoais será classificado como público ou revelado a terceiros sem consulta ao Encarregado pelo Tratamento de Dados Pessoais.

Todo dado pessoal terá seu ciclo de vida controlado e registrado desde o momento em que o GRUPO passar a ter controle do dado pessoal até o momento de seu descarte definitivo.

O Encarregado pelo Tratamento de Dados Pessoais será informado sobre os gestores responsáveis por dados pessoais e suas classificações, categorias, titulares e finalidades de tratamento, independentemente do nível de classificação do ativo de tecnologia da informação, mesmo nos casos em que o nível de classificação pudesse impedir seu acesso a elas.

8. SEGURANÇA DAS INSTALAÇÕES FÍSICAS

O acesso às premissas do GRUPO será controlado por meio de sistemas eletrônicos de autenticação que gerem registros de entrada e saída. Além disso, o acesso será monitorado com sistemas de alarme e câmeras de vídeo para registro de entrada e saída por meio do uso de chaves que não gerem registros eletrônicos.

O acesso de visitantes ou terceiros às instalações do GRUPO serão liberados caso a caso e registrados pela recepção de forma apropriada.

As chaves das diferentes instalações e áreas restritas do GRUPO serão sempre mantidas em várias cópias, ficando uma em poder de cada Diretor responsável por departamentos e outra sob responsabilidade do CEO. No caso de alteração das pessoas nesses cargos, o segredo das fechaduras será trocado.

O acesso a áreas restritas, inclusive data-centers e salas contendo servidores e equipamentos intermediários de rede, terão controles e monitoramentos específicos de acesso para que este seja limitado aos colaboradores autorizados.

O acesso de visitantes e terceiros a áreas restritas será realizado somente na companhia de um colaborador

autorizado e mediante registro apropriado do acesso pelo colaborador.

O GRUPO manterá inventários de infraestrutura e equipamentos em uso e sobressalentes, com registro das pessoas responsáveis pela sua posse e/ou manutenção. O GRUPO deve manter equipamentos sobressalentes em condições de uso de natureza e em quantidade suficientes para repor imediatamente equipamentos que necessitem de manutenção.

Serão mantidas redundâncias físicas na infraestrutura de informação do GRUPO de modo a minimizar pontos únicos de falha que possam pôr em risco a disponibilidade de recursos de rede.

A infraestrutura de informação do GRUPO, instalada segundo as normas técnicas e de boas práticas aplicáveis, será protegida de intempéries do tempo, picos de energia, infiltrações de água, interferências entre outros eventos adversos.

Datacenters e servidores localizados dentro e fora das premissas do GRUPO serão igualmente gerenciados e protegidos pelo Departamento de Infraestrutura. Servidores de nuvem serão gerenciados pelo Departamento de Infraestrutura do GRUPO com base nas medidas de proteção disponibilizadas pelos respectivos serviços.

9. SEGURANÇA DE REDES

Os equipamentos e recursos de rede serão configurados com senhas fortes sob responsabilidade dos administradores de redes.

Os equipamentos de rede terão seus firmwares e sistemas operacionais mantidos constantemente atualizados e passarão técnicas de "hardening" para prevenção de ataques e acessos indevidos.

As diversas redes locais (LANs / VLANs) e remotas (WANs) serão mantidas segregadas e a comunicação e descoberta de recursos e "hosts" de uma rede por "hosts" das demais será limitada ao mínimo.

Recursos e portas (físicas e lógicas) não utilizados serão mantidos desativados.

Serão utilizados firewalls e sistemas de detecção e prevenção de ameaça (IDS/IPS) na borda das redes.

As conexões remotas com as redes locais serão realizadas de modo protegido e criptografado, por meio de ferramentas de software disponibilizadas e configuradas pelo GRUPO (Remote Desktop).

10. SEGURANÇA DE EQUIPAMENTOS E DISPOSITIVOS

Os equipamentos e dispositivos do GRUPO serão mantidos com sistema operacional, software e firmware constantemente atualizados, inclusive mediante o uso de sistemas eletrônicos de entrega de atualizações (System Center).

Os equipamentos do GRUPO serão configurados pelo Departamento de Infraestrutura de modo a permitir a atualização remota e gerenciamento remoto, inclusive seu bloqueio e formatação via software (InTune) em caso de extravio ou roubo.

Os equipamentos do GRUPO contarão com anti-malware e firewall comerciais, que deverão ser mantidos atualizados e ativos a todo o tempo.

Programas e portas (físicas e lógicas) não utilizados serão mantidos desativados ou serão excluídos.

Será proibido:

- Utilizar equipamentos do GRUPO para fins particulares;

- Armazenar arquivos do GRUPO em dispositivos de uso pessoal, devendo ser usado o servidor (fileserver) para isso;

- Conectar dispositivos periféricos não autorizados aos equipamentos do GRUPO;

- Utilizar dispositivos de armazenamento removível como HDs e SSDs externos, pendrives e outros flash drives.

- Retirar, das dependências do GRUPO, sem autorização formal e expressa, os ativos fixos de propriedade deste, tais como, mas não se limitando a, por exemplo, desktop, monitor, teclado.

Dispositivos particulares (smartphones) serão utilizados apenas excepcionalmente, mediante habilitação de acesso ao servidor de e-mail e sistemas web mediante conexão segura. Tais dispositivos deverão ser mantidos atualizados e com anti-malware ativo pelo respectivo usuário. Serão utilizados programas de gestão remota para desconectar esses dispositivos, bem como apagar ativos de informação do GRUPO e bloquear seu acesso sempre que necessário.

Serão utilizadas medidas técnicas de segurança, inclusive bloqueio e monitoramento remoto nos termos desta Política para garantir a eficácia do disposto acima.

11. SEGURANÇA DE PROGRAMAS E BANCOS DE DADOS

Todos os sistemas lógicos, como software, firmware, sistemas operacionais, aplicativos e bancos de dados do GRUPO serão mantidos atualizados e configurados para o acesso, uso e conexão seguros.

O Departamento de Infraestrutura monitorará constantemente a descoberta ou criação de vulnerabilidades e ameaças, assim como as respectivas soluções ou medidas adicionais de segurança, de modo a evitar eventos adversos.

Fica proibida a instalação e a execução de programas não homologados ou autorizados pelo GRUPO nos equipamentos do GRUPO.

Bases de dados de produção e de testes serão fisicamente segregadas umas das outras. Bases de dados de produção também serão segregadas entre si, de forma física ou lógica, conforme seja adequado para garantia da confidencialidade dos dados contida em cada uma delas.

12. BACK-UPS

Serão realizados back-ups periódicos e automáticos dos ativos de informação em formato eletrônico, incluindo configurações e regras aplicáveis.

Back-ups incrementais serão realizados em periodicidade diária e back-ups completos em intervalos semanal e mensal. O prazo de manutenção dos back-ups mensais será de 5 (cinco) anos e os demais serão sobrescritos a cada nova iteração.

Os back-ups serão testados a cada 6 (seis) meses.

Cópias dos back-ups serão armazenadas em nuvem segura ou mantidas em servidores localizados fora das instalações do GRUPO a uma distância mínima de 5 (cinco) quilômetros.

O Departamento de Infraestrutura criará processos e normas de trabalho para dar efetividade às regras acima.

O Back-up Incremental do Fileserver é realizado nos discos físicos da Storage sempre às 19:00hrs (dezenove horas) e a cada período de 01 (um) dia, de modo que, no momento da conclusão desse back-up, é feita sua duplicação para um disco em Nuvem na Microsoft Azure. Ambos os back-ups possuem tempo de retenção de 05 (cinco) semanas para recuperação rápida.

Em complemento, o Back-up Completo do Fileserver é realizado nos discos físicos da Storage às 19:00hrs (dezenove horas) sempre na terceira sexta-feira de cada mês, de modo que, após a conclusão desse back-up, também é feita sua duplicação, que é enviada para um disco em Nuvem Azure. O tempo de retenção para o back-up completo em disco físico na Storage é de 05 (cinco) semanas, ao passo que o tempo de retenção para o back-up duplicado e enviado ao disco em Nuvem é de 60 (sessenta) semanas.

Após os períodos acima indicados, os arquivos estarão armazenados apenas nos discos Microsoft Azure (Nuvem), sendo considerados como um arquivo morto, com retenção de 05 (cinco) anos.

13. GESTÃO DE ACESSOS

O acesso a todos os ativos de informação do GRUPO será gerenciado e controlado pelo Departamento de Infraestrutura, incluindo acessos a caixas de correios compartilhadas, grupos de e-mail, grupos de fileserver e acesso a e-mails e equipamentos individuais de cada colaborador.

Serão criadas regras de controle de acesso por meio do de grupos e perfis de acesso conforme as atividades, tarefas e atribuições de cada colaborador ou grupo (role-based) e limitando-se o acesso a ativos de informação conforme a necessidade de conhecimento da informação para suas atividades, tarefas e atribuições (need-to-know basis). Acessos temporários somente serão concedidos para determinadas tarefas e de forma justificada (context-based).

As solicitações de acesso dos colaboradores serão feitas por escrito pelos respectivos gestores, por meio do sistema SiGS Solicitações e Chamados, registradas pelo Departamento de Infraestrutura e implementadas por ferramentas eletrônicas (Active Directory).

A concessão de acessos será baseada na função profissional de cada colaborador nas empresas do GRUPO e obedecerá ao critério de necessidade para a realização das atividades e tarefas inerentes àquela função.

O acesso aos ativos de informação, sistemas e equipamentos do GRUPO será realizado por meio de senhas fortes sob responsabilidade dos colaboradores que os utilizem.

Nenhum colaborador terá acesso completo aos ativos de informação, sistemas e equipamentos do GRUPO e serão minimizadas situações em que um colaborador possa acessar e apagar por conta própria os registros de seu próprio acesso e utilização.

É habilitada, para todos os usuários criados pelo GRUPO SIFRA, sejam eles novos ou antigos, a autenticação de dois fatores (MF2), a fim de que fique comprovado que o usuário é, de fato, o dono da respectiva conta Office. Essa autenticação poderá ocorrer através da geração de um código no Aplicativo Microsoft Authenticator, via ligação, ou, ainda, envio de SMS para o celular cadastrado na ocasião do preenchimento do MF2.

14. USOS ACEITÁVEIS PELOS COLABORADORES

14.1. Regras de gerais

Além das restrições colocadas nos demais tópicos desta Política, é proibido o acesso, guarda e/ou veiculação, individualmente ou em grupo, por quaisquer dispositivos, sistemas, e-mails, aplicativos e meios de comunicação corporativos ou no contexto das atividades profissionais do GRUPO, dos seguintes conteúdos:

- Material pornográfico e/ou ilegal;
- Material e/ou linguagem grosseira ou ofensiva;
- Material calunioso, abusivo ou que invada a privacidade de alguém;
- Imagens e/ou linguagem obscena ou pornográfica;
- Informação sobre atividades ilegais e incitação ao crime conforme a lei local de qualquer dos envolvidos;
- Prática, indução ou incitação de preconceito quanto à origem, raça, etnia, sexo, gênero, orientação sexual, cor, idade, crença religiosa ou qualquer outra forma de discriminação;
- Material protegido por direitos autorais, ou publicação de sons, fotos ou textos sem autorização do autor ou de seu representante legal, publicação de fotos sem autorização dos fotografados e distribuição de arquivos sem autorização de pessoas ou empresas responsáveis;
- Informação relativa à pirataria de material protegido pelas leis de direitos autorais, propriedade industrial e outros direitos intelectuais;
- Dados pessoais e/ou informações classificadas do GRUPO;
- Propaganda eleitoral, material de cunho político ou religioso, ou de viés ideológico ou partidário;
- Arquivos ou códigos maliciosos ou que o usuário sabe ou espera que sejam nocivos, incluindo vírus, "travas" ou "bloqueios", arquivos ou códigos destinados a pregar peças ou brincadeiras, correntes, entre outros.

O uso de quaisquer dispositivos, sistemas, e-mails, aplicativos e meios de comunicação corporativos ou no contexto das atividades profissionais do GRUPO será restrito aos dias e horários de trabalho de cada colaborador, salvo se este estiver em plantão, quando possuir cargo ou função cujas atribuições incluam a prontidão para resposta a qualquer momento, ou quando houver uma emergência e o usuário receber autorização de seu gestor pelo contato via aplicativo de comunicação instantânea de sua preferência.

14.2. Acesso à internet

O acesso à internet pelas redes corporativas do GRUPO será realizado mediante identificação do colaborador

e restrito a assuntos profissionais do GRUPO. Serão adotadas medidas técnicas de bloqueio de tráfego e acesso a determinados websites que sejam proibidos por esta Política.

É proibido acessar, pelas redes corporativas do GRUPO, websites alheios às atividades profissionais do colaborador, como instituições financeiras ou de pagamento, redes sociais, serviços de streaming, servidores de download de mídias, jogos, webmails e drives pessoais, pornográficos, que disponibilizem material ilícito ou conteúdo pirateado, entre outros.

Os diretores poderão solicitar liberação de acesso a websites específicos ao Departamento de Infraestrutura, para si ou para colaboradores subordinados a eles. A liberação de acesso será documentada.

As medidas técnicas de restrição de acesso a websites não serão aplicáveis aos colaboradores do Departamento de Infraestrutura devido à natureza de suas atribuições.

14.3. E-mail

O uso de e-mail corporativo do GRUPO será realizado mediante identificação do colaborador e restrito a assuntos profissionais do GRUPO.
É proibido o uso de e-mails pessoais ou autenticados para outro colaborador nas atividades profissionais do GRUPO.

Serão adotadas medidas de prevenção de vazamento de dados para bloqueio automático do tráfego de e-mails suspeitos de conter dados ou programas maliciosos, informação classificada ou dados pessoais. A liberação de e-mails bloqueados indevidamente deve ser solicitada ao Departamento de Infraestrutura de forma documentada.

14.4. Aplicativos

Poderão ser utilizados os seguintes aplicativos de comunicação instantânea nas atividades profissionais do GRUPO, em ordem de prioridade:

- **Aplicativos corporativos:** aplicativos gerenciados pelo GRUPO serão o padrão de comunicação instantânea nas atividades profissionais do GRUPO e sempre podem ser utilizados por aqueles que têm acesso a eles.

- **Outros aplicativos de comunicação instantânea homologados:** poderão ser utilizados apenas nos casos em que for impossível ou inviável o uso de um aplicativo corporativo, sendo necessária a autorização do gestor imediato do usuário para seu em determinados processos ou atividades, responsabilizando-se tanto o usuário quanto o gestor pelo uso feito do aplicativo. São eles os aplicativos de uso corporativo que possuam capacidades de comunicação instantânea built-in, as quais não sejam normalmente utilizadas em processos e atividades corporativas.

- **Aplicativos de comunicação instantânea não homologados:** não poderão ser utilizados, salvo quando for estritamente necessário para comunicação de emergência, em especial envolvendo perigo iminente à vida ou à integridade física de alguma pessoa, ou risco iminente à integridade material ou de perda de direitos do GRUPO, ou, ainda, para comunicação casual em que não haja tomada ou comunicação de decisões, assunção de obrigações, comunicação e cumprimento de instruções de trabalho ou tráfego de informações confidenciais ou dados pessoais. São eles: WhatsApp, Telegram, Facebook Messenger, Signal, Instagram, Skype, entre outros.

Os colaboradores do GRUPO utilizarão aplicativos de comunicação instantânea corporativos e homologados nas suas atividades profissionais do GRUPO, mediante uso de suas credenciais fornecidas pelo GRUPO.

Excetuados os casos especiais de plantão ou emergência acima, os colaboradores poderão desconectar ou manter os aplicativos de comunicação instantânea em modo "mudo" e não deverão respondê-los fora de seus dias e horários de trabalho. Nessas situações, os gestores dos colaboradores deverão dar preferência a outros canais de comunicação, como ligação telefônica, para emergências que requeiram resposta imediata.

A tomada ou comunicação de decisões, assunção de obrigações e a comunicação e cumprimento de instruções de trabalho por meio dos aplicativos de comunicação instantânea deverão ser restritas a emergências e documentadas e realizadas na primeira oportunidade dentro da jornada de trabalho, ou imediatamente nos casos de plantão ou emergência conforme dispostos acima.

Em caso de desligamento de um colaborador, todo o conteúdo e histórico de aplicativos de comunicação instantânea relacionados às atividades do GRUPO serão excluídos remotamente ou, em caso de

impossibilidade, deverão ser excluídos pelo colaborador. O mesmo deve ocorrer no caso de alteração de cargo ou atribuições dos usuários com relação a conteúdo e histórico de aplicativos de comunicação instantânea não relacionados com seu novo cargo ou atribuições.

Apesar de designados para uso nas atividades profissionais do GRUPO, a empresa valoriza a interação social e o bem-estar de seus empregados e terceiros, de modo que a comunicação não relacionada ao trabalho poderá ser tolerada pelos gestores nos aplicativos de comunicação instantânea, especialmente nos períodos de menor movimento, desde que o volume de comunicações seja razoável e que elas não interfiram nas comunicações dos usuários para atividades profissionais nem nos trabalhos de cada colaborador, ou incorram em conduta proibida.

15. MONITORAMENTO E REGISTRO

Dados e informações relativas à disponibilidade, tráfego, acesso e utilização de ativos de informação, sistemas, redes, aplicações, servidores, redes e e-mails corporativos, bem como suas conexões com dispositivos, tanto corporativos como particulares, serão monitorados e registrados em servidores dedicados (syslogs), com a finalidade de garantir a segurança de suas informações e sistemas.

Igualmente, será monitorada integralmente a utilização de dispositivos corporativos com a finalidade de garantir a segurança dos ativos de informação e sistemas do GRUPO. Dispositivos particulares não serão monitorados nem acessados além da extensão expressamente disposta nesta Política.

O monitoramento abrangerá também acessos externos aos equipamentos, sistemas, servidores, redes e aplicativos corporativos do GRUPO e acessos externos a ativos de informações do GRUPO por redes e sistemas de comunicação eletrônicos, inclusive o acesso aos e-mails corporativos, por meio de conexão externa (webmail) e por dispositivos móveis.

O GRUPO reserva-se o direito de registrar e monitorar os usos, acessos, dados e comunicações de ativos de informação, equipamentos, sistemas, redes, servidores e aplicativos para a finalidade específica de manutenção da legalidade e segurança no ambiente de trabalho, incluindo o monitoramento em tempo real da cópia e movimentação de arquivos nas redes corporativas e registro de palavras-chave via sistema de prevenção ao vazamento (DLP).

O Departamento de Infraestrutura deve agir imediatamente para remediar ou minimizar incidentes de segurança quando identificado mau uso das tecnologias.

Serão mantidas trilhas de auditoria aptas a comprovar a ocorrência e a autoria de atos ilícitos, descumprimento de regras corporativas e/ou uso irregular de ativos de informação, equipamentos, sistemas, redes, servidores e aplicativos corporativos.

O administrador do domínio, integrante do Departamento de Infraestrutura, deverá coletar e interpretar evidências de trilhas de auditoria mediante solicitação formal da Diretoria para as finalidades de manutenção da segurança e evitar, remediar ou minimizar incidentes de segurança, sem necessidade de aviso prévio.

O acesso aos registros e trilhas de auditoria deve ser limitado ao administrador do domínio e somente poderá ser realizado de modo justificado e registrado perante a Diretoria.

16. HOMOLOGAÇÃO DE TERCEIROS

Todo e qualquer serviço, sistema, equipamento, aplicativo, programa ou rede de terceiros que deva ter acesso, integração ou comunicação com os ativos de informação, sistemas, equipamentos, redes, ou servidores do GRUPO deverão ser objeto de homologação pelo Departamento de Infraestrutura antes de sua utilização.

Contratos relativos a tais serviços, sistemas, equipamentos, aplicativos, programas ou redes de terceiros somente serão assinados quando preverem a possibilidade de encerramento sem penalidades pelo GRUPO caso a homologação se mostre impossível ou inviável.
A homologação será realizada em ambiente de teste segregado dos ambientes de produção do GRUPO, utilizando-se, quando aplicável, somente dados e informações sintéticas ou anonimizadas.

O Departamento de Infraestrutura criará regras e processos de homologação adequados à realidade do GRUPO.

17. EVENTOS ADVERSOS

O GRUPO implantará processos de endereçamento de eventos adversos, como incidentes de segurança e desastres, que sejam aptos a interromper, remediar ou mitigar tais eventos e suas consequências adversas, bem como garantir a resiliência e continuidade dos negócios do GRUPO.

18. RESPONSABILIDADES

Cada colaborador é responsável pelo cumprimento desta Política e demais normas aplicáveis, bem como por possibilitar a boa realização dos trabalhos do Departamento de Infraestrutura.

O Departamento de Infraestrutura é responsável por dar efetividade a esta Política.